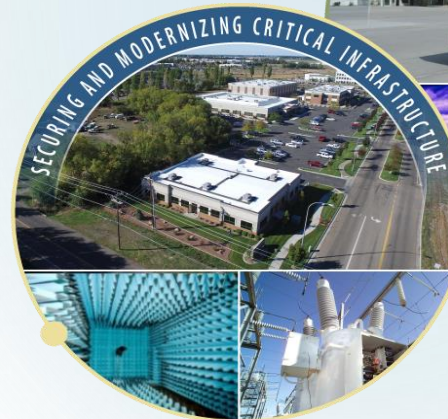


INL's Energy Security Initiatives & Cybercore Integration Center

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



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.

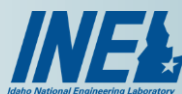
INL Mission

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

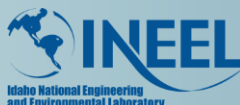


The Idaho National Laboratory – 70 Years of Groundbreaking Nuclear Energy R&D

National Reactor Testing Station



Energy Mission – Reactor Science, Safety and Sustainability Solutions



Environmental Management Mission

Building a New Laboratory



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

Nuclear Energy

National and Homeland Security

Energy and Environment

Advancing Nuclear Energy

Securing & Modernizing Critical Infrastructure

Enabling Clean Energy Systems



1949

1974

1997

2005

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

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

Critical infrastructure resiliency, cyber-informed design and recovery

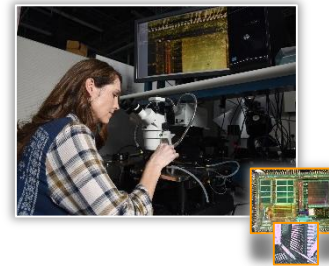


Nuclear Cybersecurity
Domestic & International

Aurora
A seminal demonstration of cyber-physical effects



Response Support
Ukraine Power Grid



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

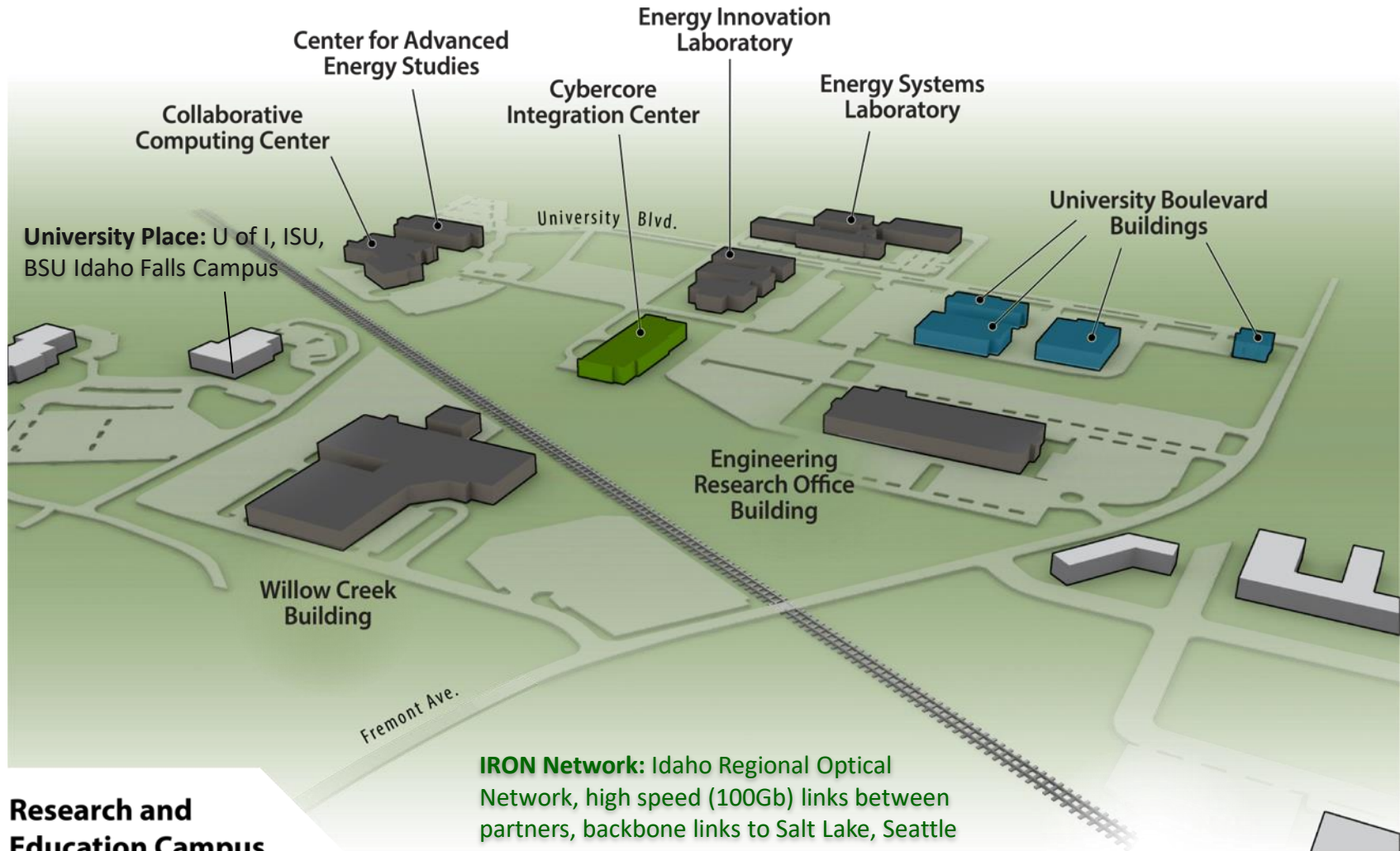
◀ REQUIRE

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*



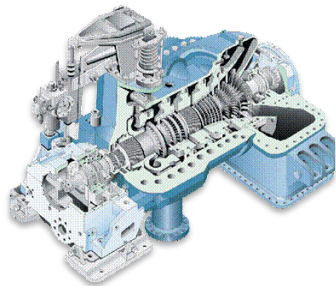
A Spectrum of Technologies and Disciplines is Required

Both are required for Intelligent & Autonomic Systems

Fundamentals of the Engineered Process

Component and System Security

Cyber Informed Engineering



Engineering-based risk analysis, resilient design, & threat disruption devices.

Situational Awareness in OT



Identify key monitoring points, new sensors, data & behavior analytics

Automated Threat Responses & Resilient Systems



Mitigate exploits before there is an impact, particularly on legacy devices.

Secure Embedded Technologies



Innovative mitigations, secure technologies within engineered designs

Secure & Robust Communications



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)



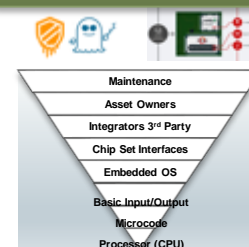
Developing new analytic tools for OT threat sharing and situational awareness

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)

[Data](#)
[Scenarios](#)
[Model](#)
[Import](#)

[Facility Types](#)
[Dependency Types](#)
[Profiles](#)
[Container Types](#)
[Continuity Types](#)

Add Top Facility Type

Electricity

Generation

Fossil Fuel Generation Plant

Coal Fired Generation Plant

Combined Heat Power Plant

Hydroelectric Facility

Wind Farm

Nuclear Generation Plant

Energy Storage

Battery

Compressed Air

Flywheel

Solar Generation Facility

Photovoltaic

Concentrated Solar

Fuel Cell

Geothermal Generation Plant

Transmission and Distribution

Substation

Direct Current Converter Station

Capacitor Station

Circuit (Line)

Dispatch and Control Center

Refinery

+

+

+

+

+

No Color Selected

+ Add Property

Name	Db Name	Data Type
No records available.		

Dependency Profiles

Dependent On -

Add +

Electricity

Hydrogen

Hydrogen Chloride

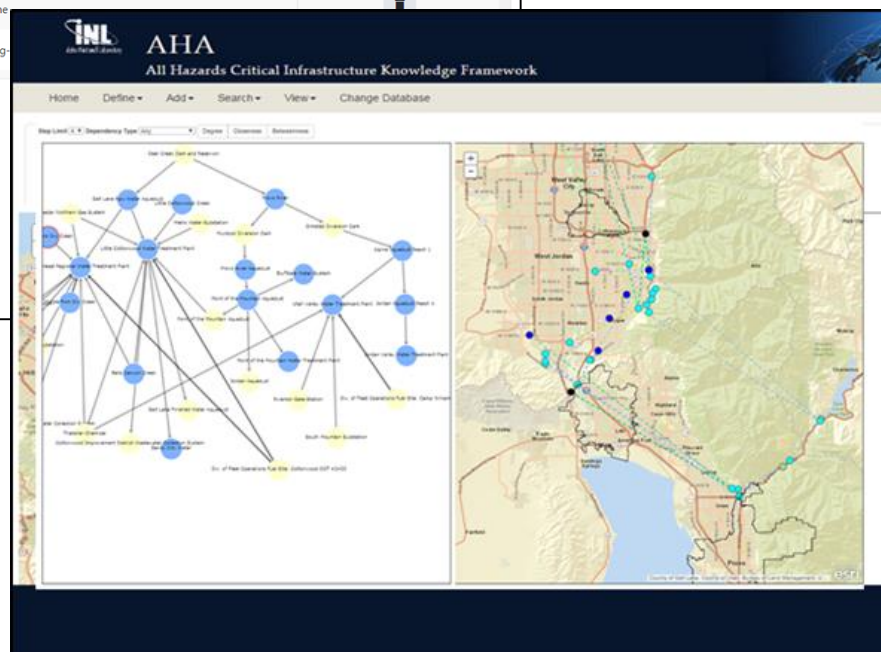
Provider Of -

Add +

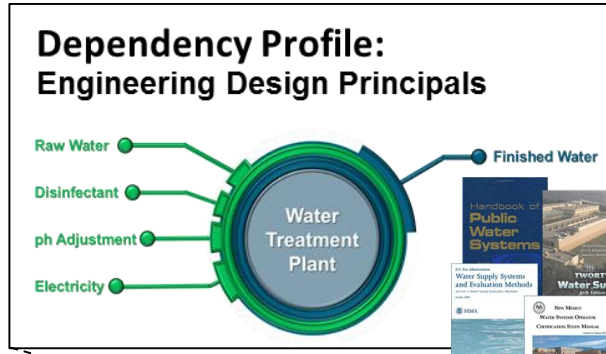
Effluent Water (Produced)

Isobutylene

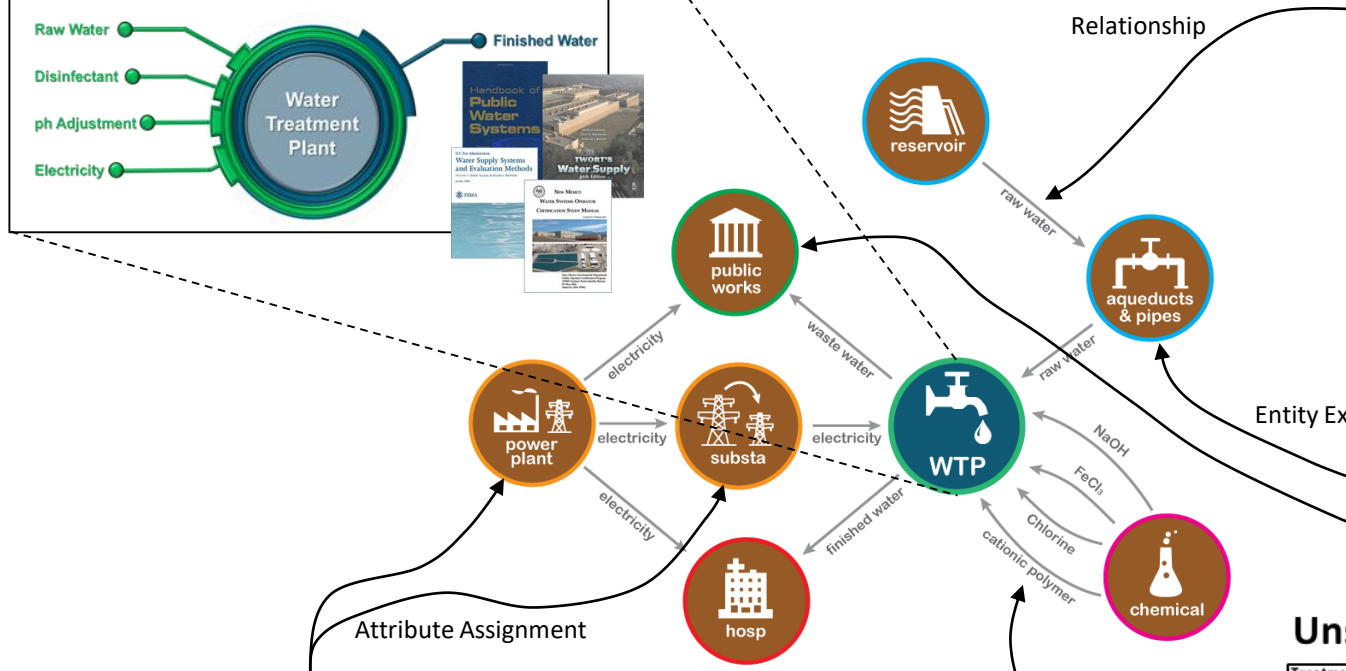
Lubricating



AHA Interdependency Characterization and Data Collection Approach



Spatial Heuristics



Entity Extraction

Relationship

Structured Data

UTILITY_ID	PLANT_CODE	PLANT_NAME	STREET_ADDRESS
1	7	10867 Tate & Lytle Decatur Plant Cogen	2200 East Eldorado St
2	8	50983 Saginaw Cogeneration	2246 Saginaw Parkway North
4	20	55454 AES Cypress LLC	
6	21	13671 AES Shady Point LLC	PO Box 1748
8	25	2527 AES Greenwood LLC	580 Plant Road
9	34	3205 Rocky River	146 Power Dam Lane
10	35	13678 AES Wisconsin Run Cogeneration Facility	11600 Mexico Farms Rd. S.E.
11	39	2529 AES Hickling LLC	11884 Hickling Rd
12	40	55788 Hospice Inc	2400 Wildcat Avenue
13	42	15675 AES Themes	141 Depot Road
14	46	55611 AES Hoylake LLC	
15	52	10002 ACE Cogeneration Facility	12801 Marjorie St.
16	60	55636 St. Joseph County Generating Facility	
17	65	50249 Azalea Consolidated Lufkin	2301 Hwy 103 East
18	67	10819 Adu Cogeneration LP	2575 Fulton Street East
19	84	6390 Tanger	4463 Janders Rd
20	84	6391 Smith Island	29877 Cabela Jones Rd
21	88	55170 Granite Ridge	21 North Wainwright Avenue
22	109	10223 AG Processing Inc	508 N Commercial
23	114	55453 Adia Energy Center	

Cogeneration Plant – Petroleum Refinery Dependency Detection

is_match	ensemble	geo_dist	sim_score	em_class	ref_name	cogen_name
1	40.65	34.18	0.88	8	Cherwon - Richmond	Richmond Cogeneration
1	57.06	76.01	0.77	6	ExxonMobil - Torrance	Torrance Refining Company, LLC
1	65.66	87.45	0.70	2	Western - Gallup	Gallup Refinery
1	92.82	222.34	0.79	8	Par Petroleum - Kapolei (Ewa Beach)	Tosco Hawaii
1	98.12	130.76	0.81	6	Shell - Puget Sound (Anacortes)	March Point Cogeneration
1	100.77	134.33	0.82	6	Paulsboro Refining	Paulsboro Refinery
1	119.89	176.54	0.81	4	Tosco - Mandan	Tosco Mandan Cogeneration Plant
1	140.82	187.73	0.83	6	Engen - Visalia	Engen Refining Visalia
1	142.15	188.37	0.51	5	Phillips 66 - Sweeny	Sweeny Cogeneration
1	146.82	284.52	0.89	4	Tosco Refining	Tosco Ref Power Recovery Train
1	158.80	255.93	0.62	8	Shell - Deer Park	Shell Deer Park
1	163.58	228.07	0.88	6	Pasadena Refining Systems	PSR FCC Generator
1	164.76	259.40	0.86	6	Shell - Martinez	Martinez Refining
1	170.54	227.28	0.69	7	Tosco - Anacortes	March Point Cogeneration
1	187.74	292.27	0.85	4	Valero - Corpus Christi (Avery Point)	Valero Refining Corpus Christi East
1	187.76	292.55	0.71	6	Wile - Sanger	Black Hawk Refinery
1	220.14	295.47	0.86	6	Cherwon - Kapolei (Honolulu)	Hawaii Cogeneration
1	238.33	318.03	0.73	8	ExxonMobil - Joliet	ExxonMobil Oil Refinery

Unstructured Data

Treatment plant power outage means all of Tampa must boil water

By MIC Robison, Jessica Vander Vliet and Richard Davidson, Times staff writers
Friday, February 27, 2015 2:44pm

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

The effects were not limited to the city of Tampa. The outage affected other parts of the state, including Orlando and Jacksonville. The outage was caused by a power line that was damaged by a squirrel. The outage was the largest in the state's history.

Until Monday morning, residents in the city of Tampa should boil any tap water for at least one minute before drinking it. The city of Tampa is advising residents to boil their tap water.

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

2 Minutes Ago

North Tampa power outage disables traffic lights

4 Minutes Ago

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

2 Minutes Ago

Institutional Approach to Academic Partnerships

The Pace & Innovation for Infrastructure Security Challenges Demand Unconventional Collaborations



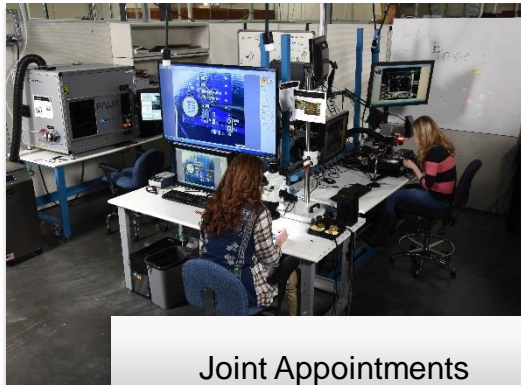
INL Contract



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

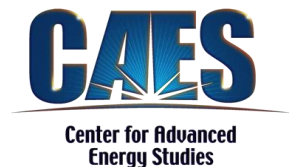
- **Exchange of scientific and engineering information**, results, and methods across Idaho's colleges and universities leveraging unique talents and avoiding duplication.
- **Virtual integration of university, college, and/or INL** lab facilities and demonstration environments facilitating a new multi-disciplinary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



University of Idaho



Idaho State
UNIVERSITY



CyberStart and Cyber FastTrack: Learning Games

cyber fasttrack

There is a shortage of cybersecurity experts in the US

Data and network breaches happen so often, it has become a question of 'when', not 'if', an organization will face their next security challenge. Cybersecurity professionals now hold some of the most critical roles in the modern workplace.

Cyber FastTrack is helping to address this shortage by exposing undergraduate and graduate students to exciting career opportunities in cybersecurity, as they develop in-demand technology skills. This free course is delivered completely online so students can complete it alongside other educational programs.

"We no longer look for people with cybersecurity degrees. We now hire cyber people if they have hands-on mastery of networking and Python and Linux and other essentials of applied computer science. Without those skills they are useless in technical roles."
- CISO, Silicon Valley Giant

Have you got what it takes?

Designed by experts in the field, Cyber FastTrack provides an unprecedented opportunity for you to quickly kick start a career in cybersecurity. It consists of three stages, each featuring a series of increasingly difficult digital challenges.

No computer science experience is required to get started! The most successful students from each stage will be invited to advance to the next stage of the program.

Here's how it works:

1.

**cyberstart
assess**

First, discover if you have the raw talent, problem-solving skills, and key characteristics to excel as a cybersecurity professional.

2.

**cyberstart
game**

Next, tackle more than 200 real-world challenges as you learn how to identify security flaws, uncover a cyber criminal's digital trail, and more.

3.

**cyberstart
essentials**

Finally, build on the foundational skills developed during Assess and Game while working through hands-on exercises, quizzes, interactive labs, and exams.

Top-scoring participants will win **scholarships** to advanced cybersecurity courses, where they will earn industry-respected certifications from the SANS Institute, the world leader in cybersecurity education and research.

Learn more at:
www.cyberft.io/student
@CyberFastTrack

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



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

The National Workforce Capability Gap

Why is a national lab involved? ...

Actionable threat analysis and information sharing

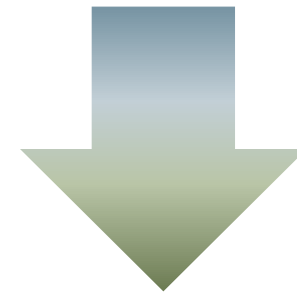
High quality and immediate incident response

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.