Idaho National Laboratory

January 27, 2022

CCN 250934

Maiea Sellers
Area Director, Seattle Regional Office
U.S. Economic Development Administration
Jackson Federal Building
915 Second Avenue, Room 1890, Seattle, WA 98174-1001

via Email

SUBJECT: Sectoral Partnership for Industrial Cybersecurity Education Good Jobs Challenge Proposal

Dear Director Sellers:

Idaho National Laboratory (INL) enthusiastically supports the Good Jobs Challenge grant proposal submitted by the Idaho State University (ISU). INL is excited to be included as an unfunded sectoral partner and is planning efforts around this proposal that fit within our current programs.

Located in Idaho Falls, Idaho, and managed by Battelle Energy Alliance, INL is one of the national laboratories of the United States Department of Energy (DOE). The laboratory performs basic and applied research in DOE strategic areas of energy, national security, science, and environment, and serves as the nation's leading center for nuclear energy research and development.

As a world leader in industrial cybersecurity, INL works across federal agencies, private industry, and academia to develop scalable and sustainable solutions designed to protect operational environments from an ever-evolving threat landscape.

Through this proposal, INL recognizes the urgent need to deliver highly relevant industrial cybersecurity training and education to address the growing capability gap to develop the qualified professionals necessary for this interdisciplinary work. In support of these efforts, and as part of our on-going partnership, the laboratory and ISU will continue the following activities:

- Leading the Industrial Cybersecurity Community of Practice – co-founded by INL and ISU, focused on education, training and workforce development efforts across industry, government, and academia
- Leveraging ISU's talent pipelines to include internships, direct hires, and joint appointments
- Increasing INL's professional development and employee education opportunities
- Serving as part of ISU's Cybersecurity Technical Advisory Committee

Cybersecurity is fundamental across scientific, engineering, business, critical infrastructure, and operational environments. The need for focused workforce development efforts, such as the Industrial Cybersecurity Education proposal, and its objectives, will create integrated learning pathways while also enabling technical education innovation, and enhancements that will benefit employers, students, and future job seekers.

INL looks forward to continuing our collaborative efforts in industrial cybersecurity workforce development and building a national talent pipeline with ISU to address these critical needs.

Sincerely,

Zach Tud

Zachary D. Tudor, CISSP, CISM
Associate Laboratory Director
National & Homeland Security

EJT:JCR

cc: W.E. Austad, INL, MS 3750
M.T. Bingham, INL, MS 3605
E.J. Taylor, INL, MS 1444

EASTERN IDAHO IS redi

MAILING ADDRESS
PO Box 51564
Idaho Falls, Idaho 83405

OFFICE: 208.522.2014

www.rediconnects.org

PHYSICAL ADDRESS
901 Pier View Drive, Suite 204
Idaho Falls, Idaho 83402

TOLL FREE: 1-877-355-0484

info@rediconnects.org

January 15, 2022

Benjamin Lampe
Clinical Instructor-Industrial Cybersecurity Engineering Technology
Idaho State University College of Technology
Eames Complex 103
921 S 8th Ave Stop 8230
Pocatello, ID 83209

Dear Mr. Lampe:

This letter is written in support of Idaho State University College of Technology and its grant application for the Economic Development Administration (EDA) American Rescue Plan Act Good Jobs Challenge. Idaho State University College of Technology is an ideal candidate to be the lead organization and backbone organization as ISU's College of Technology is poised to (1) developing and strengthening regional workforce training systems that support sectoral partnerships, (2) designing sectoral partnerships, and (3) implementing sectoral partnerships that will lead to high-quality jobs.

Regional Economic Development for Eastern Idaho (REDI) is a regional economic development organization covering 15-counties in Southeast and East Idaho (Eastern Idaho). As the lead regional economic development organization in Southeast and East Idaho, REDI brings together business, industry, government, academic, and community leaders to capitalize on Eastern Idaho's assets through investments, workforce development, education, and training, infrastructure, programs, and research capabilities to meet the needs of our regional businesses, communities, and universities. REDI works with Idaho State University and the College of Technology on education, workforce development, grants, public/private partnerships, research and technology transfer initiatives.

In closing, REDI offers our utmost support for Idaho State University College of Technology's grant application.

Sincerely,

McKnight

Teresa McKnight
Chief Executive Officer

Cc: file

OFFICE OF THE MAYOR

Rebecca L. Noah Casper | *Mayor*
Office (208) 612-8235
Fax (208) 612-8560

IDAHO FALLS

The Honorable Mike Simpson
U.S. Congress
2084 Rayburn House Office Building
Washington, DC 20515

Dear Congressman Simpson,

I am writing you in support of the University of Idaho's (UI) funding request to purchase cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative.

Idaho Falls is the 4th largest city in our state and enjoys a dynamic and growing economy. As mayor of the City of Idaho Falls, I have a front row seat for viewing the rapid growth phase our city is in. Our city, state and national economy and safety depends on secure cyberspace and resilient industrial systems, and there is a critical need for a large and highly skilled cybersecurity workforce.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. That is why cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

We enjoy a community that has excellent amenities, low crime, and inexpensive carbon-free power. When I speak to our business community and potential companies looking to relocate their operations to Idaho Falls, one of the topics that repeatedly comes up is workforce development and whether our citizens have the skills to match their needs. There is a critical need to have a cyber trained workforce that can support our increasing digital economy.

I understand that faculty members from multiple Idaho institutions are working together to develop a shared and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. This will provide an immersive hybrid virtual and physical environment training including remote access malware, ransomware, and persistent threat agents.

The UI initiative is a critical step in ensuring that we have a cyber trained workforce. This initiative will provide students in our state with real world training teaching them how to detect and defend against cyber intrusions by using real world immersive processes. Your support would allow these individuals the opportunity to use the very same tools they would in the private or public sector. We want our community and IT professionals ready and effective the moment they enter the workforce.

I believe that this investment will have broad impacts not only to Idaho Falls but our entire state. Please consider this critical request and thank you for continued leadership in Washington.

Should you have any questions, please do not hesitate to call at (208) 612-8235.

Sincerely,

Rebecca L. Noah Casper, Ph.D.
Mayor, City of Idaho Falls

New University of Idaho Robotics Center to Connect Statewide Training Facilities, Fill Labor Gap

August 25, 2022

MOSCOW, Idaho — The University of Idaho College of Engineering has launched the Center for Intelligent Industrial Robotics (CI2R), integrating new robotics research and training labs across the state to prepare students to fill the global manufacturing labor shortage.

The center links recently built statewide robotics training facilities that offer students hands-on experience solving complex robotics problems. CI2R bridges U of I's growing laboratory network through video teleconferencing and broader course availability, expanding education and research opportunities for undergraduate and graduate students across Idaho in cybersecurity, artificial intelligence and industrial automation.

The effort addresses labor shortages in robotics manufacturing, which industry leaders say must be reversed to satisfy rising demand. By 2030, 2.1 million manufacturing positions are estimated to remain unfilled, according to the Manufacturing Institute. The global robotic manufacturing systems market will double by 2026, Business Wire projects.

"We are leading the way to address workforce challenges that impact our state and nation," said Suzanna Long, dean of the College of Engineering. "Continuing our more than 60 years of industry partnerships and 30 years of cybersecurity education leadership, the new center prepares U of I to create a strong workforce that can tackle critical industry needs."

Supported by the Idaho Forest Group, one of America's largest robotic lumber mills, the U of I College of Engineering built a new lab — the Robotics, Automation and Mechatronics Laboratory — on its Moscow campus.

Videoconferencing between the new lab and U of I Coeur d'Alene's Idaho Forest Group Robotics and Automation Laboratory allows center faculty, staff and doctoral students from multiple disciplines to teach students in both locations. Students have direct access to mobile robots, mechanical arms and a variety of simulation equipment in both labs. The Coeur d'Alene lab was built in 2020.

"Through unique laboratory access and faculty mentorship, we're creating a new generation of skilled professionals able to develop complex hardware and software robotics solutions that will strengthen our global industrial manufacturing capabilities within Idaho and nationally," said CI2R Director John Shovic, associate research faculty at U of I Coeur d'Alene.

Engineering students in all disciplines can take courses in advanced robotics, real-time operating systems, industrial computer programming, machine vision, artificial intelligence and data science.

Undergraduate and graduate robotic engineering certificates will be offered in Fall 2023. Robotics course offerings will expand in Moscow and Coeur d'Alene. The labs are expected to be fully usable in all courses by Spring 2023.

Media Note: Courtesy photo and video are available for download in an online gallery. Contact Jodi Walker at jwalker@uidaho.edu for assistance.

—

Media Contacts:

John Shovic
Center for Intelligent Industrial Robotics Director, Research Faculty
208-659-5772
jshovic@uidaho.edu

Gabriel Potirniche
Department of Mechanical Engineering Chair, Professor
208-885-4049
gabrielp@uidaho.edu

Jodi Walker
Senior Director of Communications
208-885-4295
jwalker@uidaho.edu

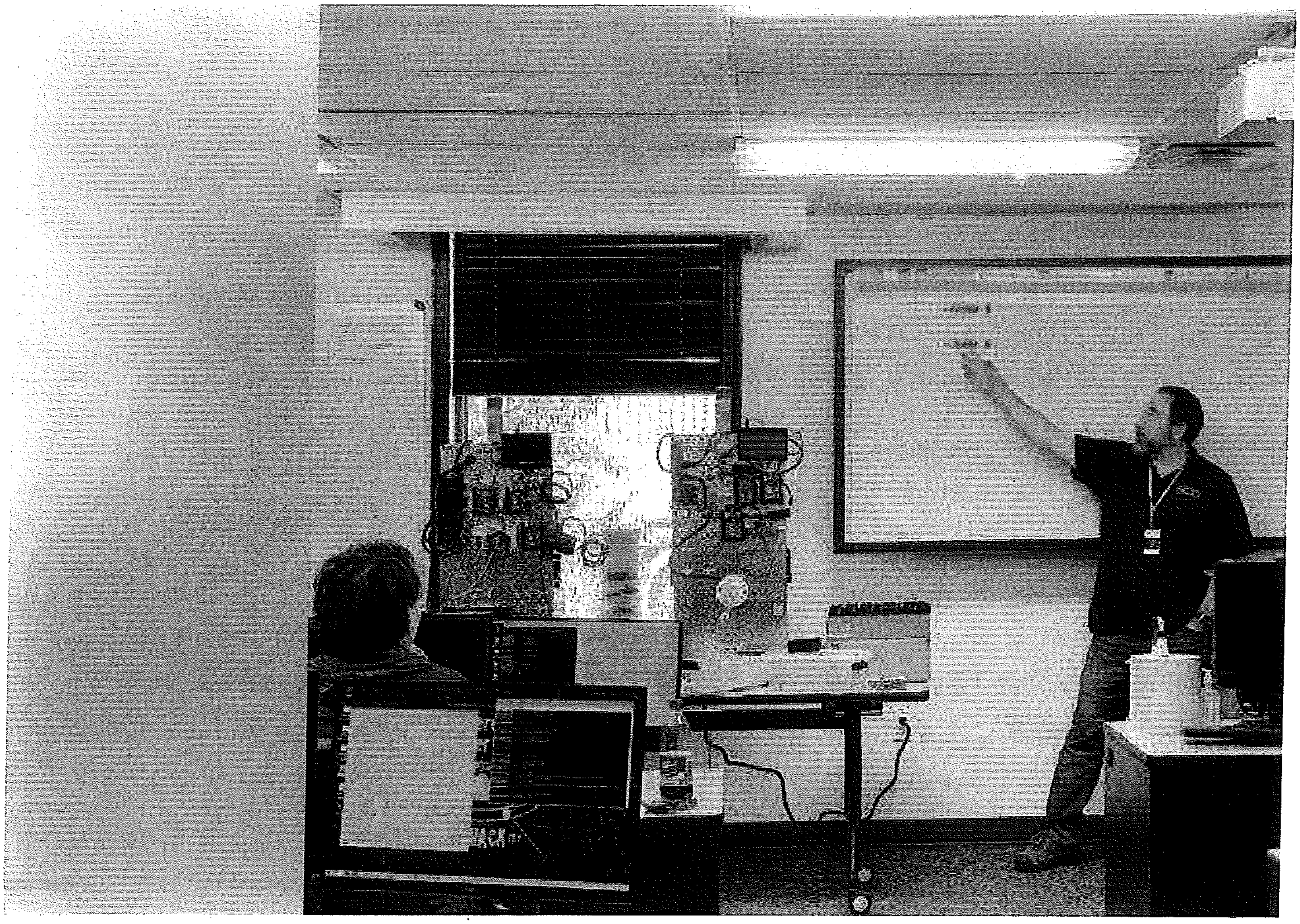
About the University of Idaho

The University of Idaho, home of the Vandals, is Idaho's land-grant, national research university. From its residential campus in Moscow, U of I serves the state of Idaho through educational centers in Boise, Coeur d'Alene and Idaho Falls, nine research and Extension centers, plus Extension offices in 42 counties. Home to nearly 11,000 students statewide, U of I is a leader in student-centered learning and excels at interdisciplinary research, service to businesses and communities, and in advancing diversity, citizenship and global outreach. U of I competes in the Big Sky and Western Athletic conferences. Learn more at uidaho.edu https://www.postregister.com/news/local/more-than-200-attend-idaho-falls-cybersecurity-conference/article_664ec6f2-4666-11ed-a46e-3f8e96e066a2.html

More than 200 attend Idaho Falls cybersecurity conference

By ILEANA HUNTER ihunter@postregister.com

Oct 8, 2022



As of August 2022, there have been more than 750 BSides events around the world, hosted in 205 cities spanning 60 c
held Friday and Saturday.

Ileana Hunter / ihunter@postregister.com

The state's only cybersecurity conference took place Friday and Saturday in the College of Eastern Idaho's Yellowstone Training Center.

The annual conference featured many workshops and speakers, helping a sold-out crowd of over 200 people gain new knowledge and understanding of the cybersecurity world.

The conference, called BSides — Idaho Falls, is part of an international organization. BSides conferences are community driven and run by volunteers in cities across the world. Each host city runs its conference a little differently based on interest and needs in its information security community.

"It's called BSides because when everyone used to use records, the A-side of the record had all the stuff the artist knew the people would like. The experimental, kind of different stuff was all on the B-side," said Ginger Wright, one of the local organizers. "We aren't your average cybersecurity conference, we are different, experimental, new and innovative."

Several people in the Idaho Falls area got together in 2017 to start a local BSides conference because of an ever-increasing interest in information security and cybersecurity.

The conference was run by different groups in previous years, making it difficult to centralize and organize. But this year three local women — Lindsey Cerkovnik, Tiffany Keller and Wright — formed a new nonprofit, the Eastern Idaho Cyber Education Alliance, to ensure the conference can be planned, organized and executed by the same organization. Cerkovnik is the alliance president.

"There is such a big cybersecurity community in Idaho Falls thanks to the (Idaho National) laboratory and different organizations such as Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency," Cerkovnik said. "To us it makes a lot of sense to have an organization that supports cybereducation for the community and gives a place for us all to have a local knowledge and colleague base."

Conference officials found that most of the conferences they had been to featured the same big-name speakers, large companies and overall disconnect among attendees. They wanted their conference to feel local, a place where people could feel a sense of community.

“A lot of the people we have teaching workshops and speaking have amazing things to share,” said Wright, the alliance’s secretary. “We wanted to take local people who wouldn’t normally get a voice and put them where they could be heard.”

The alliance’s mission is to increase opportunities in education for cybersecurity in southeastern Idaho, Cerkovnik said. Cerkovnik has attended some of the largest cybersecurity conferences in the world and said “some of the most innovative and original ideas” she has ever heard come from the BSides conferences.

“This has been a great backbone for the conference which has become so much more popular in the community.”

The conference was sold out online but people continued to show up in person and organizers worked to find them seats.

The conference had workshops on many different aspects of cybersecurity ranging from memory forensics to threat hunting. Participants both listened to and engaged with the presenters, developing an increased knowledge of cybersecurity information and

technology.
Most attendees began their day learning how to pick locks, helping them to understand that even when something seems safe and secure, the point of cybersecurity is to find those spots that look safe but can be bypassed by people who shouldn't be able to do so.

The conference even hosts a "capture-the-flag" exercise leading participants on a Jeopardy-style, digitally created, 16-question quest in which the first person to bypass the firewalls created will win.

BSides, unlike other international cybersecurity organizations, prides itself on offering unique approaches to cybersecurity education and opportunities.

The Idaho Falls event is able to capitalize on its proximity to INL's Cybercore Integration Center and the local Department of Homeland Security office.

"It is quite unusual that a community this small and in a relatively isolated area has this much expertise and support in cybersecurity," said Bri Rolston, a conference volunteer.

"There is so much diversity of skill sets here and getting people in a room and seeing that has been so much fun. You see people start out talking with local industry experts here which evolve into mentorships and then into employment opportunities."

The conference nearly doubled its attendance numbers from last year and is planning on further growth in 2023.

With nearly 700,000 cybersecurity jobs open in the United States, the country needs more people to fill those positions, Wright said.

"In Idaho we often think about jobs that are either agricultural or things like nuclear science, which, let's face it, are out of reach for many of us," Wright said. "These information technology careers we are talking about, with schools like CEI and colleges like University of Idaho and Idaho State University, are absolutely high paying careers available to anyone in Idaho Falls. Conferences like this one can get someone started." "I know people that came to the conference last year that are coming back this year with actual jobs in cybersecurity and they will have gotten that job within the last year."

IDAHO SENATE

Dear Representative Simpson:

As an Idaho State Senator, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique *Adversary as a Service* environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at 208-332-1358.

Sincerely,

Kevin Cook, Senator

GREAT SEAL OF THE STATE OF IDAHO

ESTO PERPETUA

IDAHO SENATE

Dear Representative Simpson:

As an Idaho State Senator, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique *Adversary as a Service* environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at 208-332-1313.

Sincerely,

David Lent, Senator

ROD FURNISS
DISTRICT 31
JEFFERSON, CLARK, FREMONT,
& LEMHI COUNTIES

HOME ADDRESS
346 NORTH 4456 EAST
RIGBY, IDAHO 83442
(208) 589-1100
(208) 332-1056
EMAIL: rfurniss@house.idaho.gov

House of Representatives
State of Idaho

Dear Representative Simpson:

As an Idaho State Senator, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique *Adversary as a Service* environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at 208-589-1100.

Sincerely,

Furniss

Rod Furniss

BOEING

March 3, 2023

Dear Representative Simpson:

As the Commercial Airplanes Director of Systems Product Development for The Boeing Company I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique *Adversary as a Service* environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at (425) 280-9688.

Sincerely,

Joseph Keegan

College of Eastern Idaho

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

2/22/23

Dear Representative Simpson:

As the President of College of Eastern Idaho, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique *Adversary as a Service* environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at 208.850.6707.

Sincerely,

Rick Aman, President
College of Eastern Idaho

C CLOAKED

Dear Representative Simpson:

As the CLOAKED Cybersecurity CEO, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique Adversary as a Service environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at 801.362.8730.

Sincerely,

Kent Orange Warner
CEO

CURTISS -
WRIGHT

March 3, 2023

Curtiss Wright Corporation

1350/1360 Whitewater Drive, Idaho Falls, ID 83402

SUBJECT: Letter of Support for the Idaho Cyber Initiative

Dear Representative Simpson:

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

Cybersecurity is of the utmost concern and importance to powerplants around the world, and as the nuclear industry continues to adapt to the rise and demands of the technology industry by entering the cyberspace, power plants become vulnerable in areas previously shielded from attack. The need for those who can detect and defend against cyber-attacks is vital in keeping the critical infrastructure of powerplants safe. The cybersecurity workforce does not have margins for error nor time for new employees to train and learn how to apply their basic understanding to the workforce. The University of Idaho's Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will give students the opportunity to learn critical applications through an immersive simulation environment. RADICL mimics real-world physical systems and provides simulated attacks that include malware, ransomware, and advanced persistent threat agents. This training is critical to producing a workforce that is ready and effective the moment they leave academia.

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 opportunities created by RADICL will bridge the significant gap between students and cybersecurity professionals, and the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment will greatly benefit Idaho and the cybersecurity community.

Sincerely,

Theresa Sutter

Theresa Sutter, General Manager, Curtiss-Wright

Pacific Northwest
NATIONAL LABORATORY

902 Battelle Boulevard
P.O. Box 999, MSIN J4-45
Richland, WA 99352
(509) 372-5995
david@pnnl.gov
www.pnnl.gov

March 4, 2023

Michael K. Simpson
United States House of Representatives

Dear Representative Simpson,

IN SUPPORT OF THE UNIVERSITY OF IDAHO'S REQUEST FOR INFRASTRUCTURE ALIGNED WITH THE IDAHO CYBER INITATIVE

As the principal cyber security scientist at the Pacific Northwest National Laboratory, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education. The University of Idaho is the state's flagship cybersecurity university.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique Adversary as a Service environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at (509) 372-5995.

Sincerely,

David O. Manz
Principal Cyber Security Scientist
Pacific Northwest National Laboratory

David Manz

CourseOps

The Future of Cybersecurity Education

(801) 368-4691
info@gocourseops.com
https://www.gocourseops.com

March 2, 2023

Dear Representative Simpson:

As the CEO of CourseOps, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique Adversary as a Service environment using real-world physical systems and realistic simulated internet-scale cyber-attacks.

These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment. For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at 801-368-4691.

Sincerely,

Brady Bloxham
Founder & CEO
CourseOps LLC

Dear Representative Simpson:

As a medium size business owner in Southeast Idaho, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique *Adversary as a Service* environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at 208-201-1295.

Sincerely,

Andrew Mickelsen

Mickelsen Farms

Partner

Micron

Dear Representative Simpson:

As the Deputy Chief Security Officer, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique *Adversary as a Service* environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at 208-861-8137

Sincerely,

Samuel Evans, Deputy Chief Security Officer

DRAGOS
1745 DORSEY RD, SUITE R
HANOVER, MD 21076
DRAGOS.COM

MARCH 6, 2023

Dear Representative Simpson,

As the Director of Professional Services at Dragos, I am writing to support University of Idaho's funding request to purchase the cyber-physical systems equipment and private cloud computing equipment necessary for the Idaho Cyber Initiative. Idaho's economy and safety depends on secure cyberspace and resilient industrial systems; hence, there is a critical need for a large and highly skilled cybersecurity workforce. Cybersecurity is a significant component of the Idaho Universities' five-year Strategic Research Plan for Higher Education.

As you are aware, a primary challenge in cyber security education and training is providing real world immersive training to students to teach them how to detect and defend against cyber-attacks using real physical processes, full-scale enterprise IT systems, and internet-scale cyberattacks. This training is critical to producing a workforce that is ready and effective the moment they enter the workforce. Faculty members from multiple Idaho institutions are working together to develop a shared, distributed, and immersive training environment that will integrate researchers, students, and trainees in a controlled live-fire environment unlike any other facility currently available in the United States. The Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) will provide a hybrid virtual and physical environment of enterprise-scale IT systems and bench-top physical process systems under digital control. RADICL will supply a unique *Adversary as a Service* environment using real-world physical systems and realistic simulated internet-scale cyber-attacks. These simulated attacks will include remote access malware, ransomware, and advanced persistent threat agents. This immersive simulation environment is reconfigurable, redeploy-able, and replay-able. This will allow researchers to develop better countermeasures and threat scenarios while allowing students and trainees to learn and adapt from their mistakes in a controlled environment.

For these reasons, we hope that you will support the University of Idaho's community project funding request for cyber-physical systems equipment and private cloud computing equipment. Obtaining this equipment will ensure Idaho can attract and train world class cybersecurity professionals.

Thank you for your consideration of this critical request. If you have any questions, please contact me at 980-621-8499.

Warmest regards,

Jacob Benjamin

JACOB BENJAMIN, PHD, CISSP
DIRECTOR OF PROFESSIONAL SERVICES