

Eleanor Taylor
Workforce Development Program Office
September, 2023

Accelerating Industrial Cybersecurity Workforce Development

National & Homeland Security

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552).
Exemption number and category: Exemptions 4 and 7.
Commercial/Proprietary, Law Enforcement Information,
Department of Energy review required before public release
Name/Org: S. D. Holstein, INL Chief Science Officer
Date: 08/25/2021, Guidance (if applicable): N/A

INL Idaho National Laboratory

OFFICIAL USE ONLY

1

U.S. Department of Energy National Laboratories

- Idaho National Laboratory**
Idaho Falls, Idaho
- National Renewable Energy Laboratory**
Golden, Colorado
- Argonne National Laboratory**
Argonne, Illinois
- Fermi National Accelerator Laboratory**
Batavia, Illinois
- Ames Laboratory**
Ames, Iowa
- National Energy Technology Laboratory**
Morgantown, West Virginia
Pittsburgh, Pennsylvania
- Brookhaven National Laboratory**
Upton, New York
- Princeton Plasma Physics Laboratory**
Princeton, New Jersey
- Thomas Jefferson National Accelerator Facility**
Newport News, Virginia
- Savannah River National Laboratory**
Aiken, South Carolina
- Oak Ridge National Laboratory**
Oak Ridge, Tennessee
- Los Alamos National Laboratory**
Los Alamos, New Mexico
- Sandia National Laboratory**
Livermore, California
Albuquerque, New Mexico
- Lawrence Livermore National Laboratory**
Livermore, California
- Lawrence Berkeley National Laboratory**
Berkeley, California
- SLAC National Accelerator Laboratory**
Menlo Park, California
- Pacific Northwest National Laboratory**
Richland, Washington

IDAHO NATIONAL LABORATORY

2

INL's Vision – To change the world's energy future and secure our nation's critical infrastructure.

Energy security is national security.

America's prosperity, freedom and ability to advance is inextricably linked to our resources and infrastructure. At INL, dedicated professionals defend these systems from cyber and physical threats, unauthorized intrusions and disruptions.

Protecting the nation's energy systems including the power grid, oil and gas pipelines, and renewable technology from physical or cyberthreats is one of our most important missions.

IDAHO NATIONAL LABORATORY

3

National and Homeland Security Mission Focus Areas



Solving security challenges in critical infrastructure protection and resiliency, nuclear and radiological security, and national defense.

IDAHO NATIONAL LABORATORY

4

Mission: Industrial Control System Security



Innovating and applying control-system cybersecurity solutions

- Integrating Government, Academia, & Industry
- Integrating Analysts, Engineers, & Computer Scientists
- Threat, Vulnerability, & Consequence Analysis
- Design and Engineering Culture Change
- Workforce, Training Development and Delivery

IDAHO NATIONAL LABORATORY

5

INL National & Homeland Security Directorate Workforce Development Program Office

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



- Drive a culture change in engineering**
Increase cybersecurity of systems deployed and under development
- Enhanced partnerships**
Advance control systems cybersecurity gaps
- Accelerate workforce development**
Support demand for control system cybersecurity talent

IDAHO NATIONAL LABORATORY

6

National Workforce Capability Gaps

Over 3 million unfilled cybersecurity jobs globally in 2023
 – *Cybersecurity Ventures*

Over 8 trillion In damages expected from cybercrime in 2023
 – *Cybersecurity Ventures*

Over 90% national control systems cybersecurity workforce needs are NOT being met.
 – *CyberSeek*

Key areas of focus:

- Innovative R&D and proactive validation for long-term solutions
- High quality and immediate incident response and forensics
- Actionable threat analysis, situational awareness, and information sharing
- Cyber-informed and advanced technology education
- Hands-on training and applicable skills from education

IDAHO NATIONAL LABORATORY

7

National Imperative – Defend Critical Infrastructure

- Expanding the use of minimum cybersecurity requirements in critical sectors
- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services
- Defending and modernizing Federal networks and updating Federal incident response policy

NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY

Unleashing America's Cyber Talent

JULY 31, 2023

OFFICE OF THE NATIONAL CYBER DIRECTOR
 EXECUTIVE OFFICE OF THE PRESIDENT

THE WHITE HOUSE

IDAHO NATIONAL LABORATORY

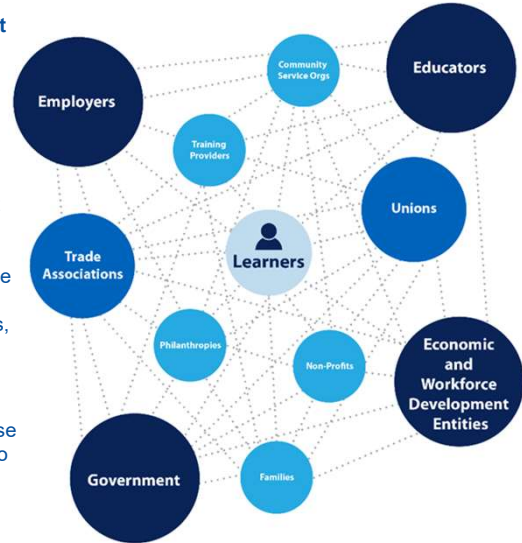
8

Adapting an Ecosystem Approach



Cyber Education and Workforce Development Ecosystems

- Stakeholders may include: learners (students, job seekers, and employees), employers, educators, trainers, government at all levels, trade associations, unions, economic and workforce development entities; non-profit organizations, civil society organizations, philanthropies
- Ecosystems take diverse forms; must be suited to specific local, regional, functional needs



9

Information Technology (IT) and Operational Technology (OT)



Information Technology



Operational Technology

	Information Technology	Operational Technology
Being controlled	Data	Physics
Measurement	Bits and bytes	Temperature, pressure, flow
Lifecycle	System lifecycle	Facility lifecycle
Consequences	Competitive disadvantage Embarrassment Financial loss	Product damage Loss of life Environmental release
Desired system characteristics	Confidentiality Integrity Availability	Safety Reliability Functionality
Educational background	Computer Science Information Systems Cybersecurity	On the job Career & Technical Education Electrical Engineering
Reporting chain	ISO CISO CIO	Shift Supervisor Plant Manager COO
Managerial accounting	Cost center	Profit center

10

Accelerating Cyber Workforce Development

The National & Homeland Security Directorate at Idaho National Laboratory is creating models & pilots to address national workforce development needs

<https://inl.gov/national-security-training/>

Advancing our talent pipeline thru core R&D partnerships and educational opportunities


- Cybercore Integration Center Academic Collaboration Laboratory
- DOE CyberStrike Training
- CISA Training/Curriculum Sharing
- ICS Community of Practice
- Cyber CHAMP
- OT Defender Fellowship
- Consequence-driven Cyber-informed Engineering and Cyber Informed Engineering
- Internships, Apprenticeships, Fellowships & Joint Appointments
- STEM Education & Outreach – Shareable Learning Modules

IDAHO NATIONAL LABORATORY

11

Cybercore Academic Collaboration Laboratory

- **Partner** to advance control systems cybersecurity
- **Deliver** on commitments to strengthen education ecosystems and build talent pipelines
- **Access** to collective resources and equipment
- **Exchange** of scientific and engineering information and collaboration
- **Align** interdisciplinary programs to address national challenges
- **Share** curriculum across partners and develop a collective body of knowledge for students



IDAHO NATIONAL LABORATORY

12

Cyber-Informed Engineering (CIE)

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to “engineer out” cyber risk** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to engender a **culture of security** aligned with the existing industry safety culture.
- CIE Implementation Guide just released: <https://www.osti.gov/biblio/1995796>



IDAHO NATIONAL LABORATORY

13

DOE CyberStrike Training

- Open-Source Intelligence
- Denial of Service
- Passive Man in the Middle Attack
- Firmware Analysis
- Controlling the Human Machine Interface
- Bypassing the Human Machine Interface
- Active Man in the Middle Attack
- Defender Mitigations



IDAHO NATIONAL LABORATORY

14

CISA Training Courses Available to Attend – No Cost

- **Two Primary Formal Course:**
 - ICS 301L (Red/Blue): ICS Evaluation – Basic
 - ICS 401L : ICS Evaluation – Intermediate/Advanced
- **Two Virtual Training Courses:**
 - ICS 301V: Prerequisite to attending the 301L
 - ICS 401V: Prerequisite to attending the 401L
- **Other ICS Training Available:**
 - 13 Online ICS Training Modules
 - Regional (Mobile) Training Course (four-day course)
 - 101 - Basic Overview of ICS Cybersecurity
 - 201 - Intermediate ICS Cybersecurity Training
 - 202 Intermediate ICS Cybersecurity Hands-on Training
 - Incorporating Menu-Driven Training
 - Incorporating TTXs



Virtual Capabilities using NetLabs


IDAHO NATIONAL LABORATORY

15

Industrial Control System (ICS) Collaboration

Industrial Cybersecurity Community of Practice (ICSCOP)

- Consists of over 350+ participants nationwide and 23+ countries from industry, academia, and government with bi-annual public workshops
- Sub-group committees and meetings on workforce development, education standards and cyber informed engineering
- Demonstrate research results at national scale



IDAHO NATIONAL LABORATORY

16

Understanding the Cyber Workforce Development Gap and Business Risk

Asked by DHS in 2018 to research these issues, INL has:

- Created an Industrial Cyber Community of Practice in 2020
- Conducted 5 years of foundational research
- Performed workforce development evaluations across industries, sectors and regions

Major discovery: **This is not a cyber issue, this is a business strategy issue**

INL's Research Response ~ The creation of a process, framework, and tool that can:

Step 1



Assess cyber "health" and "maturity"

Step 2



Identify most effective organizational cyber structure

Step 3



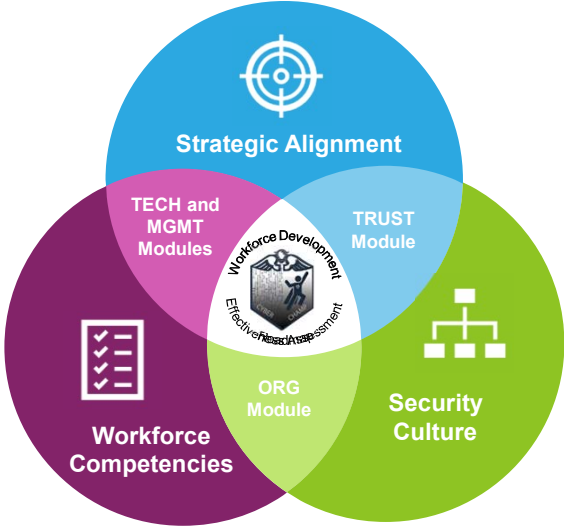
Determine competency-based training needs and recommendations

IDAHO NATIONAL LABORATORY

17

Cyber Competency Health and Maturity Progression Model (Cyber-CHAMP®)

- Develop cybersecurity workforce trends by sector
- Determine what curriculum needs to be developed of local businesses and municipalities
- Create cyber risk dashboards and meet with insurance companies to identify ROI



IDAHO NATIONAL LABORATORY

18

Operational Technology Defender Fellowship

Offered by DOE to middle to senior-level OT security managers in the U.S. energy sector:

- Provides an opportunity to understand cyber strategies
- Allows for discovery of tactics, techniques, and procedures (TTPs) adversary's use
- Foundation for ongoing skill sets to protect the nation's energy infrastructure

Objectives:

- Provide increased understanding of adversarial cyber threats
- Provide awareness of the U.S. energy infrastructure cyber defensive strategy
- Develop/discuss strategies to organize, consume, and operationalize tactical information
- Build/enhance relationships between energy sector and gov cybersecurity managers
- Equip Fellows with strategies, actionable information & connections




Operational Technology Defender Fellowship

19

IDAHO⁹NATIONAL LABORATORY

19

Consequence-driven Cyber-informed Engineering (CCE)



Changing the way engineers, operators, & senior leaders understand & mitigate the risks of cyber-enabled sabotage against their most critical systems & processes

1. Where to start?
2. How is everything digitally connected?
3. Where are the controls systems vulnerable
4. Eliminate the cyber risk

Think Like the Adversary

20

IDAHO NATIONAL LABORATORY

20

Investing in the Future

INL actively gives back to the community by supporting several ICS workforce development programs

N&HS Cybersecurity Expertise & Research Areas

- Cybercore Integration Center
- Critical Infrastructure, Security and Resilience

Related Programs and Opportunities:

- Adjunct Faculty and Invited Speakers
- Faculty Researchers
- Internships
- Practicums
- STEM Education and Outreach



Girls Go Cyberstart National Competition

IDAHO NATIONAL LABORATORY

Opportunities and Collaborations

- **Leverage existing training**
 - DHS CISA Virtual Learning Portal
 - DOE CyberStrike Training
- **Explore tool and assessment capabilities**
 - Cyber CHAMP
 - Cybersecurity Self Evaluation Tool – CSET
 - MALCOM - Promotes critical thinking skills
 - ICS All Hazards Analysis
 - <https://inl.gov/critical-infrastructure-protection/>
- **Partner and participate**
 - ICS Community of Practice - <https://inl.gov/icscop/>
 - Cyber Informed Engineering Working Groups – www.inl.gov/cie/
 - K-12 Education and Outreach
 - Government, Academia and Industry forums



IDAHO NATIONAL LABORATORY

