IGEM-HERC GRANT PROPOSAL COVER SHEET

State Board of Education

PROPOSAL NUMBER: (to be assigned by HERC)	AMOUNT REQUESTED: $2,099,700 over three (3) years

TITLE OF PROPOSED PROJECT: Library of Reconfigurable Immersive Attack and Defend Scenarios for Cybersecurity Research and Workforce Development

SPECIFIC PROJECT FOCUS:

Idaho's economy depends on secure cyberspace and resilient industrial systems, and thus demands a larger highly skilled cybersecurity workforce. We propose a game-changing capability for multi-disciplined research and workforce training. This novel, immersive environment will integrate real physical processes, full-scale enterprise IT systems, and Internet-scale cyberattacks on-demand to offer researchers, students, and trainees a controlled live-fire environment like no other currently available. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) at the University of Idaho (UI) Idaho Falls Center for Higher Education (UIIF) will provide a hybrid virtual and physical environment of enterprise-scale information technology systems and bench-top physical process systems under digital control. Combining the unique element of live adversarial activities including remote access malware, ransomware, and advanced persistent threat agents, we will create an immersive environment that is reconfigurable, redeployable, and replayable. In short, we intend to create an **Adversary-as-a-Service** offering with real-world physical systems and realistic simulated Internet-scale cyber-attacks. With this capability, our local team from UIIF and Idaho State University (ISU) will support a significantly larger number of students across our programs on this campus with hands-on project-based learning. By integrating this unique offering into the Idaho Cyber Range (ICR), we will immediately be able to reach students and collaborate with researchers from all public institutions of higher education on eight additional campuses. We will provide unique red-teaming activities across the ICR - forensics data, incident logs, and recorded 'wargame' data for use in training and research, and support for games, clubs, or training events throughout the region and across the state. Idaho's industries and the nation will be provided an increased, steady pipeline of graduates significantly better prepared to face the challenges of defending cyberspace.

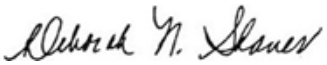
PROJECT START DATE: 7/1/2022	PROJECT END DATE: 6/30/2025
NAME OF INSTITUTION: Regents of the University of Idaho	DEPARTMENT: Computer Science, Center for Secure and Dependable Systems

ADDRESS: Center for Advanced Energy Studies, 995 MK Simpson Blvd, Idaho Falls, ID 83401

E-MAIL ADDRESS: osp@uidaho.edu	PHONE NUMBER: 208-885-6651

	NAME:	TITLE:	SIGNATURE:
PROJECT DIRECTOR/PRINCIPAL INVESTIGATOR	Michael Haney, Ph.D., CISSP	Associate Professor	
CO-PRINCIPAL INVESTIGATORS	Dr. Robert A. Borrelli Dr. Constantinos Kolias Dr. Dakota Roberson	Associate Professor Assistant Professor Assistant Professor	

NAME OF PARTNERING COMPANY:	COMPANY REPRESENTATIVE NAME:

	NAME:	SIGNATURE:
Authorized Organizational Representative	Deb Shaver, Director, Office of Sponsored Programs	

1. Name of primary Idaho public institution. University of Idaho

2. Name of Principal Investigator directing the project. Prof. Michael A. Haney

3. Project objective and total amount requested. *A total of $2,099,700 is requested over a three year period beginning FY23.* Idaho's economy depends on secure cyberspace and resilient industrial systems, and thus demands a larger highly skilled cybersecurity workforce. We propose a game-changing capability for multi-disciplined research and workforce training. This novel, immersive environment will integrate real physical processes, full-scale enterprise IT systems, and Internet-scale cyberattacks on-demand to offer researchers, students, and trainees a controlled live-fire environment like no other currently available. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) at the University of Idaho (UI) · Idaho Falls Center for Higher Education (UIIF) will provide a hybrid virtual and physical environment of enterprise-scale information technology systems and bench-top physical process systems under digital control. Combining the unique element of live adversarial activities including remote access malware, ransomware, and advanced persistent threat agents, we will create an immersive environment that is reconfigurable, redeployable, and replayable. In short, we intend to create an **Adversary-as-a-Service** offering with real-world physical systems and realistic simulated Internet-scale cyber-attacks. With this capability, our local team from UIIF and Idaho State University (ISU) will support a significantly larger number of students across our programs on this campus with hands-on project-based learning. By integrating this unique offering into the Idaho Cyber Range (ICR), we will immediately be able to reach students and collaborate with researchers from all public institutions of higher education on eight additional campuses. We will provide unique red-teaming activities across the ICR - forensics data, incident logs, and recorded 'wargame' data for use in training and research, and support for games, clubs, or training events throughout the region and across the state. Idaho's industries and the nation will be provided an increased, steady pipeline of graduates significantly better prepared to face the challenges of defending cyberspace.

4. Resource commitment. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education. The University of Idaho and Idaho State University have both committed significant resources to development of their cybersecurity programs for well over two decades. In recent years, more effort has been made to develop the capabilities of each program on the jointly-operated Idaho Falls campus. Funding from this grant will be committed primarily to the acquisition and implementation of a variety of cyber-physical systems equipment and private cloud computing equipment to develop our cyberspace 'shooting gallery' and adversary-as-a-service offering. This is the pinnacle of development of a research and education space that has evolved over many years. The UIIF and ISU faculty and staff in eastern Idaho have committed immeasurable resources in their time and skills to develop a workspace conducive of adversarial-based immersive cybersecurity education. With previous investments from our universities, including Idaho Global Entrepreneurial Mission Initiative (IGEM)-Higher Education Research Council (HERC) funding, and the Idaho Cybersecurity Education Initiative in FY21, we have dedicated over 2000 square feet of space in three adjacent rooms for cybersecurity education and research. Specifically with the funds provided to both universities as part of the governor's initiative, we now have a ready-to-occupy server room designed to support student computing needs. The PI Prof. Haney is joined on this proposal by six co-PIs from the two institutions that will design, build, and integrate the cyber-physical systems necessary for this effort. Funding from this grant will support researchers and students working collaboratively through an intensive several weeks each summer building our wargames space. Cybersecurity is a top priority for our universities, our state and our nation, and we are at a crucial time in

preparing to defend our cyberspace. With this grant, we will provide a world-class state-of-the-art research and training capability like no other.

Specific project plan and timeline. We currently assess our capability in UIIF at a Level 4 on the Technology Readiness Level (TRL) spectrum [1]. We have designed, tested, published [2–4], and validated our foundational network security zoned architecture that enables deploying, monitoring, and maintaining cyber wargames and scenarios. We have acquired space adjacent to our south side of campus to expand our computing capacity, as well as connected to the electronics laboratory on our north side ready to receive additional bench-scale cyber-physical systems. With this funding, we aim to advance to TRL 7 by developing the scale and complexity to reconfigure the environment into multiple scenarios and states of play, making our capabilities accessible to partners across the state via the Idaho Cyber Range, a key facet in workforce development [5–9]. Project phases include -

(1) Equipment acquisition,

(2) Planning,

(3) Recruitment,

(4) Scenario development, and

(5) Wargames deployment.

We will recruit graduate students and a postdoctoral researcher to direct subsequent project phases and coordinate research. Co-PIs will collaborate on a plan for the space by combining prior efforts in diverse cyber-physical systems design, to include small scale (e.g. a single pump controller) and bench-scale (e.g. a 3-tank water heat transfer loop) projects to deploy and install. The team will concurrently acquire equipment and develop playbooks and tools to initiate, detect, and defend against red team attacks. We will then bring in students, trainees, and red team volunteers to execute various projects and experiments.

Cybersecurity Hardware in the Loop Equipment. (*Lead - Borrelli*)

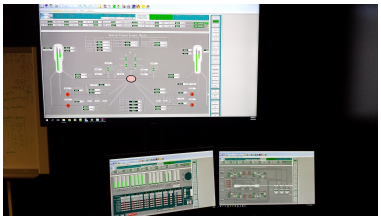


Fig. 1. WSC Simulator.

Overview. IGEM funding will be used in this Workscope to build hardware in the loop infrastructure to interface with the Western Services Corporation Simulator (WSC) to assess vulnerabilities of nuclear systems resulting from the increasing digitization across the sector. This infrastructure will simulate balance of plant with WSC or in a standalone mode extant of the nuclear reactor itself. Controls and data delivery systems will be designed to enhance system resiliency. The hardware in the loop will be a cyber-physical system to simulate secondary coolant flow, steam generation, and turbine revolution. This will represent a scaled nuclear power plant and the first phase of an experimental balance of plant test bed. Figs. 1 and 2 show WSC and a schematic of the balance of plant.

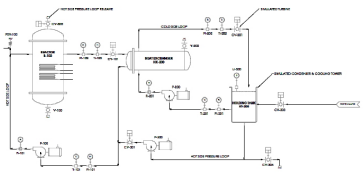


Fig. 2. Balance of plant.

Key features. The hardware will heat and cool water using a heater and heat exchanger, to simulate steam generation for representing scaled turbine revolution. No electricity will be generated. Steady turbine revolution will represent generation. A pump will drive the secondary cooling loop. Water will be transported through a flow loop to a steam generator that will spin a turbine at a nominal revolution to simulate electricity generation. Reactor 'operation' will be defined as maintaining constant turbine revolution based on operational parameters processed from WSC or simulated in a standalone mode. A human-machine interface; i.e., programmable logic controllers used in domestic nuclear plants will be used for balance of plant controls, excluding reactor operation. Sensors will monitor relevant plant operational

parameters; e.g., temperature, flow, angular momentum, etc. A 'data historian' will process operational data from WSC and serve as the interface with the hardware in the loop.

Research Objective. One of the primary objectives of this project is to develop several hardware-in-the-loop cyber-physical systems for interface with the *Western Services Corporation Simulator (WSC)* and other simulators and virtual IT environments to -

(1) Assess vulnerabilities of advanced nuclear power plant controls,

(2) Devise mitigation strategies to enhance *resiliency*, and

(3) Establish an experimental platform into interdisciplinary University curricula.

Action items.

Task I. Construction & implementation (*Full team*)
- Construct the balance of plant infrastructure and test system.

Task II. Vulnerability assessment to cyberattack (*Lead - Haney; Support - Borrelli*)
- Model past cyberattacks at nuclear power plants.

Task III. Measured plant data validity (*Lead - Borrelli; Support - Roberson*)
- Determine data quality for normal operations compared to cyberattack.

Task IV. Industrial automation algorithm & controls development (*Lead - Roberson; Support - Borrelli*)
- Development of diagnostics for cyberattack indication.

Task V. Advanced digital controls and HMI (*Lead - Roberson; Support - Borrelli*)
- Modify PLCs for data delivery under cyberattack.

Task VI. Enhanced situational awareness (*Full team*)
- Test balance of plant performance.

Task VII. Incorporation into curriculum (*Full team*)
- Develop laboratory exercises for relevant courses.

Funding. (*Full team*)

Task I. DOE-NEUP.	*February.*
Task II. DOE-CESER.	*Availability of funding.*
Task III. NSF-CPS.	*Rolling.*
Task IV. NSF-SaTC.	*Rolling.*
Task V. DHS-NCAE-CD.	*Rolling.*
Task VI. NSF-EPSCoR.	*Rolling.*
Task VII. DoD-DEPSCoR.	*Availability of funding.*

Recruitment. (*Full team*) Recruiting will largely commence after the Equipment Acquisition and overlapping with Planning. Faculty have regular recruiting activities over the academic year, into which this grant activity will be incorporated accordingly.

Task I. Montana Technological University Career Fair.	*September.*
Task II. Utah State University Graduate School Fair.	*September.*
Task III. American Nuclear Society Student Conference Career Fair.	*Spring.*
Task IV. UIIF Graduate Visit Day.	*Spring.*
Task V. BYU-Idaho Career Fair.	*Spring; Fall.*

5. Potential economic impact. Nearly every aspect of the Idaho economy, and nearly all of the foundational systems that underpin modern civilization, depend on the security of cyberspace and cyber-physical systems. These systems are under constant reconnaissance and threat of attack. Idaho's economy across all sectors is in immediate need of a larger and better prepared cybersecurity workforce [10, 11]. Idaho's research universities are uniquely positioned to work on the most advanced challenges in cyber-physical systems security and train the next generation of skilled workers to overcome these challenges. By building unique capabilities in Idaho Falls that can be accessed from other classrooms and laboratories across the state, this project will have direct and immediate positive impact on both the local and regional economy, statewide public and private sector organizations, and national security. Our immersive and highly realistic environment will not only serve to attract Idaho's students into the field of cyber-physical systems security and other STEM fields of post-secondary study; it will also fill a gap in training environments between the more commonly available virtual platform environments that provide 'hands-on' cybersecurity experience with small scale virtual desktops, and the full-open firehose learning experience of 'on-the-job training' that most current employees in the cybersecurity field have relied upon [12–14]. This project will not only increase our capacity at UIIF to recruit and graduate more students for the workforce, those students will be more effectively trained and better prepared to be effective on the job on day one, a fact which will multiply the impact on Idaho's economy [15]. Currently, there are an estimated 3,000 unfilled cybersecurity-related jobs in the state of Idaho alone. Best estimates of unfilled jobs in this field nationally are in the low millions and growing. With this grant, we will be able to quadruple our capacity to serve students in Idaho Falls, and provide a unique capability for educating students across all of the Idaho public institutes of higher education. Cybercrime, especially ransomware attacks, are a perpetual risk and economic burden across all sectors. Run of the mill cybercrimes are a constant drain on our state's economy. Ransomware attacks are increasing in frequency and intensity at an alarming rate. Acts of cyberterror and cyberwar are a more likely event than ever before. Attacks like those against Colonial Pipeline or JBS meat processing company could happen to any of Idaho's businesses or state agencies.

Idaho is currently working across the state to increase overall capacity and improve our programs in cybersecurity research, education, and workforce development. The team of experts assembled for this project are prepared to add a capability to the state like no other currently available nationwide. This capability will play a significant role in helping achieve the Presidents' Leadership Council vision of providing the premier education system for cyber-physical systems security. The strength and size of that education system will contribute to attracting students, businesses, federal government agencies, and contracts to the state. We are confident that RADICL in Idaho Falls will be a major differentiator in this larger statewide effort.

Additionally, this project has large potential to commercialize several technology service offerings and components. The concept of Adversary-as-a-Service is a novel one that will likely prove valuable in a number of industries and sectors as a training and skills assessment aid. Our design plans will allow the highly complex "internet in a box" concept to be replicated in other training and research environments. As the technology is matured and organized, the research team will work with technology transfer experts from each of our universities to establish a commercialization plan.

6. Criteria for measuring success. Our objective is to train cybersecurity professionals via scenario-based live-fire exercises. Our objective in education and workforce development is to increase our capacity for multiple cohorts of students on the Idaho Falls campus to work with these environments. Metrics for success are -

(1) Increased enrollments and graduates on the Idaho Falls campus from both the UI and ISU various cybersecurity degree and certificate programs. Our goal is to increase the Idaho Falls cybersecurity-

related programs of both UI and ISU to their physical seating capacity. With classroom space for 16 students and running multiple student cohorts concurrently, we anticipate growing to annually graduating 64 students through a 2-year program (e.g. an associate's degrees junior and senior years of a bachelor's degree, or a master's degree). We expect this effort will have measurable impact on the number of unfilled cybersecurity jobs in the region even during the life of this funding. Programs similar to this have shown a near 100% job placement success rate for graduates, and we expect our rates to be the same.

(2) Number of participating students across the other 8 campuses connected to the Idaho Cyber Range, although potential capacity is difficult to predict currently.

(3) Number of high school students we reach via tours, demonstrations, camps, and competitions that will be made possible through this effort. Previous summer camps hosted in this space in Idaho Falls have reached over 200 participants in the first 5 years. Through our enhanced systems, immersive scenarios, and remote access capabilities, and by organizing efforts to reach out to clubs and classes across the region, we expect the number of students reached and recruited to grow tenfold during the course of this funding.

(4) Collaboration through the number of trainees from industry partners that align with us for scenario-based training exercises and work with us to design realistic environments and scenarios. Development of surveys and tests to show learning outcomes and effectiveness of training will show the proficiency of our graduates.

(5) Existing alumni tracking processes at ISU and UI will be used to track the level of success of students who are integrated into the workforce.

(6) We will leverage this consequential development of much needed capabilities to seek new sustained funding from multiple federal sources for both cybersecurity research and workforce development. Through seeding these capabilities, the collective UIIF team, as well as the broader collaborative Idaho state system of schools will be much more competitive for federal grants. By creating a resource for cyber-physical systems security learning content, platforms, and experiences that can be leveraged across the state, we will provide fuel to empower our statewide cybersecurity efforts and lead to successes in building expertise and creating novel technologies that strengthen Idaho's future.

7. Budget. We are requesting $2,099,700 over three years. Please see attached budget sheets that accompany this full proposal.

8. Budget justification.

A. Personnel Costs. During each academic year Dr. Michael Haney will contribute 6% of his time or approximately 93.6 hours to the project. Co-PI's Dr. R. A. Borrelli, Dr. Dakota Roberson, and Dr. Konstantinos Kolias will contribute 2% of their time each academic year, or approximately 31.2 hours. During each summer of the project the PI and Co-PI's will work 80 hours on the project. We have included a 3% increase in faculty salaries each academic year. Pay rate is based on current yearly salary as determined by the academic contract between the University of Idaho and the employee. Faculty fringe benefits are based on the negotiated Consolidated Fringe Rate (CFR) for faculty of 29.40%. These rates are effective July 1, 2021 and can be found at https://www.uidaho.edu/finance/budget-office/fringe-benefits. One Post-Doctoral Fellow will be hired to work full-time in the second and third years of the project and will be paid according to the University of Idaho's guidelines regarding Post-Doctoral Fellowships. We've included a 3% increase

in salary between the second and third years of the project. Post-Doctoral fringe benefits are based on the negotiated Consolidated Fringe Rate for staff of 40.80%. These rates are effective July 1, 2021 and can be found at https://www.uidaho.edu/finance/budget-office/fringe-benefits. Two M.S. students will work 780 hours during the academic year and 560 hours in the summer during each year of the project. M.S. students at the University of Idaho – Idaho Falls campus are paid an hourly rate of $20.41 per hour. Student fringe benefits are based on the negotiated Consolidated Fringe Rate (CFR) for students of 3%. These rates are effective July 1, 2021 and can be found at https://www.uidaho.edu/finance/budget-office/fringe-benefits.

B. Equipment. The major focus of the efforts being proposed is the assemblage of research and training equipment on the University Place campus to create a complex of rooms conducive to adversarial-based cybersecurity education and training that is both project oriented and research driven. The approach to assembling this equipment and deploying it to these rooms is in appropriate phases and coordinated between the University of Idaho and the Idaho State University team. The latter is proposing the learner-facing work areas in the industrial zoned room, our electronics and cyber-physical systems laboratory classroom (see Facilities in the appendix to this proposal for an explanation of zones and rooms). The equipment and materials in the sub-award section of this proposal are essential to achieving the goals of this proposed effort. In this section, we describe the equipment proposed by the University of Idaho team which includes the mid-scale research-oriented cyber-physical equipment in the industrial zone, the enterprise IT zones running on private cloud hardware and student-facing computer workstations, and the replicated Internet and adversarial environments.

(1) Research-oriented Cyber-Physical Equipment: $275,000

   (a) Year one: Nuclear Balance of Plan system - $75k
   (b) Year two: Electrical grid with distributed generation and RTDS - $100k
   (c) Year three: Water, Agriculture, and Transportation systems – $100k

In the first year of this project, we propose beginning by building on the capacity we have created on the Idaho Falls campus in nuclear power plant simulations. The first mid-scale cyber-physical system we propose acquiring is a cooling tank and pump system that represents operations of the Balance of Plant systems of a nuclear power plant. This closed loop system will consist of several tanks, pumps, valves, and pipes, and the operation of it will be controlled by a handful of Programmable Logic Controllers (PLCs) and a Human-Machine Interface, as well as networking and data collection components. This equipment system design and specification has been available to the research team for some time and a detailed plan for its installation and integration with our existing nuclear reactor simulators is ready for execution. This equipment will provide the researchers and our students and industry partners with a sophisticated platform to conduct a number of cybersecurity experiments. It will further support a number of configurations and playbooks in our adversary-based cybersecurity training exercises. And importantly, this equipment will seed ongoing research and future funding efforts in this space.

In the second year of this project, we will expand our mid-scale CPS equipment with electric grid sector systems. With the emergence of a bi-directional grid, utilities will need enhanced reliability, security and edge analytics to incorporate distributed renewable resources at scale. Thus, utility infrastructure modernization will require a vast array of internet-of-things devices (IOT) to collect data to be aggregated at the substation level for deep insight into grid operation at distribution level voltages which utilities currently cannot assess. Virtualized substations (i.e., software-defined automation and control systems) will be used to aggregate and synthesize this data to paint a comprehensive picture for grid operators of the status of the system and help them respond to more rapidly changing market signals based on changing demand, weather and overall grid health. Therefore, the equipment needed to virtualize a substation will provide a

unique opportunity to advance the state-of-the-art in the area of grid automation to enable secure and reliable operations with high levels of renewable resources. Specifically, a real-time digital simulator (RTDS) coupled with a micro data center for a substation using a rugged IEC61850-capable VPR server will be used to implement the virtual machines, hypervisor, virtual protection relays, and virtual networks. Students will use this system as we work to develop new intelligent edge control systems for asset optimization, vision base monitoring, and distributed energy resource management. Using a protection relay to turn lights on and off to signify an unintended trip off of a feeder on the distribution system will provide an excellent visual representation of a CPS which can be manipulated.

In the third year, we propose to assess lessons learned during the first two years, as well as insights brought to the team by our postdoctoral researchers and industry partners. We will propose a design and system specification to create a mid-scale system for the agriculture sector and address a cyber-physical system in the food, energy, water nexus. One such system under consideration is a network of irrigation canals and pumps operated as a micro-grid. We again budget $100,000 for this system in year three.

Each of these closed loop systems that will be incorporated into our complex will serve as seeds for ongoing research by the co-PIs in their respective fields and specialization areas. Further, this baseline equipment will serve the special purpose of fostering the transfer of knowledge from research laboratory to classroom to training environment. This equipment will be designed to be targeted, instrumented to measure the effects of cybersecurity attacks, and recorded to replay attack scenarios for training equipment operators and other defenders.

(2) Small-scale Reconfigurable Cyber-Physical Systems: $50,000

The second category of equipment consists of a variety of small-scale cyber-physical systems that represent more general concepts and may not be industry sector-specific. This category of equipment will allow us to create a "shooting gallery" of systems that present targets in cyberspace for students and researchers to explore dynamic cybersecurity issues such as reconnaissance, targeting, profiling, assessing, exploiting, and controlling remote cyber-physical systems. These various components will be installed throughout the two rooms and serve as a reconfigurable set of potential targets for attack and defense activities. Similar to a shooting gallery at a carnival or state fair, systems can exist on an isolated network that allows players/learners to scan the network, acquire and prioritize targets, assess vulnerabilities and exploit weaknesses to compromise the system. Compromise may consist of "capturing the flag" and identifying a unique code on the target, which triggers the physical device in some way (e.g. lighting a panel, changing the image on a screen, sounding a bell or alarm or playing a song, moving an object such as raising or lowering a flag). Devices may simulate simplified systems or sub-systems with clear goals and learning objectives for each, with an easy means of resetting the target after a student has acquired it. Examples of possible solutions we wish to incorporate can be found from suppliers of Escape Rooms that are growing in popularity across the country [16]. Locks can be timed or digitally controlled to open cabinet doors or drawers, or reveal new clues as learners progress through the network. Each station should also include a camera so that students, researchers, and trainees can watch the physical device get triggered and reset, even at a distance, whether in the next room on our campus, or in a classroom or remote connection from across the state.

There are many possibilities for specific gadgets to incorporate in our cyber-physical systems shooting gallery, and the co-PIs have enjoyed brainstorming. A typical gadget will consist of a small-scale Raspberry Pi computing kit and a control board, several relays and electronic accessories, a small display screen, a mounting board, a wireless keyboard and mouse to program for setup and reconfiguration, and a selection of actuators and sensors that can light bulbs or move items or armature with small motors. Each gadget should be constructed for an average of $1000, and we plan to incorporate 30 such gadgets in the first year, with additional funding in subsequent years to adapt, improve, and expand the offering.

(3) Classroom equipment: $96,000 (8 stations, $4k each, 3 years to 24 stations).

In order to enable the corporate IT activities and security operations, as well as attacking "red team" activities, we require to outfit our classrooms with up-to-date computer workstations in our enterprise zone space. Note, this equipment is separate from the ISU sub-award that is outfitting the cyber-physical systems laboratory-classroom. This student equipment will outfit the enterprise zone laboratory-classroom in CHE 104. We are budgeting $4,000 per workstation, including dual monitors, peripherals, and sufficient capacity to operate multiple virtual machines simultaneously. We propose acquiring 8 workstations in the first year, and 8 additional workstations in each subsequent year, totaling 24 at a cost of $96,000.

(4) Private Cloud Computing Equipment: $300,000 ($150k first year, $75k each new year.)

We are proposing creating a resource available to students on our campus and across the state via private network connections. The resource we are creating will require significant computing capacity for a large scale deployment of enterprise-grade IT systems as well as the simulated activity of major Internet service providers and nation-state actors. This requires us to build and maintain private cloud computing capabilities on our closed and isolated network. Recently, our facilities have been renovated to expand capacity for power, cooling, and access control to support a significant on-premise computing environment. With this grant, we will be able to equip our new student server room and provide this much needed capacity. In the initial year of this project, we will require the purchase of two mid-scale computing clusters which we estimate at $75,000 each. Scale will matter most as we make this cloud-based environment accessible across the Idaho Cyber Range, interacting with assets in Pocatello and Moscow, with multiple lab environments also potentially accessible from across the state. Via the closed-loop airlocked network system of the RADICL-IF and ICR, we can provide "Adversary-as-a-Service" in a private Internet simulation, with a library of playbooks and configuration scenarios to choose from. This environment will run in several clusters and will support a robust virtualization platform for a large number of reconfigurable computing systems that would be applicable to a number of sectors and industries. One cluster will be dedicated to the simulated Internet systems where we will be able to provide google.com, facebook.com, etc, as well as ransomware command-and-control servers, and foreign adversary IP ranges to be used by the red team during training exercises and research experiments. The capacity of these servers in the first year will provide the baseline for creating the framework of immersive environments and playbooks. As we expand our offerings and tie into additional physical and cyber-physical system components, we will add additional computing capacity in the second and third years at $75,000 per year.

C. Travel: None.

D. Participant Support Costs: None

E. Other Direct Costs.

(1) Materials and Supplies: $56,000.

Construction materials and miscellaneous hardware expenses to appropriately address the equipment needs in the physical space, such as door locks and badge readers, mounting platforms for physical equipment, modification to hang items on the walls, etc. Given our estimates of mounting hardware for each unit to be $200 x25 units = $5000, badge readers to be installed at $3000 per door x5 doors, cabling, and contractor fees for running cables between all three rooms at $5000, wall repairs, and painting. We are proposing $20,000 to cover costs in the first year, with an additional $20,000 in the second year and $16,000 in the third year for these materials and supplies. Total is $56,000.

(2) Publication Costs/Page Charges: $2200

Costs related to publishing for each conference, based on the ANS transactions rate of $400 per publication

per conference. These rates can be found here: http://www.ans.org/meetings/c_1.

(3) Consultant Services: None

(4) Computer Services: None

(5) Subcontract with Idaho State University: $900,000

(6) Other: $5,000

We are requesting an additional $5,000 to cover the costs of searching for postdoctoral research fellows.

(7) Tuition, Mandatory Fees, and Student Health Insurance Plan: $55,620.60

Academic year tuition, fees, and student health insurance for one graduate student is $13,566 and is based on current student in-state full-time graduate student fees for the 2020-2021 academic year. The University of Idaho waives out-of-state fees for graduate research assistants (GRAs). A 5% increase has been included for the second year as outlined in the University's strategic plan.

F. Total University Project Costs. $2,099,700 This includes a total of all direct costs related to the project.

G. Amount Requested. $2,099,700

9. Project management. A GANTT chart is shown in Tab. 1 below. It covers overall Project Phases and Workscopes. We expect significant overlap and collaboration amongst Investigators.

Table 1. Timeframe for Execution of Proposed Project.

Activity	Y1				Y2				Y3			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Equipment acquisition	X	X	X									
Planning		X	X	X								
Scenarios			X	X	X							
Wargames					X	X	X	X	X	X	X	
Hardware in the loop			X	X	X	X	X	X	X	X		
Funding	X	X	X	X	X	X	X	X	X	X	X	X
Recruitment						X		X		X		X
Crosscutting issues											X	X

10. Additional institutional and other sector support. For over a decade, RADICL on the UI main campus in Moscow has developed methods of managing virtual machine technologies for cybersecurity education. Similarly, the NIATEC program on the ISU Pocatello main campus has maintained a number of IT systems for education and research, and has more recently deployed many industrial cyber-physical systems for training in the ESTEC program. Funding these efforts over the years demonstrates institutional commitment and leadership in this space. Further commitment can be seen in this assembly of faculty researchers all relatively new to eastern Idaho. Over 2000 square feet of space in three adjacent rooms has now been dedicated to cybersecurity efforts training and education in Idaho Falls. Efforts to date to equip this space have been supported by limited funding and benefited greatly by repurposed surplus equipment. Most significantly the two institutions combined funds from the Idaho Cybersecurity Education Initiative to invest in a student computer server room. This room will support our local private cloud environment, hosting the systems for enterprise IT networks and simulated employee activity running on new servers to be acquired through this grant. The middle room offers space divided for instruction and wargaming

with dedicated spaces for attack and defense teams and a sophisticated multi-tiered network management system uniquely designed to sandbox and control simulated Internet traffic and cyber-attacks. This room also has video teleconference capabilities made possible by previous IGEM support. The third room houses an electronics laboratory-classroom which has seen new life in recent semesters. This grant would provide for deployment of cyber-physical systems in this room for display, demonstration, attack and defend work. By interconnecting all three rooms, we will build a series of complex simulated enterprise and industrial environments. This will provide a solid foundation for research focused on a number of challenges in industrial control systems and the Internet of Things. Bench-scale process control systems are necessary to explore solutions to these challenges, and the research will benefit greatly from the high-fidelity simulated attack environment we will also provide. Future researchers will also benefit from the attack datasets we collect and make available, a very scarce resource. Each process system will be designed to directly support and enable research of one or more of the co-PIs in various sectors.

Combined, our 'shooting gallery' of equipment will allow for incorporating the adversarial behavior element in further systems defense research. The products of this project will support collaboration and partnerships in a number of domains current and in the future. We continue to discuss these efforts with a number of utilities and businesses in our region, and many have expressed strong support for such a simulated environment that can be reconfigured to mimic their own. Letters of support will be obtained from a number of these partners. Our workspace is now primed to develop this next level of capacity and will be immediately available to the rest of the state via the Idaho Cyber Range, made possible by our strong IRON partnership. Finally, The Presidents' Leadership Council has expressed their prioritization and strong support for cybersecurity education and research across the state, and this effort will go a long way towards achieving their vision.

11. Future funding. Funding programs at the federal level specifically to support cybersecurity or cyber-physical systems research and workforce development include two National Science Foundation (NSF) multi-directorate programs: Secure and Trustworthy Cyberspace and Cyber-Physical Systems. Funding ranges from several hundred thousand to several million dollar grants. These grant programs are designed to support the advanced work this project would enable. The Department of Energy sponsors research and development grants through the Office of Cybersecurity, Energy Security, and Emergency Response (CESER). These goals closely align with this group's interests and current efforts. The Department of Energy (DOE) also sponsors academic institutions through the Nuclear Energy University Program (NEUP). In most recent years Nuclear Energy University Program (NEUP) included a call for proposals for cybersecurity and digital instrumentation for the nuclear sector. The National Centers of Academic Excellence in Cyber Defense (NCAE-CD) program has enabled funding from Department of Homeland Security (DHS) and other agencies to be managed by the 'CAE Community' of which both ISU and UI are members, making us eligible to compete for these funds. Funding calls are often for expansion or enhancement of existing programs. Both UI and ISU maintain Cybercorps Scholarship for Service programs primarily on their main campuses, but with both programs represented by co-PIs to this proposal. Additionally, Idaho is an Established Program to Stimulate Competitive Research (EPSCoR) State. NSF provides additional funding opportunities through this program across Directorates in order to disperse federal funds more equitably nationwide. Neighboring EPSCoR States include Wyoming, Montana, Nevada, and New Mexico offering expansive collaborative opportunities going forward from this grant. Similarly, there is the Defense Established Program to Stimulate Competitive Research (DEPSCoR) initiative, which is directed for Department of Defense (DoD) interests. By expanding capacity and support in Idaho Falls, we will pursue expansion of these multi-million dollar funding sources for student support, bringing more students to the Idaho Falls campus.

Appendix A: Facilities and Equipment

Summary If awarded, this proposal will be carried out at the facilities in the University Place campus in Idaho Falls, Idaho, which are jointly operated by the University of Idaho and Idaho State University. A research library, access to student commons, and a substantial supporting staff consisting of technical writers, financial coordinators, and accountants provide supporting infrastructure to facilitate innovative and cutting-edge research. This grant proposal would fund the coordination and inter-connection of three adjacent rooms in the Center for Higher Education (CHE) building. The first of these rooms is the existing RADICL laboratory-classroom, described below. The room adjacent and to the north has previously been an electronics laboratory and we propose creating the Cyber-Human-Physical Systems (CHiPS) laboratory-classroom. The room adjacent and to the south of RADICL has recently been renovated as a computer server room through funding provided by the Idaho Cybersecurity Education Initiative. Each of these spaces is described in more detail below. Together, through this funding, these rooms will form a cybersecurity research, education, and training complex that offers multiple scales of hybrid virtual and real cyber-physical systems and Adversary-as-a-Service offerings.

Research centers, laboratories, and physical facilities

Reconfigurable Attack-Defend Instructional Computing Laboratory. The Reconfigurable Attack -Defend Instructional Computing Laboratory (RADICL) is located at the Idaho Falls Center and is the hub for cybersecurity under the direction of Prof. Haney. 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 the National Science Foundation (NSF Award 0416757). Since its inception, 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.

In 2017, RADICL expansion to the Idaho Falls Center (RADICL-IF) was initiated. RADICL-IF is a 900 square-foot classroom that has been equipped with a dedicated power transformer and distribution subpanel, as well as a networking cabinet, to provide power distribution and Ethernet capabilities throughout the room. The physical construction and layout of this room is designed to foster group work and peer instruction, as well as to facilitate the wargames, with a wide variety of equipment on ample workspace for 16 students. The classroom has been divided into two areas, the front area for lecture-oriented instruction, and the back area for interactive activities including adversarial wargames. This classroom will be equipped through this grant with up-to-date workstations and IT infrastructure and services designed for supporting attack and defend exercises. Through previous funding efforts, this room has been equipped with classroom video-conferencing equipment and live instruction can be telecast into or out of this classroom.

RADICL enables teams of students and researchers to create and deploy multiple independent experiments that are quick to set up and modify. Within the context of these isolated experiments, students and researchers are able to design, implement, examine, explore, and develop a detail-oriented and hands-on view of modern computing infrastructures, along with their associated applications and protocols, and their strengths, weaknesses, and vulnerabilities. In addition, in RADICL, students and researchers are able to develop a clear, detail-oriented, and experiential understanding of the approaches, techniques, and tools used to protect todays computing systems and applications. RADICL is designed as a state-of-the-art computing laboratory that enables hands-on and student oriented instruction integrated with graduate and undergradu-

ate research. However, currently all computing hardware available in this facility has been acquired through surplus acquisition from UI and ISU and is beyond end-of-life.

CHE Room 106. The room adjacent to the south of RADICL-IF was recently renovated to create a student-accessible datacenter. Through funds made available by the Idaho Cybersecurity Education Initiative and with cooperation of ISU and UI, this 15x30 room was divided to create storage and workspace in the front, with a new wall and door to provide environment isolation and access control for the back of the room. This space has been modified to expand power and cooling to support a significant computing platform installation. We are proposing the purchase of equipment which will be installed and operated in this new space.

Cyber-Human-Physical Systems Laboroatory. The room adjacent to the north of RADICL-IF (CHE 104) is another 30x30 classroom-laboratory that has previously been used as an electronics laboratory and most recently as a storage facility. Through this grant, we will make use of the available space and bring it new life as the Cyber-Human-Physical Systems (CHiPS) Laboratory. As this campus is shared and jointly operated by UI and ISU, both classroom-laboratories will be available for courses taught through each university. Discussions with the Idaho State Board of Education about jointly-listed courses, adjunct faculty, and means of sharing resources to effectively reach more students are ongoing. Leadership from both universities have agreed to share the classrooms in question for the purpose of cybersecurity education.

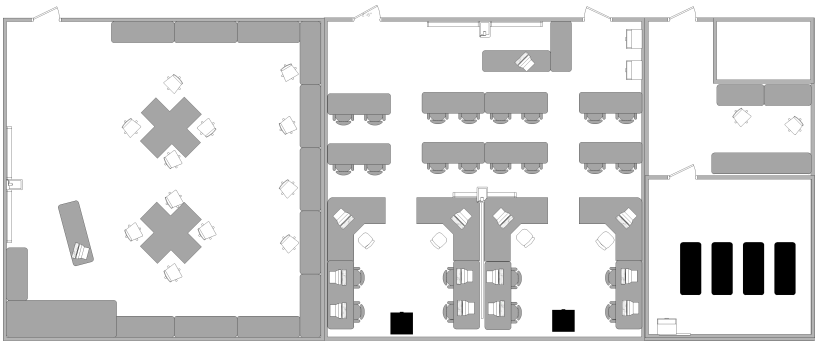


Fig. 3. Cybersecurity Room Complex

Significant infrastructure is already in place in CHE 101, including ample storage cabinets, a large workbench and wall space for the research equipment proposed here, and raised electronics workbenches for 8 students with sufficient electric power and project storage. This allows for easy adaptation for the cyber-physical systems work described in this proposal to take place.

Through previous IGEM grant support, state-of-the-art videoconferencing equipment has been procured to support inter-campus live and hands-on instruction efforts. This videoconferencing equipment has supported the delivery of courses to and from Idaho Falls to the campuses in Moscow and Coeur d'Alene, as well as ISU courses taught with extension to the Pocatello campus. This proposal seeks the funding to transform this space into a state-of-the-art cybersecurity research and training complex supporting a large variety of activities that will be available to learners throughout the state.

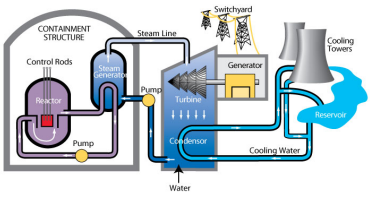


Fig. 4. Nuclear Power Plan Simulator

Western Services Corporation Plant Simulator. Western Services Corporation (WSC) is headquartered in Frederick, Maryland and was founded in 1996. Currently, WSC employs 85 people. Nuclear power plant simulators are 40% of its main business. Plant simulators can be used for I&C modeling, thermal hydraulics, electrical generation and distribution systems, human factors, logic and control system testing, and plant optimization. Nuclear plant simulators are installed in about 20 locations worldwide, including the Palo Verde Generating Station. Profs. Borrelli and Haney obtained the pressurized water reactor simulator for CAES. It based on a two loop design for use in this project. The simulator includes over 75 graphic control screens, with 10,000 supervised points.

A full-featured trending system can monitor multiple operational transients. An 'Instructor Station' allows for introducing hundreds of malfunctions during operation. The developers license allows for development of cybersecurity incidents into an Instructor Station which will serve as a test bed to this project. The plant simulator is housed in the Applied Visualization Laboratory at CAES. Profs. Borrelli and Haney have assembled a multi-mode hybrid high performance computing platform to provide a computational infrastructure to support simulator operations. This platform will be used as a central component in our research complex and coupled initially with the Nuclear Balance of Plant analogue equipment.

The Idaho Cyber Range. With project management and leadership from Professor Haney, the last two years have seen unprecedented cooperation among the eight public institutes of higher education in Idaho in the area of cybersecurity education. The most visible result of that collaborative effort is the create of the Idaho Cyber Range. The Idaho Cyber Range is an inter-connected private network of cybersecurity education and research facilities on each of the state's public campuses. Operated by the Idaho Regional Optical Network, facilities across the state can be interconnected at gigabit speeds. Each site (laboratory or classroom) can operate autonomously and can connect to share data sources, virtual machines, system configuration, and cybersecurity attack-defend playbooks. Each of the state's community colleges has created a training Security Operations Center for students to work with large-scale datasets such as logs and security alerts, practicing detection and response techniques. This proposal seeks to equip the Idaho Falls location in a way to provide Adversary-as-a-Service, which will be accessed across the state using the Idaho Cyber Range.

General University Resources

National Center for Academic Excellence in Information Assurance/Cybersecurity Education. The University of Idaho 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) now (CAE/CDE). The first designation was in 1999 and later successfully renewed in 2005, 2008, and 2014. The current designation certificate expires in 2022 and our renewal application has been filed.

University of Idaho. The University of Idaho 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 bachelors, 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. The centers and computing facilities to education and research are described below. The University Information Technology Services maintains 22 computer laboratories dedicated to academic use.

College of Engineering. The College of Engineering is composed of 6 academic departments and 5 research and development centers. The college has about 200 faculty and staff and a student body of 1500 undergraduate students and 350 graduate students. The College of Engineering has several full-time dedicated Information Technology personnel and one full-time Information Technology 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 Idaho Falls Center has a full-time dedicated systems administrator working to ensure the availability of teaching computing infrastructure and systems in coordination with the main Moscow campus.

University of Idaho Library. The University of Idaho library houses over one 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 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.

College of Eastern Idaho. The University of Idaho shares Robotics and Manufacturing Laboratories with the College of Eastern Idaho, which houses 3D printers, Robots, Laser Engraver, as well as other machines for manufacturing. Further details about the campus facilities are provided at http://www.cei.edu/.

Idaho National Laboratory Prof. Haney is jointly appointed to Idaho National Laboratory and thus has access to INL facilities external to CAES. Both Profs. Haney and Borrelli have badge access to the Idaho Falls campus of the laboratory. Idaho National Laboratory if part of the United States Department of Energy complex of national laboratories. Idaho National Laboratory serves as a multi-program laboratory with competencies in energy and national security, as well as high performance computing applications. Further information is provided at https://inl.gov/.

Center for Advanced Energy Studies CAES houses the University Investigators and the NuScale Simulator. It is a 55,000 square foot LEED Gold Certified research and teaching facility made up of the previously identified consortium of four universities and national laboratory. CAES is a collaborative environment which serves to cultivate world class interdisciplinary research in energy systems. Faculty, students, and staff from all of the affiliate members have office and work space at CAES, allowing each availability to resources that the individual institutions do not have access to otherwise. Workspace will be made available at CAES for personnel funded for this project.There are no parking or additional security restrictions to access the facility.

CAES has an auditorium, gallery, and two meeting rooms with videoconferencing capabilities with professional support staff and technicians. Use of space at CAES is provided to member affiliates at no cost. Researchers at CAES have access to servers on the High Performance Computing environment hosted by Idaho National Laboratory at no additional cost.

CAES offers eight laboratories, four of which can handle radioactive materials, a three dimensional, computer assisted virtual reality environment (CAVE), and microscopy and characterization suite (MaCS).The CAES website provides details regarding the available resources, facilities, and each laboratory at - https://caesenergy.org/.

CAES has a host of instruments and various laboratories and computing facilities as part of its public/private collaborative mission. Laboratories include -

- Advanced Materials Laboratory,
- Radiochemistry Laboratory,
- Analytical Chemistry Laboratory,
- Analytical Instrumentation Laboratory,
- Geothermal Fluids Laboratory,
- Microscopy and Characterization Suite,
- Advanced Transportation Laboratory, and
- Computer Assisted Virtual Environment in the Applied Visualization Laboratory.

Six other groups are affiliated with CAES, providing expertise and equipment in specialized research areas. These are -

- Energy Policy Institute (EPI),
- Nuclear Science User Facilities (NSUF),

- Energy Systems Technology and Education Center (ESTEC),
- Autonomous Systems Center of Excellence (ASCE),
- Center for Space Nuclear Research (CSNR), and
- CAES Energy Efficiency Research Institute (CEERI).

These facilities and resources available to researchers and students at the Idaho Falls Center bolster the capabilities of the project team to successfully complete the proposed research project. University of Idaho NuScale Power, LLC, Plant Simulator. The NuScale Simulator is currently under installation at CAES to be completed in Spring 2021. The Simulator uses NuScale proprietary code NRELAP5 to simulate thermal-hydraulic phenomena and Studsvik S3K for the core physics model. It provides real-time operation and includes models for representing protection and control systems for a 12-module NuScale power plant. The Simulator was awarded to the University of Idaho through a Department of Energy Infrastructure Grant. It can be used for a wide variety of research pathways, including innovative operations methods, flexible operation, cybersecurity, and hybrid energy systems analysis. The Simulator offers extensive data collection capabilities.

Personnel resources Project funding will be largely invested in one Postdoctoral Fellow and six graduate students. The Investigators have designated responsibilities for the defined research Tasks, and their time has been allocated accordingly to achieve project goals. Appropriate allocation of funds and related expenses therein will be supervised by the Principal Investigator with support from the designated Financial Coordinator, who will be located at the Idaho Falls Center. The Systems Administrator at the Idaho Falls Center is responsible for maintaining computing equipment and services.

Appendix B: Biographical Sketches

NAME: Michael Haney

POSITION TITLE & INSTITUTION: Assistant Professor - University of Idaho

A. PROFESSIONAL PREPARATION
(see PAPPG Chapter II.C.2.f.(i)(a))

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE (if applicable)	YEAR (YYYY)
University of Tulsa	Tulsa, OK	Computer Science	Ph.D.	2015
University of Tulsa	Tulsa, OK	Computer Science	M.S.	2013
University of Kentucky	Lexington, KY	Mathematics	B.S.	1998

B. APPOINTMENTS
(see PAPPG Chapter II.C.2.f.(i)(b))

From - To	Position Title, Organization and Location
2015 - Present	Assistant Professor, University of Idaho, Idaho Falls, ID Jointly-appointed: Idaho National Laboratory Center for Advanced Energy Studies (CAES) Center for Secure and Dependable Systems (CSDS) Affiliated Faculty, Nuclear Engineering Program, University of Idaho
2011 - 2015	Graduate Research Assistant, Institute for Information Security, The University of Tulsa, Tulsa, OK
2013 - 2015	Technology/Cybersecurity Consultant - Institutional Review Board, The University of Tulsa, Tulsa, OK
2011 - 2013	Senior Security Consultant, True Digital Security, Tulsa, OK
2008 - 2011	Senior Security Consultant, FishNet Security, Boston, MA
2002 - 2008	Manager (Consultant), Ernst & Young, LLP, Boston, MA
2001 - 2002	Senior Security Analyst, WilTel Communications (now L3), Tulsa, OK

C. PRODUCTS

(see PAPPG Chapter II.C.2.f.(i)(c))

Products Most Closely Related to the Proposed Project

1. Trevor MacLean, R.A. Borrelli, and Michael Haney, "Cyber Security Modeling of Non-Critical Nuclear Power Plant Digital Instrumentation", International Journal of Critical Infrastructure Protection XIII, Springer International Publishing, S. Shenoi and J. Staggs (eds), pp 87-100, Springer, 2019.
2. John Peterson, Michael Haney, and R.A. Borrelli, "An overview of the methodologies for cyber security vulnerability assessments conducted in nuclear power plants," Journal of Nuclear Engineering and Design, Vol 346, May 2019, 75-84. https://doi.org/10.1016/j.nucengdes.2019.02.025
3. Michael Haney, "Leveraging Cyber-Physical System Honeypots to Enhance Threat Intelligence," International Journal of Critical Infrastructure Protection XIII, S. Shenoi and J. Staggs (eds), pp 209-233, Springer, 2019.
4. Michael McGregor, Zach Lontz, Daniel Conte de Leon, and Michael Haney, "Network Air Locks, Not Air Gaps, to Preserve LAN Security," 23rd Colloquium for Information Systems Security Education (CISSE 2019) Las Vegas, NV, 10-12 June 2019.
5. Jillepalli, Ananth A. Daniel Conte de Leon, Ibukun A. Oyewumi, Jim Alves-Foss, Brian K. Johnson, Clinton L. Jeffery, Yacine Chakhchoukh, Michael A. Haney, and Frederick T. Sheldon. "Formalizing an Automated, Adversary-aware, Risk Assessment Process for Critical Infrastructure." Proceedings of the IEEE Texas Power and Energy Conference 2019 (IEEE-TPEC-2019), February 7-8, 2019, College Station, Texas, USA.

Other Significant Products, Whether or Not Related to the Proposed Project

6. Oliver, David and Michael Haney, "Preparing the Next Cyber-Resilient Workforce through Crosspollination Education" Resilience Week (RWS 2017), September, Wilmington, DE. IEEE, 2017.
7. Oliver, David, and Michael Haney, "Curriculum Development for Teaching Critical Infrastructure Protection", 21st Colloquium for Information Systems Security Education (CISSE 2017), Proceed of, 12-14 June, 2017, Las Vegas, NV.
8. Hiromoto, Robert E., Michael Haney, and Aleksander Vakanski, "A Secure Architecture for IoT with Supply Chain Risk Management," 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS17): Technology and Applications, 21-23 September, 2017, Bucharest, Romania, IEEE 2017.

D. SYNERGISTIC ACTIVITIES

(see PAPPG Chapter II.C.2.f.(i)(d))

1. Dr. Haney developed and established the Graduate Certificate of Critical Infrastructure Resilience at the University of Idaho, a cross-disciplinary certificate for graduate students in Computer Science, Technology Management, Electrical Engineering, Mechanical Engineering or Civil Engineering.
2. Collaboration between the Idaho National Laboratory and the University of Idaho has allowed Dr. Haney to provide cybersecurity expertise to an innovative interdisciplinary course on Grid Resilience.
3. Advisory Board Member for ISU/ESTEC Energy Systems Cyber-Physical Security Program
4. Advisory Board Member for BSides Idaho Falls Security Conference
5. Director of the Cybercore Summer Camps sponsored by the INL and College of Eastern Idaho.

NSF BIOGRAPHICAL SKETCH

NAME: Borrelli, R. A.

POSITION TITLE & INSTITUTION: Associate Professor, University of Idaho - Idaho Falls Center for Higher Education

(a) PROFESSIONAL PREPARATION -(see PAPPG Chapter II.C.2.f.(a))

INSTITUTION	LOCATION	MAJOR / AREA OF STUDY	DEGREE (if applicable)	YEAR YYYY
Worcester Polytechnic Institute	Worcester, MA	Mechanical/Nuclear Engineering	BS	1996
Worcester Polytechnic Institute	Worcester, MA	Civil/Environmental Engineering	MS	1999
University of California-Berkeley	Berkeley, CA	Nuclear Engineering	PHD	2006

(b) APPOINTMENTS -(see PAPPG Chapter II.C.2.f.(b))

2021 - present Associate Professor, University of Idaho - Idaho Falls Center for Higher Education, Department of Nuclear Engineering and Industrial Management, Idaho Falls, ID

2015 - 2021 Assistant Professor, University of Idaho - Idaho Falls Center for Higher Education, Department of Nuclear Engineering and Industrial Management, Idaho Falls, ID

2012 - 2015 Adjunct Professor, Diablo Valley Community College, Department of Architecture and Engineering , Pleasant Hill, CA

2009 - 2012 Postdoctorate Researcher, University of California-Berkeley, Department of Nuclear Engineering, Berkeley, CA

2007 - 2009 Research Associate, The University of Tokyo, Department of Nuclear Engineering/Management, Tokyo

(c) PRODUCTS -(see PAPPG Chapter II.C.2.f.(c))

Products Most Closely Related to the Proposed Project

1. Mena P, Borrelli RA., Kerby L. Nuclear reactor transient diagnostics using classification and AutoML. Nuclear Technology. 2021. DOI: 10.1080/00295450.2021.1905470
2. Borrelli RA, Delligatti M, Heidrich B. Borated aluminum cask design for onsite intermediate storage - Preliminary neutronics design and certification analysis. Nuclear Engineering and Design. 2020; 363. DOI: 10.1016/j.nucengdes.2020.110666
3. Lee J, Borrelli RA. Sensitivity analysis and application of advanced nuclear accounting methodologies on the high reliability safeguards model: Use of discrete event simulation for material throughput in fuel fabrication. Nuclear Engineering and Design. 2019; 345:183.
4. Carter J, Borrelli RA. Neutron physics study of an integral molten salt reactor using Monte Carlo N-Particle code. Nuclear Engineering and Design. 2020; 365. DOI: 10.1016/j.nucengdes.2020.110718
5. Peterson J, Haney M, Borrelli RA. An overview of methodologies for cyber security vulnerability assessments conducted in nuclear power plants. Nuclear Engineering and Design. 2019; 346:75.

Other Significant Products, Whether or Not Related to the Proposed Project

1. Tacke J, Borrelli R, Roberson D. Advanced frequency-domain compensator design for subsystems within a nuclear generating station. Progress in Nuclear Energy. 2021; 140. DOI: 10.1016/j.pnucene.2021.103914
2. Lee J, Shigrekar A, Borrelli RA. Hazard and operability analysis of a pyroprocessing facility. Nuclear Engineering and Design. 2019; 348:131.
3. Redfoot E, Borrelli RA. Analysis of nuclear renewable hybrid energy systems modeling and nuclear fuel cycle simulators. Nuclear Technology. 2018; 204:249.
4. Borrelli RA. A high reliability safeguards approach for safeguardability of remotely-handled nuclear facilities: 1. Functional components to system design. Journal of Nuclear Materials Management. 2014; XLII:4.
5. Borrelli RA. A high reliability safeguards approach for safeguardability of remotely-handled nuclear facilities: 2. A risk-informed approach for safeguards. Journal of Nuclear Materials Management. 2014; XLII:27.

(d) SYNERGISTIC ACTIVITIES -(see PAPPG Chapter II.C.2.f.(d))

1. American Nuclear Society: Executive Committee - Nuclear Nonproliferation Policy Division
2. University of Idaho: Faculty Advisor - American Nuclear Society University of Idaho Student Section
3. Idaho Section of the American Nuclear Society: Board of Directors; Coordinator - Smoke Detector Donation Program

Curriculum Vitae for Dakota Roberson, Ph.D.
Assistant Professor, Department of Electrical and Computer Engineering
Affiliate Faculty, Department of Nuclear Engineering
University of Idaho – Idaho Falls, Center for Advanced Energy Studies
995 MK Simpson Boulevard, Idaho Falls, ID 83401

EDUCATION

University of Wyoming – Ph.D., Electrical Engineering; Graduate Minor, Statistics; May 2017.
University of Wyoming – B.S., Electrical Engineering; Minor, Mathematics; May 2013.

APPOINTMENTS

- UNIVERSITY OF IDAHO – *Asst. Professor, Electrical & Computer Engineering,* 8/17 – Present.
- UNIVERSITY OF IDAHO – *Affiliate Faculty, Nuclear Engineering,* 5/19 – Present
- U.S. DEPARTMENT OF DEFENSE – *Defense Science Board Member,* 11/20 – Present.
- THE WHITE HOUSE – *White House Fellow, U.S. Department of Defense,* 8/19 – 8/20.
- SANDIA NATIONAL LABORATORIES – *Electric Power Systems Research Group,* 5/13 – 6/17.
- UNIVERSITY OF WYOMING – *Electric Motor Research Laboratory,* 5/11-5/12.
- DELCON SYSTEMS – *Photovoltaic Generator Design & Construction,* 5/10-5/11.

FIVE RELATED PUBLICATIONS

1. O'Brien J, **Roberson D**. "Synchrophasor spoofing detection and remediation for wide-area damping control." Electric Power Systems Research. 2021 October; 199:107445.
2. Tacke J, Borrelli R, **Roberson D**. "Advanced frequency-domain compensator design for subsystems within a nuclear generating station." Progress in Nuclear Energy. 2021 October; 140:103914
3. **Roberson D**, et al. "Improving Grid Resilience Using High-Voltage dc: Strengthening the Security of Power System Stability." IEEE Power and Energy Magazine. 2019; 17(3):38-47.
4. Page C, Johnson B, **Roberson D**, Nuqui R. "Increasing Grid Resilience Via Cyber-Secure Series Multiterminal LCC HVDC Transmission Systems." 2020 52nd North American Power Symposium (NAPS). 2020 52nd North American Power Symposium (NAPS); ; Tempe, AZ, USA. IEEE; c2021
5. **Roberson D,** O'Brien J. "Asymmetric Dual Sensor Latency in Distributed Control. IEEE Transactions on Power Systems." 2019 November; 34(6):4533-4541.

ADDITIONAL PRODUCTS

6. Al Rashdan A, **Roberson D**. "A Frequency Domain Control Perspective on Xenon Resistance for Load Following of Thermal Nuclear Reactors." IEEE Transactions on Nuclear Science. 2019; 66(9):2034-2041.
7. Hatton J, Johnson B, **Roberson D**, Nuqui R. "Increased Grid Resilience Via Cyber-Secure VSC Multiterminal HVDC Systems." 2019 IEEE Power & Energy Society General Meeting (PESGM). 2019 IEEE Power & Energy Society General Meeting (PESGM); ; Atlanta, GA.
8. **Roberson D**, O'brien J, inventors. US Patent No. 10,355,485 B2: "Variable loop gain using excessive regeneration for a delayed wide-area control system." 2019 July.
9. **Roberson D**, O'Brien J. "Variable Loop Gain Using Excessive Regeneration Detection for a Delayed Wide-Area Control System." IEEE Transactions on Smart Grid. 2018 November; 9(6):6623-6632.
10. **Roberson D**, Ellison J, Bhatnagar D, Schoenwald D. "Performance Assessment of the PNM Prosperity Electricity Storage Project: A Study for the DOE Energy Storage Systems Program." Sandia National Laboratories Technical Report, SAND2014-2883. 2014.

Synergistic Activities Related to Proposed Project

1. Dr. Roberson is a Member of the Defense Science Board, a committee of civilian experts appointed to advise the U.S. Department of Defense on scientific and technical matters. It was established in 1956 on the recommendation of the second Hoover Commission. The DSB conducts multiple simultaneous studies each year. Study topics are selected from requests made by Department of Defense or Congressional leaders. The Board shall be composed of not more than 45 members and not more than 12 Senior Fellow members, who are eminent authorities in the fields of science, technology, manufacturing, acquisition, and other matters of special interest to the Department of Defense. The Board members shall be appointed by the Secretary of Defense, and their appointments will be renewed on an annual basis.

2. The President of the United States appointed Dr. Roberson to the position of White House Fellow in August of 2019. Founded in 1964 by Lyndon B. Johnson, the White House Fellows program is one of America's most prestigious programs for leadership and public service. White House Fellowships offer exceptional young men and women first-hand experience working at the highest levels of the federal government. Selected individuals typically spend a year working as a full-time, paid Fellow to senior White House Staff, Cabinet Secretaries. Fellows also participate in an education program consisting of roundtable discussions with leaders from the private and public sectors, and trips to study U.S. policy in action both domestically and internationally. Fellowships are awarded on a strictly non-partisan basis.

3. Dr. Roberson has led and contributed to the development of substantial intellectual property with multi-institutional collaborations, "Image-Driven Self-Navigation of Drones in Indoor Environments" (patent pending, Serial No. 62/934,976) and "Variable Loop Gain Using Excessive Regeneration Detection for a Delayed Wide-Area Control System" (U.S. Patent No.: 10,355,485 B2). The former was nominated and selected as a finalist for the R&D 100 Award, a decoration which has "served as the most prestigious innovation awards program for the past 56 years, honoring great R&D pioneers and their revolutionary ideas in science and technology."

4. Dr. Roberson initiated and continues to lead the Center for Advanced Energy Studies (CAES) *Codebreaker* Seminar Series which speaks monthly to CAES inhabitants (as well as the Eastern Idaho community at large) about the breakthroughs related to cutting-edge research in power and energy. CAES houses Dr. Roberson's research team and is a world-class facility with five research institutions resident (University of Idaho, University of Wyoming, Idaho National Laboratory, Idaho State University, and Boise State University), providing an unmatched synergistic environment for the cultivation of internationally recognized interdisciplinary research in energy systems.

5. Through a collaborative effort between the Idaho National Laboratory and the University of Idaho, Dr. Roberson provides a course module for innovative interdisciplinary course on *Grid Resilience*. Delivered in the Fall semester of each academic year, the course seeks to teach students from various technical backgrounds (math, statistics, engineering, computer science, etc.) the concepts of grid resilience and stability, stimulating interdisciplinary collaborative efforts. Since its introduction, dozens of students with a wide array of backgrounds have learned cybersecurity, control systems, statistics and power system theory through the wide dissemination of the material in this course.

NAME: Constantinos Kolias

POSITION TITLE & INSTITUTION: Assistant Professor, University of Idaho

A. PROFESSIONAL PREPARATION - (see PAPPG Chapter II.C.2.f.(i)(a))

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE (if applicable)	YEAR (YYYY)
George Mason University	Fairfax, VA, USA	CS/Cybersecurity	Post-Doc	2014-2018
University of the Aegean	Samos, GR	CS/Cybersecurity	PhD	2008-2014
University of the Aegean	Samos, GR	CS/Cybersecurity	MSc	2005-2007
Technological Educational Institute of Athens	Athens, GR	CS	BSc	2002-2005

B. APPOINTMENTS - (see PAPPG Chapter II.C.2.f.(i)(b))

From - To	Position Title, Organization and Location
2018-Present	Assistant Professor, University of Idaho, Idaho, Idaho Falls

C. PRODUCTS - (see PAPPG Chapter II.C.2.f.(i)(c)) Products Most Closely Related to the Proposed Project

1. Kurt Vedros, Georgios Michail Makrakis, Constantinos Kolias, Min Xian, Daniel Barbara, Craig Rieger. "On the Limits of EM Based Detection of Control Logic Injection Attacks In Noisy Environments", In:2021 Resilience Week (RWS). IEEE 2021
2. Kolias, Constantinos, R. A. Borrelli, Daniel Barbara, and Angelos Stavrou. "Malware detection in critical infrastructures using the electromagnetic emissions of plcs." Transactions 1, no. 1 (2019): 519-522.
3. Kolias, Constantinos, Daniel Barbará, Craig Rieger, and Jacob Ulrich. "EM Fingerprints: Towards Identifying Unauthorized Hardware Substitutions in the Supply Chain Jungle." In 2020 IEEE Security and Privacy Workshops (SPW), pp. 144-151. IEEE, 2020.
4. Chatzigiannis, Panagiotis, Foteini Baldimtsi, Constantinos Kolias, and Angelos Stavrou. "Black-Box IoT: Authentication and Distributed Storage of IoT Data from Constrained Sensors." In Proceedings of the International Conference on Internet-of-Things Design and Implementation, pp. 1-14. 2021.
5. Rieger, Craig, Constantinos Kolias, Jacob Ulrich, and Timothy R. McJunkin. "A cyber resilient design for control systems." In 2020 Resilience Week (RWS), pp. 18-25. IEEE, 2020.

Other Significant Products, Whether or Not Related to the Proposed Project

1. Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. "DDoS in the IoT: Mirai and other botnets." Computer 50, no. 7 (2017): 80-84.
2. Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Stefanos Gritzalis. "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset." IEEE Communications Surveys & Tutorials 18, no. 1 (2015): 184-208.
3. Kolias, Constantinos, Angelos Stavrou, Jeffrey Voas, Irena Bojanova, and Richard Kuhn. "Learning Internet-of-Things security" hands-on"." IEEE Security & Privacy 14, no. 1 (2016): 37-46.
4. Efstratios Chatzoglou, Georgios Kambourakis, and Constantinos Kolias. Empirical Evaluation of AttacksAgainst IEEE 802.11 Enterprise Networks: The AWID3 Dataset . In:IEEE Access9 (2021), pp. 34188 34205.
5. Georgios Kambourakis, Constantinos Kolias, and Angelos Stavrou. The Mirai Botnet and the IoT ZombieArmies . In:Proceedings of the 36th international conference for military communications (MILCOM). (Baltimore,MD). IEEE Press. 2017.

D. SYNERGISTIC ACTIVITIES - (see PAPPG Chapter II.C.2.f.(i)(d))

Guest Editor
- Special Issue on "Cybersecurity in the IoT Era", IEEE Computer, 2018
- Special Issue on "Botnets", Information Applications, Information, 2019, MDPI
- Special Issue on "Design of Intelligent Intrusion Detection Systems", Electronics, 2021, MDPI

Associate Editor
- Journal of Information Security and Applications (JISAS), Elsevier, years: 2021-now

Editorial Board
- Communications Surveys & Tutorials, IEEE, years: 2021-now

Effective 10/04/2021 NSF BIOGRAPHICAL SKETCH OMB-3145-0058

NAME**: Benjamin Lampe**

POSITION TITLE & INSTITUTION: Clinical Instructor, Idaho State University

A. PROFESSIONAL PREPARATION - (see PAPPG Chapter II.C.2.f.(i)(a))

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE (if applicable)	YEAR (YYYY)
University of Wyoming	Laramie, WY	Electrical Engineering	BAS	2011
University of Idaho	Moscow, ID	Computer Science	MAS	2018

B. APPOINTMENTS - (see PAPPG Chapter II.C.2.f.(i)(b))

From - To Position Title, Organization and Location

2012 - 2015, Control System Engineer, Naval Nuclear Laboratory, Scoville, ID

2015 - 2018, Systems Analyst, Naval Nuclear Laboratory, Scoville, ID

2018 - 2021, Enterprise Architect, Naval Nuclear Laboratory, Scoville, ID

2022 - Present, Clinical Instructor, Idaho State University, Pocatello, ID

C. PRODUCTS - (see PAPPG Chapter II.C.2.f.(i)(c)) Products Most Closely Related to the Proposed Project

B. Lampe “Technical Industrial Network Strategy for the Nuclear Naval Laboratory”. Internal Publication (2018)

Other Significant Products, Whether or Not Related to the Proposed Project

D. SYNERGISTIC ACTIVITIES - (see PAPPG Chapter II.C.2.f.(i)(d))

Idaho State University Site Director for the Idaho Cyber Range

NAME: Sean McBride

POSITION TITLE & INSTITUTION: Idaho State University

A. PROFESSIONAL PREPARATION
(see PAPPG Chapter II.C.2.f.(i)(a))

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE (if applicable)	YEAR (YYYY)
Idaho State University	Pocatello, Idaho, USA	Information Systems	BBA	2004
Idaho State University	Pocatello, Idaho, USA	Business Administration - Information Assurance	MBA	2006
Thunderbird - Arizona State University	Glendale, Arizona, USA	Global Management	MGM	2010
LaTrobe University	Melbourne, Australia	Cybersecurity	PhD	2021

B. APPOINTMENTS
(see PAPPG Chapter II.C.2.f.(i)(b))

From - To	Position Title, Organization and Location
Aug 2017 - Present	Instructor and Program Coordinator, Industrial Security, Idaho State University
Oct 2018 – Present	Industrial Cybersecurity Specialist, Idaho National Laboratory
Jan 2016 – Jul 2017	Director – Industrial Control System Security; Manager – Attack Synthesis, FireEye
Mar 2015 – Jan 2016	Critical Infrastructure Lead Analyst, iSIGHT Partners
Dec 2008 – Mar 2015	Co-founder; Director of Analysis, Critical Intelligence
Jun 2006 – Dec 2008	Cyber Security Researcher/Analyst, Idaho National Laboraroty

C. PRODUCTS

(see PAPPG Chapter II.C.2.f.(i)(c))

Products Most Closely Related to the Proposed Project

S. McBride, J. Slay, C. Schou (2021). "A Vertically Integrated Pathway for Infusing Engineering Technicians with Industrial Cybersecurity Competencies". Colloquium for Information Systems Security Education (CISSE).

I. Ngambeki, S. McBride, J. Slay. (2021). "Knowledge Gaps in Curricular Guidance for ICS Security". Colloquium for Information Systems Security Education (CISSE).

S. McBride (2020). "Building an Industrial Cybersecurity Workforce: A Manager's Guide". https://inl.gov/wp-content/uploads/2020/12/ICS_Workforce-ManagersGuide2020.pdf

S. McBride (2019). "Untrusting the Grid" Power Grid International. https://www.power-grid.com/td/untrusting-the-grid/

Other Significant Products, Whether or Not Related to the Proposed Project

McBride, S. "Cyber-Attacks: Who's Keeping Score" War on the Rocks (2017). https://warontherocks.com/2017/07/cyber-attacks-whos-keeping-score/

McBride, S. "What about the plant floor? Six Subversive Concerns for Industrial Environments" (2017). https://www.fireeye.com/blog/threat-research/2017/04/six-subversive-concerns-for-ics-environments.html

McBride, S., Ashcraft, J., Belk, N. "Overload: Critical Lessons from 15 years of ICS Vulnerabilities"; (2016). https://www.fireeye.com/blog/threat-research/2016/08/overload-critical-lessons-from-15-years-of-ics-vulnerabilities.html

D. SYNERGISTIC ACTIVITIES

(see PAPPG Chapter II.C.2.f.(i)(d))

Co-Chair Industrial Cybersecurity Workforce Development Community of Practice

Professional consulting in the field of cyber threat intelligence

Member Champion, International Society of Automation Global Cybersecurity Alliance Traning and Education Charter Project

NAME: Ryan Lind

POSITION TITLE & INSTITUTION: IT Security Engineer, Idaho State University

A. PROFESSIONAL PREPARATION - (see PAPPG Chapter II.C.2.f.(i)(a))

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE (if applicable)	YEAR (YYYY)
Oregon State University	Corvallis, OR	Computer Science	BAS	2003
Idaho State University	Pocatello, ID	Masters of Business Administration	MBA	2006

B. APPOINTMENTS - (see PAPPG Chapter II.C.2.f.(i)(b))

From - To	Position Title, Organization and Location
2006 - 2012	Information Tech, Idaho State University, Pocatello, ID
2012 - Present	IT Security Engineer, Idaho State University, Pocatello, ID

Appendix C: Current and Pending Support

NSF CURRENT AND PENDING SUPPORT

PI/co-PI/Senior Personnel: Haney, Michael

PROJECT/PROPOSAL CURRENT SUPPORT

1. Project/Proposal Title: Idaho National Laboratory Joint Appointment

   Proposal/Award Number (if available):

   Source of Support: Idaho National Laboratory

   Primary Place of Performance: University of Idaho, Idaho Falls

   Project/Proposal Support Start Date (if available): 2019/10

   Project/Proposal Support End Date (if available): 2021/09

   Total Award Amount (including Indirect Costs): $405,791

   Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project:

Year	Person-months per year committed
2019	4.41
2020	4.41
2021	4.41

2. Project/Proposal Title: NuScale Simulator at the Center for Advanced Energy Studies

   Proposal/Award Number (if available):

   Source of Support: Department of Energy Infrastructure

   Primary Place of Performance: University of Idaho - Center for Advanced Energy Studies

   Project/Proposal Support Start Date (if available): 2019/10

   Project/Proposal Support End Date (if available): 2021/09

   Total Award Amount (including Indirect Costs): $285,763

   Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project:

Year	Person-months per year committed
2019	0.1

Year	Person-months per year committed
2020	0.1

3. Project/Proposal Title: Renewal: University of Idaho CyberCorps (R) SFS Program 2016

   Proposal/Award Number (if available):

   Source of Support: National Science Foundation, DGE, CyberCorps (R) Scholarship

   Primary Place of Performance: University of Idaho, Idaho Falls

   Project/Proposal Support Start Date (if available): 2016/09

   Project/Proposal Support End Date (if available): 2021/08

   Total Award Amount (including Indirect Costs): $405,081

   Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project:

Year	Person-months per year committed
2016	0.5
2017	0.5
2018	0.5
2019	0.5
2020	0.5

PROJECT/PROPOSAL PENDING SUPPORT

1. Project/Proposal Title: CPS: Frontier: Cyber-informed design, education, and training for cyberthreat resiliency with real-time reactor simulation

   Proposal/Award Number (if available):

   Source of Support: National Science Foundation

   Primary Place of Performance: University of Idaho - Idaho Falls

   Project/Proposal Support Start Date (if available): 2021/08

   Project/Proposal Support End Date (if available): 2026/07

   Total Award Amount (including Indirect Costs): $4,576,655

   Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project:

Year	Person-months per year committed
2021	1.08
2022	1.08
2023	1.08
2024	1.08
2025	1.08

R. A. Borrelli
University of Idaho · Idaho Falls Center for Higher Education
Department of Nuclear Engineering and Industrial Management

Project/Proposal Title: 2021 NRC Trade School and Community College Program Source of Support: Nuclear Regulatory Commission Total Award Amount: $162,224 Award Period: 2022.05.01 - 2024.04.30 Location of Project: College of Eastern Idaho, Idaho Falls ID Status: Pending Person-Months Per Year Committed to the Project: 0.33
Project/Proposal Title: Digital Instrumentation and Controls Design to Prevent, Detect, and Mitigate Cyberthreats Source of Support: Nuclear Regulatory Commission Total Award Amount: $498,267 Award Period: 2022.10.01 - 2025.09.30 Location of Project: University of Idaho · Idaho Falls Center for Higher Education Status: Pending Person-Months Per Year Committed to the Project: 0.45
Project/Proposal Title: Mountain West Cyber & Energy Alliance Source of Support: Department of Energy - University Based Cybersecurity Centers Total Award Amount: $2,500,000 Award Period: 2022.10.01 - 2024.09.30 Location of Project: University of Idaho; Boise State University; Idaho State University; University of Wyoming; Purdue University; Washington State University Status: Pending Person-Months Per Year Committed to the Project: 0.45
Project/Proposal Title: Secure Cyberspace and Resilient Industrial Systems Workforce Development Source of Support: Idaho Global Entrepreneurial Mission Initiative Total Award Amount: $2,099,700 Award Period: 2022.10.01 - 2025.09.30 Location of Project: University of Idaho · Idaho Falls Center for Higher Education Status: Pending Person-Months Per Year Committed to the Project: 0.45
Project/Proposal Title: Experimental determination of interactions between the radiation fields of Dragonfly's MMRTG and titan's environment Source of Support: Idaho NASA EPSCoR Research Initiation Grant Total Award Amount: $82,962 Award Period: 2021.08.01 - 2022.07.31 Location of Project: University of Idaho · Idaho Falls Center for Higher Education Status: Current Person-Months Per Year Committed to the Project: 0.75

Project/Proposal Title: NuScale Simulator at the Center for Advanced Energy Studies
Source of Support: DOE Infrastructure
Total Award Amount: $321,525
Award Period: 2019.10.01 - 2022.09.30
Location of Project: Center for Advanced Energy Studies
Status: Current
Person-Months Per Year Committed to the Project: n/a

*PI/co-PI/Senior Personnel Name: Constantinos Kolias

***Required fields**

Note: NSF has provided 15 project/proposal and 10 in-kind contribution entries for users to populate. Please leave any unused entries blank.

Project/Proposal Section:

Current and Pending Support includes all resources made available to an individual in support of and/or related to all of his/her research efforts, regardless of whether or not they have monetary value.[1] Information must be provided about all current and pending support, including this project, for ongoing projects, and for any proposals currently under consideration from whatever source, irrespective of whether such support is provided through the proposing organization or is provided directly to the individual. This includes, for example, Federal, State, local, foreign, public or private foundations, non-profit organizations, industrial or other commercial organizations, or internal funds allocated toward specific projects. Concurrent submission of a proposal to other organizations will not prejudice its review by NSF, if disclosed.[2]

[1] If the time commitment or dollar value is not readily ascertainable, reasonable estimates should be provided.
[2] The Biological Sciences Directorate exception to this policy is delineated in PAPPG Chapter II.D.2.

Projects/Proposals

1. *Project/Proposal Title : INL: Resilient Attack Interceptor for Intelligent Devices

*Status of Support : (•) Current ( ) Pending ( ) Submission Planned ( ) Transfer of Support

Proposal/Award Number (if available):

*Source of Support: Department of Energy

*Primary Place of Performance : University of Idaho, Idaho Falls

Project/Proposal Start Date (MM/YYYY) (if available) : 10/2019

Project/Proposal End Date (MM/YYYY) (if available) : 09/2022

*Total Award Amount (including Indirect Costs): $ 215,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2020	1.00	4.	
2. 2021	1.00	5.	
3. 2022	0.25		

*Overall Objectives : Develop methods and prototype for the identification of code injection attacks via Electromagnetic signal analysis, that get involuntarily transmitted by the device. Mitigate the impact of environmental noise.

*Statement of Potential Overlap : No overlap.

Projects/Proposals

2. *Project/Proposal Title : LDRD: Adaptive Fingerprinting of Control System Devices through Generative Adversarial Networks

*Status of Support : (•) Current ( ) Pending ( ) Submission Planned ( ) Transfer of Support

Proposal/Award Number (if available):

*Source of Support: Department of Energy

*Primary Place of Performance : University of Idaho, Idaho Falls

Project/Proposal Start Date (MM/YYYY) (if available) : 09/2021

Project/Proposal End Date (MM/YYYY) (if available) : 10/2024

*Total Award Amount (including Indirect Costs): $ 214,366

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	1.00	4.	
2. 2023	0.25	5.	
3. 2024	0.25		

*Overall Objectives : Develop methods and a system for the fingerprinting of alternative executional paths for anomaly detection, via the analysis of EM signals. This project extends current knowledge and insists in the automatic generation of artificial EM signals through the use of Generative Adversarial Networks. By doing so the need for manual collection of signals will be minimized.

*Statement of Potential Overlap : No overlap.

Projects/Proposals

3. *Project/Proposal Title : LDRD: Target-Aware Fuzzing

*Status of Support : (•) Current ( ) Pending ( ) Submission Planned ( ) Transfer of Support

Proposal/Award Number (if available):

*Source of Support: Department of Energy

*Primary Place of Performance : University of Idaho

Project/Proposal Start Date (MM/YYYY) (if available) : 09/2021

Project/Proposal End Date (MM/YYYY) (if available) : 10/2024

*Total Award Amount (including Indirect Costs): $ 185,261

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	0.25	4.	
2. 2023	0.25	5.	
3. 2024	0.25		

*Overall Objectives : Extend existing fuzzing tools by integragting machine learning, primarily Generative Adversarial Networks (GANs). Define of a standardized binary format for input: Neural Networks (NNs), including GANS, have defined immutable dimensions. Definition of a method for selecting sections of target binary files to standardize. Developing ML techniques for digesting a standardized binary file and informing a fuzzing.

*Statement of Potential Overlap : No overlap.

Projects/Proposals

4. *Project/Proposal Title : InTRiCPS - InTrinsically Resilient Cyber Physical System

*Status of Support : ○ Current ◉ Pending ○ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: Office of Naval Research

*Primary Place of Performance : University of Idaho, Couer d'Alene

Project/Proposal Start Date (MM/YYYY) (if available) : 01/2022

Project/Proposal End Date (MM/YYYY) (if available) : 12/2024

*Total Award Amount (including Indirect Costs): $ 1,723,915

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	2.00	4.	
2. 2023	2.00	5.	
3. 2024	2.00		

*Overall Objectives : We will develop methods to integrate and preserve data trustworthiness factors in control messages using ciphered integration and watermarking. We will provide tools to ensure availability and resiliency of LSCS functions demonstrated at end-user sites to validate agency/industry acceptance.

*Statement of Potential Overlap : No overlap.

Projects/Proposals

5. *Project/Proposal Title : Enabling Outsourcing of Nuclear Data with Attack-Resistant Federated Learning Optimized for Anomaly Detection Tasks

*Status of Support : ○ Current ◉ Pending ○ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: Department of Energy - NEUP

*Primary Place of Performance : University of Idaho, Idaho Falls

Project/Proposal Start Date (MM/YYYY) (if available) : 09/2022

Project/Proposal End Date (MM/YYYY) (if available) : 10/2024

*Total Award Amount (including Indirect Costs): $ 800,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2023	1.00	4.	
2. 2024	1.00	5.	
3. 2025	1.00		

*Overall Objectives : Introduce novel federated learning techniques optimized for the task of anomaly detection. The efforts will focus primarily on heterogeneous and vertically-partitioned data. Quantify the level of subjectiveness of federated anomaly detection techniques against sophisticated adversarial data-poisoning and model-poisoning techniques. Propose novel protection techniques against adversarial attacks affecting federated models.

*Statement of Potential Overlap : No overlap.

Projects/Proposals

6. *Project/Proposal Title : A Secure Communication Protocol for Instrumentation and Control Systems Based on the Devices' Immutable Characteristics and Side-Channel Analysis

*Status of Support : ○ Current ◉ Pending ○ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: Department of Energy - NEUP

*Primary Place of Performance : University of Idaho, Idaho Falls

Project/Proposal Start Date (MM/YYYY) (if available) : 09/2022

Project/Proposal End Date (MM/YYYY) (if available) : 10/2025

*Total Award Amount (including Indirect Costs): $ 800,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2023	1.00	4.	
2. 2024	1.00	5.	
3. 2025	1.00		

*Overall Objectives : Introduce a method and a system based on the analysis of EM signals for identifying violations in the intended control flow caused by malware infections. Provide a framework based on side-channel analysis for identifying the presence of hardware trojans. Propose a methodology for combining the output of the two approaches to sophisticated adversarial activity. Investigate the susceptibility of the proposed approach to sophisticated adversarial activity.

*Statement of Potential Overlap : No overlap.

*PI/co-PI/Senior Personnel Name: Dakota Roberson

***Required fields**

Note: NSF has provided 15 project/proposal and 10 in-kind contribution entries for users to populate. Please leave any unused entries blank.

Project/Proposal Section:

Current and Pending Support includes all resources made available to an individual in support of and/or related to all of his/her research efforts, regardless of whether or not they have monetary value.[1] Information must be provided about all current and pending support, including this project, for ongoing projects, and for any proposals currently under consideration from whatever source, irrespective of whether such support is provided through the proposing organization or is provided directly to the individual. This includes, for example, Federal, State, local, foreign, public or private foundations, non-profit organizations, industrial or other commercial organizations, or internal funds allocated toward specific projects. Concurrent submission of a proposal to other organizations will not prejudice its review by NSF, if disclosed.[2]

[1] If the time commitment or dollar value is not readily ascertainable, reasonable estimates should be provided.
[2] The Biological Sciences Directorate exception to this policy is delineated in PAPPG Chapter II.D.2.

Projects/Proposals

1. *Project/Proposal Title : Converter Agnostic High Voltage DC Grid Energy Highway to Facilitate Bulk Renewable Integration at the National Level (HYGRID)

*Status of Support : ○ Current ◉ Pending ○ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: U.S. Department of Energy ARPA-E

*Primary Place of Performance : University of Idaho

Project/Proposal Start Date (MM/YYYY) (if available) :

Project/Proposal End Date (MM/YYYY) (if available) :

*Total Award Amount (including Indirect Costs): $ 200,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	1.00	4.	
2. 2023	1.00	5.	
3. 2024	1.00		

*Overall Objectives : Develop new HVDC control concepts and small signal stability studies of large power grids under high penetrations of renewable energy.

*Statement of Potential Overlap : No overlap in work products or project aims.

Projects/Proposals

2. *Project/Proposal Title : INL Faculty Joint Appointment, National & Homeland Security Directorate

*Status of Support : (•) Current ( ) Pending ( ) Submission Planned ( ) Transfer of Support

Proposal/Award Number (if available):

*Source of Support: Idaho National Laboratory

*Primary Place of Performance : University of Idaho, Idaho Falls, ID

Project/Proposal Start Date (MM/YYYY) (if available) : 10/2021

Project/Proposal End Date (MM/YYYY) (if available) : 09/2022

*Total Award Amount (including Indirect Costs): $ 59,391

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2021	1.50	4.	
2. 2022	1.50	5.	
3.			

*Overall Objectives : Support INL N&HS directorate priorities in research, education and outreach as a faculty joint appointee

*Statement of Potential Overlap : no potential overlap

Projects/Proposals

3. *Project/Proposal Title : Cybersecure FACTS Control Development

*Status of Support : (•) Current ( ) Pending ( ) Submission Planned ( ) Transfer of Support

Proposal/Award Number (if available):

*Source of Support: Hitachi ABB Power Grids

*Primary Place of Performance : University of Idaho

Project/Proposal Start Date (MM/YYYY) (if available) : 04/2020

Project/Proposal End Date (MM/YYYY) (if available) : 12/2021

*Total Award Amount (including Indirect Costs): $ 100,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2020	2.00	4.	
2. 2021	1.50	5.	
3.			

*Overall Objectives : develop control system for dFACTS equipment which account for potential cyber attacks on equipment

*Statement of Potential Overlap : none

Projects/Proposals

4. *Project/Proposal Title : Mountain West Grid Resilience Initiative

*Status of Support : ○ Current ○ Pending ◉ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: US Department of Energy CESER

*Primary Place of Performance : University of Idaho, Idaho Falls, ID

Project/Proposal Start Date (MM/YYYY) (if available) : 04/2022

Project/Proposal End Date (MM/YYYY) (if available) : 04/2024

*Total Award Amount (including Indirect Costs): $ 1,275,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	1.50	4.	
2. 2023	1.50	5.	
3.			

*Overall Objectives : Consortium of universities to develop distribution system operation schemes as new market and regulatory conditions evolve and the grid's energy mix changes rapidly

*Statement of Potential Overlap : none

Projects/Proposals

5. *Project/Proposal Title : Cybersecurity Advisory Team for State Solar (CATSS)

*Status of Support : ○ Current ○ Pending ◉ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: National Association of State Energy Officials

*Primary Place of Performance : University of Idaho, Idaho Falls, ID

Project/Proposal Start Date (MM/YYYY) (if available) : 12/2021

Project/Proposal End Date (MM/YYYY) (if available) : 08/2022

*Total Award Amount (including Indirect Costs): $ 10,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2021	0.50	4.	
2. 2022	1.50	5.	
3.			

*Overall Objectives : advise NASEO and proposal awardees on cybersecurity issues regarding CATSS priorities

*Statement of Potential Overlap : none

*PI/co-PI/Senior Personnel Name: Benjamin Lampe

***Required fields**

Note: NSF has provided 15 project/proposal and 10 in-kind contribution entries for users to populate. Please leave any unused entries blank.

Project/Proposal Section:

Current and Pending Support includes all resources made available to an individual in support of and/or related to all of his/her research efforts, regardless of whether or not they have monetary value.[1] Information must be provided about all current and pending support, including this project, for ongoing projects, and for any proposals currently under consideration from whatever source, irrespective of whether such support is provided through the proposing organization or is provided directly to the individual. This includes, for example, Federal, State, local, foreign, public or private foundations, non-profit organizations, industrial or other commercial organizations, or internal funds allocated toward specific projects. Concurrent submission of a proposal to other organizations will not prejudice its review by NSF, if disclosed.[2]

[1] If the time commitment or dollar value is not readily ascertainable, reasonable estimates should be provided.
[2] The Biological Sciences Directorate exception to this policy is delineated in PAPPG Chapter II.D.2.

Projects/Proposals

1. *Project/Proposal Title : RADICL Lab

*Status of Support : ○ Current ◉ Pending ○ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: HERC iGEM Grant

*Primary Place of Performance : Idaho Falls University Place Campus

Project/Proposal Start Date (MM/YYYY) (if available) : 07/2022

Project/Proposal End Date (MM/YYYY) (if available) : 06/2025

*Total Award Amount (including Indirect Costs): $ 2,100,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	0.50	4.	
2. 2023	1.00	5.	
3. 2024	1.00		

*Overall Objectives : Establish Student Stations for Workforce development and aptitude testing exercises
Establish 2 trainers for Workforce development and aptitude testing exercises

*Statement of Potential Overlap : None, work is accomplished during summer months.

*PI/co-PI/Senior Personnel Name: Sean McBride

***Required fields**

Note: NSF has provided 15 project/proposal and 10 in-kind contribution entries for users to populate. Please leave any unused entries blank.

Project/Proposal Section:

Current and Pending Support includes all resources made available to an individual in support of and/or related to all of his/her research efforts, regardless of whether or not they have monetary value.[1] Information must be provided about all current and pending support, including this project, for ongoing projects, and for any proposals currently under consideration from whatever source, irrespective of whether such support is provided through the proposing organization or is provided directly to the individual. This includes, for example, Federal, State, local, foreign, public or private foundations, non-profit organizations, industrial or other commercial organizations, or internal funds allocated toward specific projects. Concurrent submission of a proposal to other organizations will not prejudice its review by NSF, if disclosed.[2]

[1] If the time commitment or dollar value is not readily ascertainable, reasonable estimates should be provided.
[2] The Biological Sciences Directorate exception to this policy is delineated in PAPPG Chapter II.D.2.

Projects/Proposals

1. *Project/Proposal Title : Hierarchical Software Quality Assurance

*Status of Support : ○ Current ◉ Pending ○ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available): LRBAA 18-01-SEC CYB 06-01-0023-VP Type III

*Source of Support: Department of Homeland Security

*Primary Place of Performance : Pocatello, ID

Project/Proposal Start Date (MM/YYYY) (if available) :

Project/Proposal End Date (MM/YYYY) (if available) :

*Total Award Amount (including Indirect Costs): $ 136,472

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	1.00	4.	
2.		5.	
3.			

*Overall Objectives :

i) Measure source code quality and maturity of ICS and cloud-based software (i.e., Azure) in supply and production chains,
ii) Assess the composition, stylometry and origination of software to verify that they are truthful, complete and accurate, as described in software bill of materials, and
iii) Identify security zones and sensitive sections of source code
McBride will apply these objectives to industrial environments

*Statement of Potential Overlap :

LRBAA deals with software assurance implications.
CESER proposal deals with electric grid implications.

Projects/Proposals

2. *Project/Proposal Title : CESER - Mountain West Grid Resilience Initiative

*Status of Support : ○ Current ○ Pending ◉ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available): DE-FOA-0002503

*Source of Support: U.S. Department of Energy

*Primary Place of Performance : Pocatello, ID

Project/Proposal Start Date (MM/YYYY) (if available) :

Project/Proposal End Date (MM/YYYY) (if available) :

*Total Award Amount (including Indirect Costs): $ 150,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	1.00	4.	
2.		5.	
3.			

*Overall Objectives :

*Statement of Potential Overlap :

LRBAA deals with software assurance implications.
CESER proposal deals with electric grid implications.
IGEM deals with equipment for Idaho Falls lab

Projects/Proposals

3. *Project/Proposal Title : Sectoral Partnership for Industrial Control Systems Security

*Status of Support : ○ Current ○ Pending ◉ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: EDA ARPA Good Jobs Challenge

*Primary Place of Performance : Pocatello, Idaho

Project/Proposal Start Date (MM/YYYY) (if available) :

Project/Proposal End Date (MM/YYYY) (if available) :

*Total Award Amount (including Indirect Costs): $ 20,000,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	0.50	4. 2025	0.50
2. 2023	0.50	5. 2026	0.50
3. 2024	0.50		

*Overall Objectives : Establish a consortium of industrial cybersecurity employers
Expand capacity to deliver quality education and training opportunities
Create a registered apprenticeship program for industrial cybersecurity
Develop the industrial cybersecurity education and training community of practice

*Statement of Potential Overlap : Focused on capacity building in pocatello and on education rather than research.

Projects/Proposals

4. *Project/Proposal Title : SFS for Inter-mountain West

*Status of Support : ○ Current ○ Pending ◉ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: NSF SFS Program

*Primary Place of Performance : Pocatello, Idaho

Project/Proposal Start Date (MM/YYYY) (if available) :

Project/Proposal End Date (MM/YYYY) (if available) :

*Total Award Amount (including Indirect Costs): $ 5,000,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	1.00	4. 2025	1.00
2. 2023	1.00	5. 2026	1.00
3. 2024	1.00		

*Overall Objectives : Create interdisciplinary cybersecurity professionals for the federal government.

*Statement of Potential Overlap : Focused on serving federal workforce needs.

*PI/co-PI/Senior Personnel Name: Ryan Lind

***Required fields**

Note: NSF has provided 15 project/proposal and 10 in-kind contribution entries for users to populate. Please leave any unused entries blank.

Project/Proposal Section:

Current and Pending Support includes all resources made available to an individual in support of and/or related to all of his/her research efforts, regardless of whether or not they have monetary value.[1] Information must be provided about all current and pending support, including this project, for ongoing projects, and for any proposals currently under consideration from whatever source, irrespective of whether such support is provided through the proposing organization or is provided directly to the individual. This includes, for example, Federal, State, local, foreign, public or private foundations, non-profit organizations, industrial or other commercial organizations, or internal funds allocated toward specific projects. Concurrent submission of a proposal to other organizations will not prejudice its review by NSF, if disclosed.[2]

[1] If the time commitment or dollar value is not readily ascertainable, reasonable estimates should be provided.
[2] The Biological Sciences Directorate exception to this policy is delineated in PAPPG Chapter II.D.2.

Projects/Proposals

1. *Project/Proposal Title : RADICL Lab

*Status of Support : ○ Current ◉ Pending ○ Submission Planned ○ Transfer of Support

Proposal/Award Number (if available):

*Source of Support: HERC iGEM Grant

*Primary Place of Performance : Idaho Falls University Place Campus

Project/Proposal Start Date (MM/YYYY) (if available) : 07/2022

Project/Proposal End Date (MM/YYYY) (if available) : 06/2025

*Total Award Amount (including Indirect Costs): $ 2,100,000

*Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project

*Year (YYYY)	*Person Months (##.##)	Year (YYYY)	Person Months (##.##)
1. 2022	0.50	4.	
2. 2023	0.50	5.	
3. 2024	0.50		

*Overall Objectives : Establish Integrations between IRI students and the RADICL Lab experience offerings.

*Statement of Potential Overlap : None

Appendix D: Senior Personnel

Dr. Michael Haney is an Associate Professor of Computer Science and Cybersecurity with the University of Idaho and holds a joint appointment as cybersecurity researcher with the Idaho National Laboratory. He is an associate of the Center for Advanced Energy Studies in Idaho Falls, ID and of the Center for Secure and Dependable Systems in Moscow, ID. He is also an affiliate faculty for the UI's Nuclear Engineering and Technology Management programs. He received his M.S. and Ph.D. in Computer Science from the University of Tulsa in 2013 and 2015, respectively. He received his B.S. in Mathematics from the University of Kentucky in 1998. Currently, his research interests are in visualization and graph analysis of network and system log data to improve intrusion detection and response for large-scale networks. He studies cybersecurity issues of energy systems supporting a more resilient "smart" infrastructure. This includes creating models and simulations of large scale industrial cyber-physical control systems (e.g. power generation systems, water treatment plants, oil refineries), modeling and studying the effects of cyber-attacks against these systems and designing tactical security solutions as well as robust risk mitigation strategies for these systems.

Prior to joining Academia, Dr. Haney had 15 years of industry experience designing, implementing, and managing information assurance programs for SMB and Fortune 500 consulting clients in many industries, including financial services, energy, retail, healthcare, telecom, software, manufacturing, and education, as well as city, state, and federal government agencies. He has previously taught security training courses for the SANS Institute, Walmart Stores, ISACA, USN SPAWAR, US Secret Service, and the UK Royal Military Police. He maintains several industry and government security certifications, including PCI QSA, GSEC, GCIA, GCIH, GCFA, and CISSP.

Dr. Haney will provide the overall guidance and direction of this effort. His primary focus will be on the integration of systems across the laboratory complex, and on the development of adversarial capabilities. He will be responsible for oversight of the postdoctoral research fellows and the mentorship of graduate students on the project.

Dr. R. A. Borrelli Nuclear Engineering is an Associate Professor in the Department of Nuclear Engineering and Industrial Management at the University of Idaho - Idaho Falls Center for Higher Education. He has expertise with the back-end of the fuel cycle through dissertation and postdoctorate research and the front end of the fuel cycle with current research, with computational modeling of the fuel cycle, including safeguards- and security-by-design, as well as cybersecurity of nuclear installations. Prof. Borrelli is a co-PI of this project and will be responsible for infrastructure development related to energy systems, nuclear plants, risk assessment, and cybersecurity. He teaches Principles of Nuclear Engineering, Nuclear Fuel Cycle Analysis, and Risk Assessment at UI and is active nationally in the American Nuclear Society, including faculty adviser for the University of Idaho American Nuclear Society Student Section.

Dr. Dakota Roberson is an Assistant Professor in the Department of Electrical and Computer Engineering at the University of Idaho. He intends to use this equipment for several purposes, including the advancement of his research goals and training of graduate students in electrical engineering. Grad students will be implementing novel control and security strategies on the equipment to demonstrate initial results to be used in the pursuit of Department of Energy grant funds to further develop the virtualized substation and distribution system operations concepts. Specific programs in DOE have expressed great interest in this topic recently, including the Cybersecurity, Energy Resilience and Emergency Response (CESER) program, and Idaho's investment in this equipment will provide foundational results for Dr. Roberson has also begun working with numerous regional utilities and others in this area, including Idaho Falls Power, Intel, Western Area Power Administration, Avista, and the Idaho National Lab, so this project will help further his research

and education in advanced electric power grid control and operations.

Dr. Constantinos Kolias joined the Computer Science Department at the University of Idaho in 2018. Before that he served as a Research Assistant Professor under the supervision of Angelos Stavrou, in the CS Department at George Mason University. He received his doctorate in 2014 from the University of the Aegean under the supervision of Georgios Kambourakis. His main research interest revolves around security and privacy for the Internet of Things and critical infrastructures. He is also active in the design of intelligent Intrusion Detection Systems (IDS) with a special interest in privacy preserving distributed IDS. Other areas of interest include mobile and wireless communications security, and privacy enchasing techniques for the Internet. In 2015 he created and released the first wireless dataset specifically intended for research in wireless security, namely the AWID dataset. Today AWID has been downloaded and used as a benchmark by hundreds of organizations and universities. Dr. Kolias's research focus areas include security and privacy of the Internet of Things (IoT) and industrial systems, particiularly the cybersecurity issues of smart grids and other critical infrastructures. He will focus in this project on the integration of both small and mid-scale cyber-physical systems in our facilities.

Ben Lampe, (Idaho State University) received his Bachelor of Science in Electrical Engineering from the University of Wyoming. Immediately after, he was employed by the Naval Nuclear Laboratory (NNL) for the past 10 years. During his tenure at the NNL, he received a Masters of Science in Computer Science from the University of Idaho. As the control system engineer, he has experience designing and building systems that controlled processes across water, power, radiation detection, radiation and building hvac sectors. After he transitioned from control systems into IT as part of the exclusive IT Leadership Development Program within NNL, his role became the OT Enterprise Architect.

Ben's professional achievements during his tenure with the NNL include drafting, architecting, and implementing the Nationwide Operational Technology (OT) Technical Strategy for the US Naval Reactor Program. This strategy is implemented and used currently across the United States at all facilities within the Naval Nuclear Laboratory program. Currently holds a Postsecondary Limited Occupational Specialist in Engineering Technology, Information Technology and Electronics Technology from the Idaho Division of Career Technical Education, and an Alerton Certified Engineer credential.

Sean McBride, (Idaho State University) Within Idaho State University's Energy Systems Technology Education Center (ESTEC), Sean McBride runs the nation's only 2 year, hands-on degree to specialize in defending industrial facilities from cyber attacks and incidents. Sean joined ISU after leaving FireEye, where he developed the firm's Industrial Control Systems (ICS) security business strategy. Sean's professional accomplishments include pioneering work in threat and vulnerability intelligence, which evolved into the DHS ICS-CERT, and co-founding Critical Intelligence to focus on the unique intelligence needs of industrial entities. Over the past decade, Sean has written extensively for his customers, provided expert analysis for the popular press, and briefed the results of his work at leading professional conferences such as RSA and S4. Sean earned an MBA in the NSA Scholarship for Service Program at ISU in 2006. He earned a Masters in Global Management from Thunderbird – Arizona State University in 2010. He is currently a doctoral candidate at La Trobe University, Australia, under the mentorship of Dr. Jill Slay Sean will offer laboratory, curricular, and instructional design input based on his work developing education and training standards for industrial cybersecurity.

Ryan Lind, (Idaho State University) has operated as the system administrator and supervisor for the National Information Assurance Training and Education Center (NIATEC) and the Informatics Research Institute (IRI) since 2006, and is responsible for system and network architecture, security, and maintenance. As supervisor of our Scholarship for Service students Ryan provides guidance and oversight of the candidates

day to day work activities in forwarding their security focused projects and education. Starting in 2014 we began creating, hosting, and functioning as the white team for the NIATEC Invitational Collegiate Cyber Defense Competition (NICCDC), while we pride ourselves on this being a student built and run competition, Ryan operates as the primary technical and policy consultant for the students. Our competition is built to test business, policy, and technical aspects of cyber security. In 2018 we began incorporating Industrial Control System challenges into the competition and modeling our competition network after the Purdue Model.

Appendix E: Other

E.1 ISU Sub-Award Documentation

ISU focus in this grant partnership is workforce training and development. The funds allocated to ISU in support of the R.A.D.I.C.L. space is intended to be used to stock, implement, and facilitate workforce training and development efforts. These workforce development efforts include the skills, knowledge, and experience necessary to create effective Cyber-physical Security Analysts and Cyber-informed Industrial technicians. By funding this effort, ISU-College of Technology is enhanced in its scale and abilities to provide quality workforce training and development. Additionally, this lab will also enable ISU to introduce amplitude testing services for Idaho and Federal employers. Just like how software developers must take a coding exam during an interview, this RADICL Lab will enable ISU to provide Industrial exams to potential new hires during their interview processes as well as to existing employees to help employers validate their aptitudes to job responsibilities.

This funding will be used to implement a total of 8 fixed student stations and 8 non-fixed student stations will be deployed initially with this grant. The student stations will consist of an Industrial Ethernet Switch, a Desktop Computer (fixed) or Laptop (non-fixed), desktop monitors, a station IP camera (fixed), a Raspberry Pi, an Arduino microcontroller, a CodeSys compliant micro PLC, a few breadboards, a variable power source, oscilloscope, an RF Spectrum Analyzer, and an inventory of electronics accessories (e.g., Resistors, Capacitors, Sensors, cabling). The non-fixed Student stations will be stored in wheeled transport boxes.

Two Fixed Lab experiences will be implemented with this funding for bootcamps, high school camps, and other transitory student exercises. These two fixed Lab experiences will be driven by a Rockwell PLC and consist of a main chassis with a controller, network cards, and local I/O cards, additional remote I/O chassis with a network card, and local I/O cards, an Industrial Ethernet Switch. These fixed lab experiences will initially be deployed to represent a power generation exercise and a power distribution exercise which currently do not exist in the South East Idaho region at our institutions. The Power Generation exercise will be handled by a set of small scale motors, sensors, and circuit breakers. The Power Distribution exercise will be handled by a set of LED light bulbs, sensors, and circuit breakers.

Four additional desktop PCs with two monitors each and two network switches will be procured and sit along the back wall on the RADICL Lab. These four stations will be deployed with SCADA software that allows for either the two fixed lab experiences or any of the 16 student stations to report data and provide exercises that integrate across many “sectors" which is becoming an increasingly important skill set in this data-driven workforce. All procured equipment will remain as the property of the RADICL Lab.

E.2 Letters of Support

CURTISS-WRIGHT

February 1. 2022

Higher Education Research Council Idaho State Board of Education Idaho State University 650 West State Street, 3rd Floor Boise, ID 83702

SUBJECT: Letter of Support for UI's and ISU's joint IGEM Higher Education Research Council Grant Proposal

Dear Members of the Higher Education Research Council:

Curtiss-Wright (CW) Nuclear Division, located in Idaho Falls, ID, provides a comprehensive range of products and services that sustain the safe, reliable, and cost-effective operation of nuclear power plants worldwide. We offer proactive solutions to critical plant issues and provide both analog and digital solutions.

CW is committed to involving the community to raise awareness of global needs in the nuclear industry. To this end, we recently hosted a group of local high school students at our facility for one day as part of a six-day CyberCore STEM Summer Camp. Our goal was centered on introducing students to various topics relating to cybersecurity, circuit design, soldering, and much more. Students were provided an overview of our company and industry, went on a facilities tour, learned about basic electronic theory and electronic components, participated in discussions on STEM careers, and completed a soldering course and project. This successful event was sponsored by College of Eastern Idaho, University of Idaho, Idaho National Laboratory, Rocky Mountain Power, and CW.

There is a great need to have a well-prepared, highly skilled cybersecurity workforce in place to help move the nuclear industry forward. Having a solid background in STEM and analytical skills, with an emphasis on cyber-physical systems is important to the infrastructure of our industry on a local and global level. The proposal put forth by the University of Idaho and Idaho State University researchers provides opportunities for strong collaboration between CW, regional industry partners, and the other Idaho public institutes of higher education. CW is committed to our partnership with Idaho state public schools, colleges, and universities and looks forward to continuing collaborative efforts around innovative platforms such as this one.

Sincerely,

Theresa Sutter

Theresa Sutter, General Manager, Curtiss-Wright

Idaho State University

January 14, 2022

Office of the Idaho State Board of Education
Higher Education Research Council
Idaho Global Entrepreneurial Mission Initiative
IGEM-HERC
650 W State St, STE 307
Boise, ID 83720

Re: iGEM Grant Proposal – U of I and ISU collaboration in Idaho Falls

Dear Committee Members,

On behalf of Idaho State University College of Technology, I am writing this letter of collaboration and support for the Idaho Global Entrepreneurial Mission Initiative (iGEM) proposal to create an effective cybersecurity lab experience on the Idaho Falls campus. Our College's focus is to support the R.A.D.I.C.L. Lab to be used to facilitate workforce training and development efforts in the cyber-physical security sector with the end goal of empowering cyber-physical security analysts and cyber-informed industrial technicians with the skills, knowledge, and experience necessary in today's workforce.

Our industry partners have identified a need for technicians to gain a deeper understanding of critical infrastructure vulnerabilities and how to mitigate them. If funded, this project will enhance the College of Technology's scale and ability to provide quality workforce training and development. Additionally, this lab will also enable ISU to introduce amplitude testing services and provide Industrial exams to a new and existing workforce.

This collaboration will provide an additional layer of workforce training and development beyond what we are currently doing in the College of Technology. Our partnership will have a greater reach to many more students and provide opportunities for high quality learning experiences.

The College of Technology is pleased to provide this letter of support for the iGEM proposal, and we are dedicated to moving this project forward! As committed stakeholders in this project, we are confident that Idaho students will benefit from enhanced lab experiences, while meeting a growing workforce need.

Sincerely yours,

Debra Kay Ronneburg

Debra Ronneburg
Interim Dean | College of Technology

Eames Complex | Room 18
921 South 8th Ave., Stop 8230 | Pocatello, ID 83209
(208) 282-2602 | debraronneburg@isu.edu

College of Eastern Idaho
1600 South 25th East • Idaho Falls, Idaho 83404-5788 • 208.524.3000 • www.cei.edu

January 31, 2022

This letter is in support of a request for a HERC IGEM grant to help to build on the work already in progress through funding from the State of Idaho supporting the development, research, and creation of the Idaho Cyber Range. This grant would build upon the capacity to extend the current work protecting education, corporate and physical infrastructure from cyber-attacks. The funding would provide researchers and students with a realistic environment in which to develop skills for protecting computer networks and connected devices from cyber-attacks. The grant would assist with the purchase of both equipment and other resources required to provide a comprehensive learning environment that could be used to identify and thwart attacks against those systems critical to both commerce and infrastructure. Those networks and physical systems are critical to protecting our freedoms and way of life from those who might wish harm.

The College of Eastern Idaho has invested resources, personnel, and facilities in this endeavor, but as we assist with the education of over eighty students in learning cybersecurity skills this semester, we know that the needs of Idaho and the many stakeholders are far greater than current resources allow. The resources this grant would provide will allow the universities and colleges in our state to collaborate and utilize the power of the Cyber Range and the collective knowledge of our higher education system to strengthen the labor pool in Idaho to meet the needs critical to our futures.

On behalf of the College of Eastern Idaho, I strongly support the creation of the Idaho Cyber Range knowing this will help us train technicians and ensure a better future for all our citizens.

Sincerely,

Rick Aman, PhD
President, College of Eastern Idaho

COLLEGE OF SOUTHERN IDAHO

OFFICE OF THE PROVOST
208.732.6281 • Fax 208.736.4785

February 1, 2022

Office of the Idaho State Board of Education
Higher Education Research Council
Idaho Global Entrepreneurial Mission Initiative-IGEM-HERC
650 W State Street, Ste 307
Boise, ID 83720

Re: iGEM Grant Proposal | University of Idaho Cybersecurity Lab

Dear Higher Education Research Council Members,

On behalf of the College of Southern Idaho, I am pleased to provide this letter of support for the Idaho Global Entrepreneurial Mission Initiative (iGEM) proposal for the *Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL)*. While much progress has been made in Idaho cybersecurity education in recent years, there is much left to do. The proposed RADICL projects include enhancements of great interest to CSI especially with regard to the promise of the Idaho Cyber Range improvements. The proposal specifically mentions support for the four Idaho community colleges and we are grateful for this consideration.

Beyond the direct benefits to our own cybersecurity educational programming, we also support the conceptual framework and intent of the proposal in order to provide Idaho employers the technicians and professionals they so desperately need, alongside the opportunities to create a "safer Idaho" for her citizenry.

Please accept this letter of support and know that CSI will be pleased to participate in the projects if and when called upon to do so.

Respectfully,

Todd Schwarz, Ph.D.
Provost

References

[1] TWI, Ltd, 2020. What are Technology Readiness Levels (TRLs)?

[2] Mena, Pedro, Borrelli, R. A., Kerby, Leslie. Nuclear Technology 208, 232.

[3] Peterson, John, Haney, Michael, Borrelli, R. A., 2019. An overview of methodologies for cyber security vulnerability assessments conducted in nuclear power plants. Nuclear Engineering and Design 346, 75.

[4] MacLean, Trevor, Borrelli, R. A., Haney, Michael A., 2019. 'Cybersecurity modeling of non-critical nuclear power plant digital instrumentation.' Critical Infrastructure Protection XIII. Jason Staggs, Sujeet Shenoi, eds. in: Chapter 5, 277.

[5] Larrucea, Xabier, Santamaría, Izaskun, 2020. Designing a cyber range exercise for educational purposes. In: Murat Yilmaz, Jörg Niemann, Paul Clarke, Richard Messnarz, eds., Systems, Software and Services Process Improvement. Springer International Publishing. ISBN 978-3-030-56441-4, 302.

[6] Arshad, Sobia, Alam, Masoom, Al-Kuwari, Saif, Khan, Muhammad Haider Ali, 2021. Attack specification language: Domain specific language for dynamic training in cyber range. In: 2021 IEEE Global Engineering Education Conference (EDUCON). 873. doi:10.1109/EDUCON46332.2021.9454094.

[7] Nock, Oliver, Starkey, Jonathan, Angelopoulos, Constantinos Marios, 2020. Addressing the Security Gap in IoT: Towards an IoT Cyber Range. Sensors 20. doi:10.3390/s20185439.

[8] Yamin, Muhammad Mudassar, Katt, Basel, Gkioulos, Vasileios, 2020. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security 88, 101636.

[9] Chouliaras, Nestoras, Kittes, George, Kantzavelou, Ioanna, Maglaras, Leandros, Pantziou, Grammati, Ferrag, Mohamed Amine, 2021. Cyber ranges and testbeds for education, training, and research. Applied Sciences 11, 1809.

[10] Workman, Michael D., Luévanos, J. Anthony, Mai, Bin, 2021. A Study of Cybersecurity Education Using a Present-Test-Practice-Assess Model. 1. doi:10.1109/TE.2021.3086025.

[11] van Steen, Tommy, Deelman, Julia R. A., 2021. Successful Gamification of Cybersecurity Training. Cyberpsychology, Behavior, and Social Networking 24, 593.

[12] Scholefield, Sam, Shepherd, Lynsay A., 2019. Gamification Techniques for Raising Cyber Security Awareness. In: Abbas Moallem, ed., HCI for Cybersecurity, Privacy and Trust. Springer International Publishing. ISBN 978-3-030-22351-9, 191.

[13] Fenton, Demitrius, Traylor, Terry, Hokanson, Guy, Straub, Jeremy, 2019. Integrating Cyber Range Technologies and Certification Programs to Improve Cybersecurity Training Programs. In: Michael E. Auer, Thrasyvoulos Tsiatsos, eds., The Challenges of the Digital Transformation in Education. Springer International Publishing. ISBN 978-3-030-11935-5, 632.

[14] Alqahtani, Hamed, Kavakli-Thorne, Manolya, 2020. Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR). Information 11, 121.

[15] Shivapurkar, Mandar, Bhatia, Sajal, Ahmed, Irfan, 2020. Problem-caed learning for cybersecurity education. Journal of The Colloquium for Information Systems Security Education 7, 6.

[16] Escape Room Supplier, 2022. Electronic Props. https://www.escaperoomsupplier.com/product-category/electronic-props/.

Acronyms

CAES Center for Advanced Energy Studies.

CESER Office of Cybersecurity, Energy Security, and Emergency Response.

CPS Cyber-Physical Systems.

DEPSCoR Defense Established Program to Stimulate Competitive Research.

DHS Department of Homeland Security.

DoD Department of Defense.

DOE Department of Energy.

EPSCoR Established Program to Stimulate Competitive Research.

HERC Higher Education Research Council.

ICR Idaho Cyber Range.

IGEM Idaho Global Entrepreneurial Mission Initiative.

ISU Idaho State University.

NCAE-CD National Centers of Academic Excellence in Cyber Defense.

NEUP Nuclear Energy University Program.

NSF National Science Foundation.

PLC Programmable Logic Controller.

RADICL Reconfigurable Attack-Defend Instructional Computing Laboratory.

SaTC Secure and Trustworthy Cyberspace.

TRL Technology Readiness Level.

UI University of Idaho.

UIIF Idaho Falls Center for Higher Education.

WSC Western Services Corporation Simulator.