INL's Energy Security Initiatives & Cybercore Integration Center

Wayne Austad
Technical Director
Cybercore Integration Center
Wayne.Austad@inl.gov

www.inl.gov

Idaho National Laboratory

INL is a Key Leader in Tomorrow's Energy Future

INL Vision

INL will change the world's energy future and secure our critical infrastructure.

INL Mission

Discover, demonstrate, and secure innovative nuclear energy solutions, other clean energy options, and critical infrastructure.

The Idaho National Laboratory – 70 Years of Groundbreaking Nuclear Energy R&D

Building a New Laboratory

National Reactor Testing Station

1949

Energy Mission – Reactor Science, Safety and Sustainability Solutions

1974

Environmental Management Mission

1997

INEEL & ANL-W combined to create the new Idaho National Laboratory

- Nuclear Energy
- National and Homeland Security
- Energy and Environment

2005

- Advancing Nuclear Energy
- Securing & Modernizing Critical Infrastructure
- Enabling Clean Energy Systems

2019

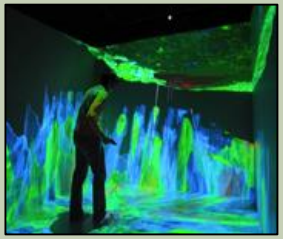
INL's Science & Technology Initiatives for Our Nation's Strategic Energy Security Mission

Strategic Science & Technology Initiatives

Nuclear Energy Competitiveness and Leadership

Integrated Nuclear Fuel Cycle Solutions

Advanced Integrated Energy Systems



Advanced Design and Manufacturing

Secure & Resilient Cyber Physical Systems

Strategic initiatives are built on solid capability foundations to address grand challenges and advance energy and security goals for the nation

World-Leading Control Systems Cybersecurity Capabilities

INL's proven success in R&D, interdisciplinary teams, and deployment of effective solutions

Aurora
A seminal demonstration of cyber-physical effects

Cyber assessment, analysis & training

DHS NCCIC (ICS-CERT)
Red/Blue Training

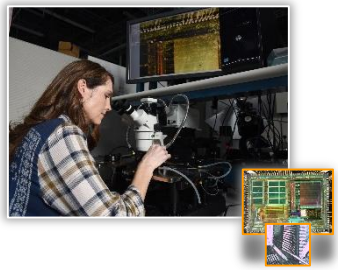
Nexus of electric grid, wireless communications, control systems cyber RDD&D

Control Systems Cybersecurity R&D

Response Support
Ukraine Power Grid

Critical infrastructure resiliency, cyber-informed design and recovery

Nuclear Cybersecurity
Domestic & International



Critical Energy Control Component and System Evaluations
Supply Chain Program

CYBERCORE integration center

Integrate best-in-class science and technology capabilities to balance the nation's R&D portfolio between urgent near term and long term impacts on high consequence systems

Critical National Challenges in Control Systems Cyber

A More Holistic Approach to People, Partnerships, and Technology is Needed

National measure/ countermeasure approach is not sustainable, scalable, or anticipatory

Fundamental science & engineering of cyber challenges are inadequately advanced

R&D and complex solutions require expensive systems and large-scale proving grounds

Technical expertise is in limited supply and mostly consumed in operations

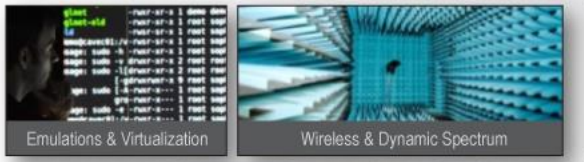
Cybercore Integration Center

Building an Enduring Control Systems Cybersecurity Innovation Capability

Virtual Research Park

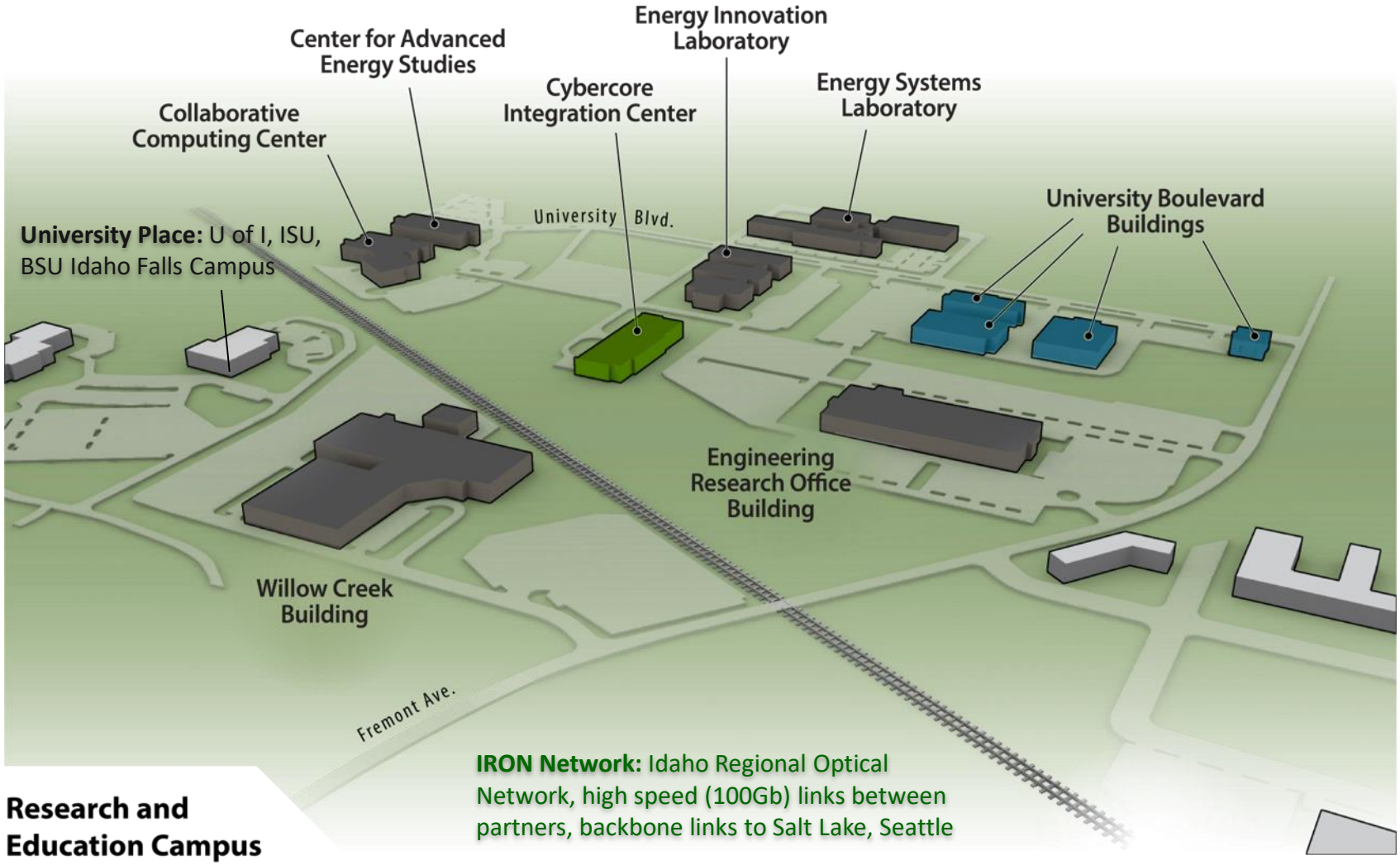
Interdisciplinary Talent Pipeline

Urgent Mitigation REQUIRE **Large Scale Validation** REQUIRE **Transformational R&D**



Expanding the Research & Education Ecosystem

Centers of Gravity for Programs (Cybercore/C3), University R&D (CAES), Education (University Place)
Build an Idaho Ecosystem for "hands-on" collaboration to create new talent and nurture innovation

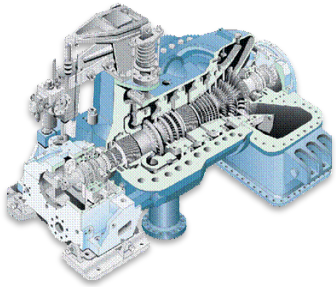
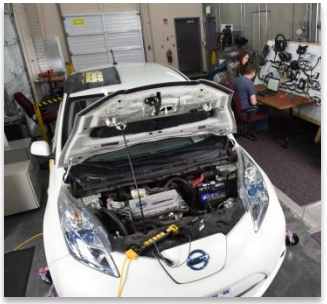
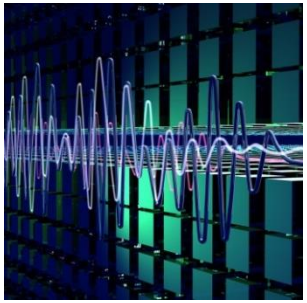


A Spectrum of Technologies and Disciplines is Required

Both are required for Intelligent & Autonomic Systems

Fundamentals of the Engineered Process

Component and System Security

Cyber Informed Engineering	Situational Awareness in OT	Automated Threat Responses & Resilient Systems	Secure Embedded Technologies	Secure & Robust Communications
				
Engineering-based risk analysis, resilient design, & threat disruption devices.	**Identify key monitoring points, new sensors, data & behavior analytics**	**Mitigate exploits before there is an impact, particularly on legacy devices.**	**Innovative mitigations, secure technologies within engineered designs**	**Integrate security based on "physics" of the channel communication**

Risk and Impact Analysis informs focus for R&D

Energy-Cyber Portfolio: R&D, Education for Industry

Consequence-driven Cyber-informed Engineering (CCE)

Mitigate the high impact negative consequences of cyber attack with engineering-based solutions

Cybersecurity for OT Environment (CYOTE)

Monitoring, collecting, and sharing of critical OT cybersecurity indicators for operational assets.

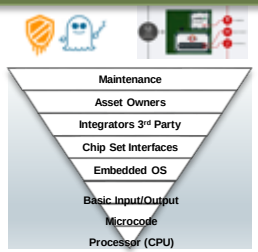
Cyber Analytics Tools & Techniques (CATT)

Developing new analytic tools for OT threat sharing and situational awareness

CyTRICS (Digital Supply Chain)

Finding, mitigating common-mode vulnerabilities in OT components, subcomponents

Firmware Indicator Translation (FIT)



Integrated Binary Analysis tools and environment for embedded systems

M2M Automated Threat Response (MMATR)

Mitigate exploits before impact, incorporating functional limits of legacy devices.

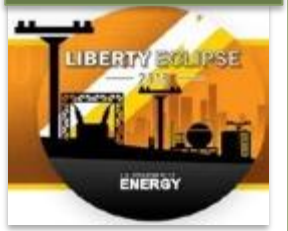
DARPA RADICS

Developing solutions to enable effective and secure restoration of cyber-impacted power grids

Cyber Strike Workshops

Translating real-world cyber events into training to protect US utilities at every step of the OT cyber kill chain

Liberty Eclipse Exercise



Exercises to strengthen the whole of government energy incident response

Cyber Security for Renewable Energy

R&D Roadmap for securing emerging and distributed energy infrastructure from cyber attack

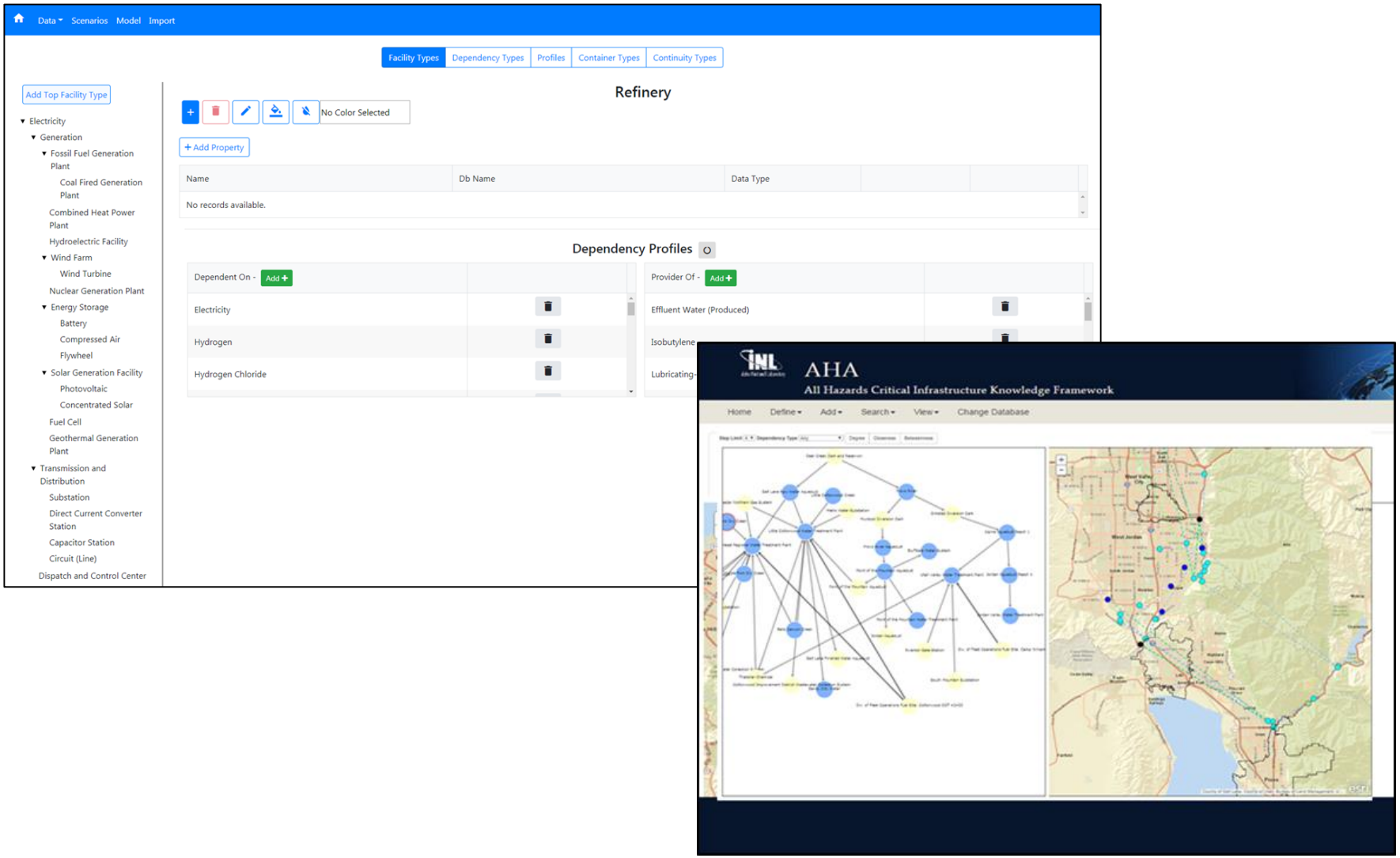
California Energy Systems 2100 (CES-21)

Utility partnerships on common R&D challenges, and validated on actual equip integrated on test range

Structured Threat Intelligence Graph (STIG)

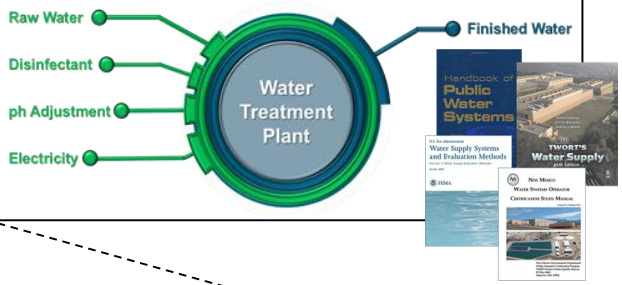
Open Source software to visualize technical threat information shared via STIX / TAXII / JSON code

All Hazards Analysis Framework (AHA)



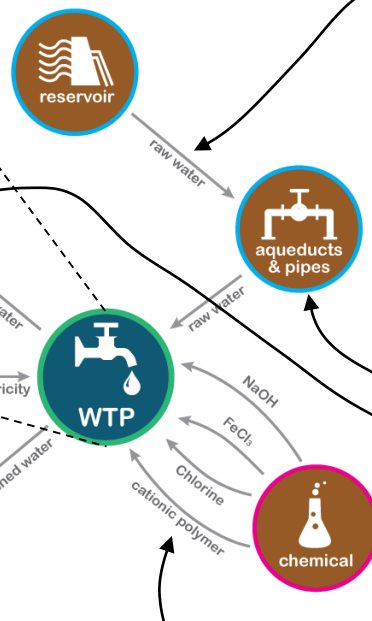
AHA Interdependency Characterization and Data Collection Approach

Dependency Profile:
Engineering Design Principals



Spatial Heuristics

Relationship



Entity Extraction

Attribute Assignment

Structured Data

Cogeneration Plant – Petroleum Refinery Dependency Detection

is_match	ensemble	geo_dist	sim_score	em_class	ref_name	cogen_name
1	40.65	54.16	0.88	6	Chevron - Richmond	Richmond Cogen
1	57.08	76.01	0.77	6	Exxonmobil - Torrance	Torrance Refining Company, LLC
1	65.66	87.45	0.70	2	Western - Gallup	Gallup Refinery
1	91.82	122.34	0.75	6	Par Petroleum - Kapolei (Ewa Beach)	Tesoro Hawaii
1	98.12	130.76	0.81	6	Shell - Puget Sound (Anacortes)	March Point Cogeneration
1	100.77	134.33	0.92	6	Paulsboro Refining	Paulsboro Refinery
1	133.93	178.54	0.91	4	Tesoro - Mandan	Tesoro Mandan Cogeneration Plant
1	140.82	187.73	0.93	6	Ergon - Vicksburg	Ergon Refining Vicksburg
1	142.15	189.37	0.51	5	Phillips 66 - Sweeny	Sweeny Cogen Facility
1	145.92	194.52	0.89	4	Toledo Refining	Toledo Ref Power Recovery Train
1	158.30	210.93	0.62	3	Shell - Deer Park	Shell Deer Park
1	163.58	218.07	0.88	6	Pasadena Refining Systems	PRSI FCC Generator
1	164.74	219.60	0.86	6	Shell - Martinez	Martinez Refining
1	170.54	227.28	0.69	7	Tesoro - Anacortes	March Point Cogeneration
1	187.74	250.27	0.85	4	Valero - Corpus Christi (Avery Point)	Valero Refinery Corpus Christi East
1	187.74	250.55	0.71	6	Wrb - Borger	Black Hawk Station
1	220.14	293.47	0.88	5	Chevron - Kapolei (Honolulu)	Hawaii Cogen
1	239.33	319.03	0.75	8	Exxonmobil - Joliet	ExxonMobil Oil Joliet Refinery

Unstructured Data

Treatment plant power outage means all of Tampa must boil water

By Will Hobson, Jessica Vander Velde and Richard Danielson, Times staff writers
Friday, February 22, 2013 2:44pm

TAMPA — A rodent, most likely a squirrel, chewing on a [illegible] Friday morning caused a power failure that led to an unprecedented [illegible] for 560,000 people and businesses and left them scrambling [illegible] weekend.

RELATED NEWS/ARCHIVE

Power outage zaps traffic lights in New Tampa
2 Months Ago

North Tampa power outage disables traffic lights
6 Months Ago

Firefighters patch toxic gas leak at water treatment plant; no injuries reported
7 Months Ago

The effects were [illegible] disappeared under [illegible] each other in line [illegible] And residents acr[illegible] notice affected the [illegible] their tap water.

Until Monday mo[illegible] should boil any [illegible] fruits or vegetable[illegible] minute. This affe[illegible] 100,000 of them [illegible] Tampa.

Relationship

Institutional Approach to Academic Partnerships

The Pace & Innovation for Infrastructure Security Challenges Demand Unconventional Collaborations

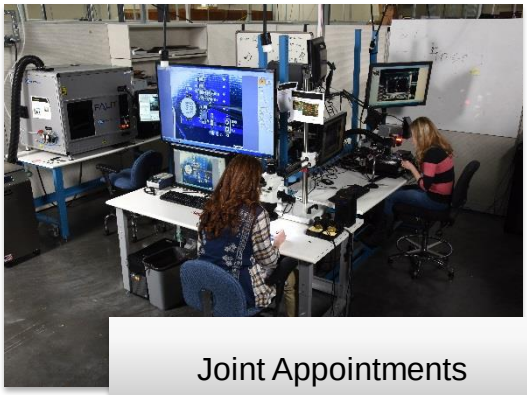
INL National University CONSORTIUM

INL Contract

CAES Center for Advanced Energy Studies

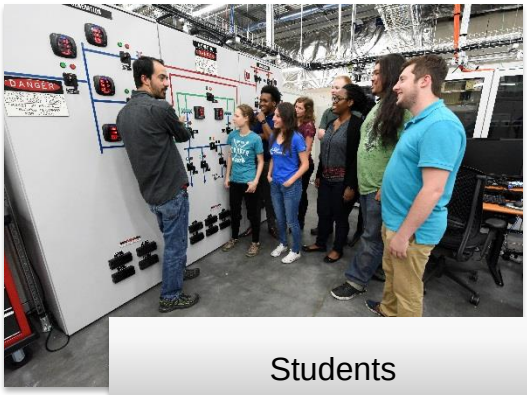
Regional Partners

Strategic University Partnerships for Education & Research



Joint Appointments

Researchers



Students

Strategically align interdisciplinary programs, with hands-on collaboration on hard national challenges, to enable the innovation and excitement that accelerates national talent pipelines.

Idaho Research & Education Ecosystem

Re-Imagine Our Education Institutions & Partnerships

- **Exchange of scientific and engineering information, results, and methods across Idaho's colleges and universities leveraging unique talents and avoiding duplication.**
- **Virtual integration of university, college, and/or INL lab facilities and demonstration environments facilitating a new multi-disciplinary approach to education.**
- **Joint national grand challenge R&D projects and proposals that could generate additional funding as well as faculty and student excitement.**

Idaho National Laboratory

BOISE STATE UNIVERSITY

CAES Center for Advanced Energy Studies

University of Idaho

Idaho State University

CyberStart and Cyber FastTrack: Learning Games

Gov. Little, INL, & STEM Action Center

CyberStart = High Sch FastTrack = College

No prior experience required, 300 hrs of game learning

27 States in Game

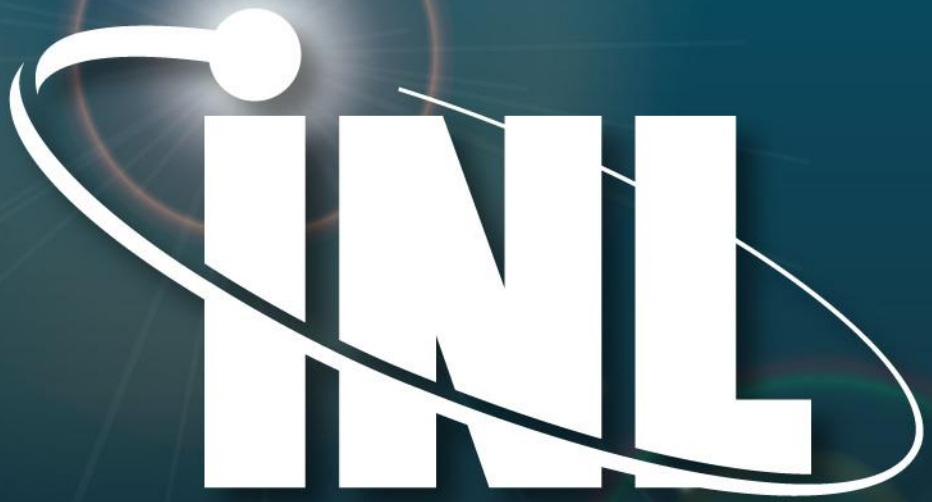
165 Idaho Students, 5th/capita (as of 4/27)

$2.5M scholarships for SANS Courses, College

INL, Cisco, Vanguard, Fannie Mae

https://www.cyber-fasttrack.org/
(Sign up until May 10, 2019)

"The nation desperately needs more highly-skilled cyber professionals, and we have evidence that CyberStart improves the quality and preparation of people entering the cybersecurity industry." – Allan Paller



Idaho National Laboratory

Cybercore Integration Center's Mission

Address the most critical control systems challenges that require a national collaborative, inter-disciplinary environment

Drive a national R&D agenda
that creates a balanced portfolio between urgent and long-term challenges.

Partner at a grand level
to enable capabilities and impacts across the nation.

Accelerate workforce development
for control system cybersecurity talent.

An Enduring Control Systems Cybersecurity Innovation Capability

17

The National Workforce Capability Gap

Why is a national lab involved? …

- Actionable threat analysis and information sharing
- High quality and immediate incident response
- Innovative R&D and validation for deployable, long-term solutions
- Cyber-informed and advanced technology education
- Relevant training and performance-based competency in education

Specialized expertise to address control systems cybersecurity threats is less than 10%* of national need

A multidimensional, long-term approach is needed:

- Hands-on experiences
- Initial competency & refresh
- Professional teams
- Critical Thinking

*INL's insight gained from the many requests for expertise from U.S. Government and private sector leads to this estimation.