

January 27, 2021

**Ron Fisher**

Director, Infrastructure Assurance and Analysis Division



# Idaho National Laboratory Physical Infrastructure Analysis Support to the U.S. Department of Homeland Security

# Overview

- INL continues to support the U.S. Department of Homeland Security (DHS) in carrying out their cybersecurity mission
- Highlighted Focus Areas:
  - Cyber Workforce Development
  - COVID-19 Response
  - All Hazards Analysis (AHA)
  - Infrastructure Playbook
  - Election Security
  - Operation Warp Speed (OWS)

**INL is the top DHS-funded U.S. Department of Energy (DOE) National Laboratory**

**FY20: INL recognized for critical role in supporting DHS's efforts to enhance the security and resilience of industrial control systems (ICS) and critical infrastructure**

92

## RESEARCH AND DEVELOPMENT (in thousands of dollars)

	Fiscal year 2019 enacted	Fiscal year 2020 budget request	Committee recommendations
Cybersecurity	4,695	24,091	3,000
Infrastructure Security	3,216	1,216	1,216
Integrated Operations	5,215	5,215	5,215
Subtotal, Research and Development	13,126	30,522	9,431

## CYBERSECURITY

The fiscal year 2020 budget request proposes an increase of \$19,396,000 for CISA cybersecurity R&D while concurrently reducing S&T cybersecurity research by \$24,091,000 compared to the fiscal year 2019 enacted level. The Committee rejects this shell game

The Committee recognizes the critical role of Idaho National Laboratory [INL] in supporting the Department's efforts to enhance the security and resilience of industrial control systems and critical infrastructure. INL currently supports a variety of CISA requirements, including the technical evaluation of cyber-physical disruptions and the identification of infrastructure dependencies. The Committee believes CISA can further utilize the expertise of the lab to help identify both tactical and strategic risks that could disrupt National Critical Functions, including Supplying Water, through the INL's water security testbed and All Hazards Analysis framework. The diversity of capability present at INL can also allow CISA to assess and analyze a range of other cross-sector risk areas, such as shared cross-sector pipeline industrial control systems vulnerabilities. The Committee includes \$3,000,000 above the request for CISA to leverage INL's water security testbed and All Hazards Analysis framework to support these critical objectives.

areas, such as shared cross-sector pipeline industrial control systems vulnerabilities. The Committee includes \$3,000,000 above the request for CISA to leverage INL's water security testbed and All Hazards Analysis framework to support these critical objectives.





# Future Directions: Idaho Cyber Project

Customized solution for government entities and private sector businesses

## Expected Project Results:

- Skills testing resources
- Clear path to identify education/skills needed for the various cyber career fields
- Assist businesses with access to employer-driven educational opportunities
- Identifying cybersecurity training needs for existing employees
- Create centralized location for sharable cybersecurity curriculum
- Assist academia to visualize and tailor curriculum to meet employer's needs

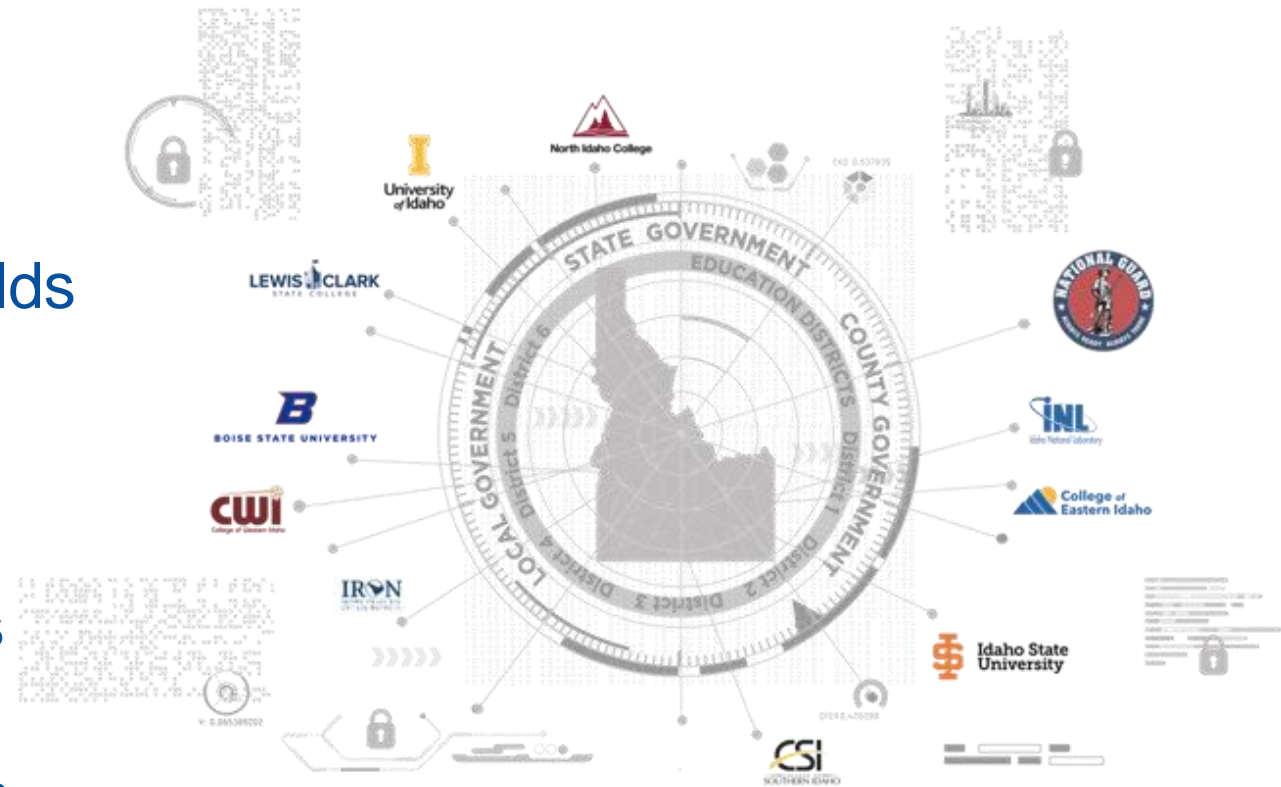


Image Credit: BSU Cyberdome Logo

# COVID-19 Response Overview

## Direct Support to Incident Response

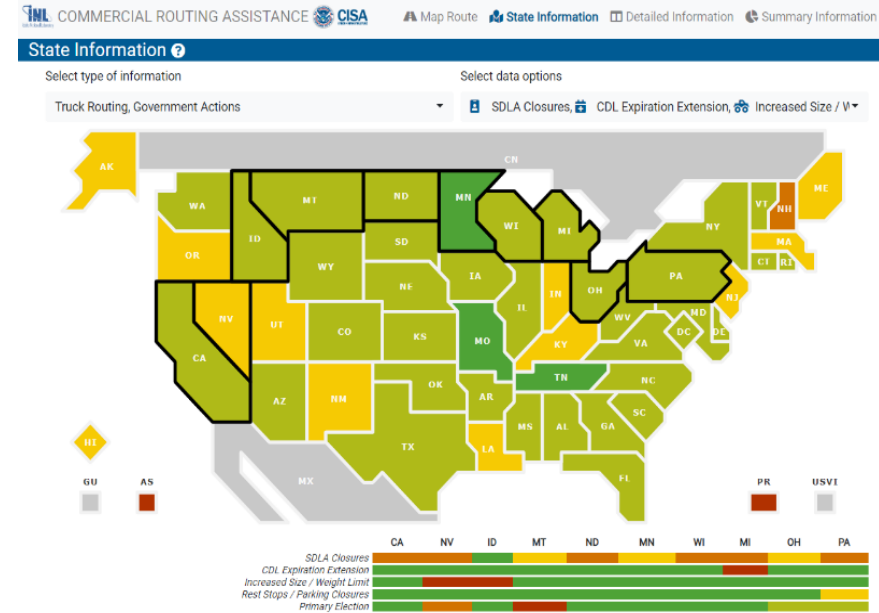
- Facilitated healthcare supply chain outreach efforts between DHS officials in New York City and critical product suppliers
- Facilitated a session among the nation's largest oxygen suppliers to enable DHS and HHS to better understand needs and challenges as infections rise
- Supported DHS CISA efforts at Federal Emergency Management Agency HQ on topics from hospital operational challenges to mortuary supply chains

## Business Reopening

- Conducted rapid assessment for CISA of potential factors affecting business reopening
- Identified critical considerations, pre-existing resources, and potential elements for "reopening checklists"

## Analysis of Future Infrastructure Challenges

- CISA is increasingly focused on potential future challenges to the Nation's infrastructure and longer-term recovery
- INL is advising CISA on approaches to these priorities and soon will be fully engaged in future issue scanning and discrete analysis of specific future concerns



[cra.inl.gov](http://cra.inl.gov)

With support from DHS CISA, INL designed, developed, and deployed the Commercial Routing Assistance (CRA) tool:

- Merges coordinated and vetted data streams
- Plots multiple automated or custom routing options
- Visualizes state regulations and actions that a driver may encounter along a route

# All Hazards Analysis (AHA)

AHA is an optimized framework for the collection, storage, analysis, and visualization of critical infrastructure information

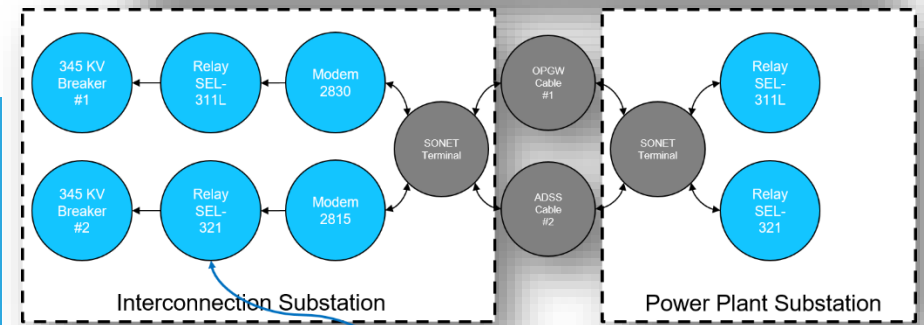
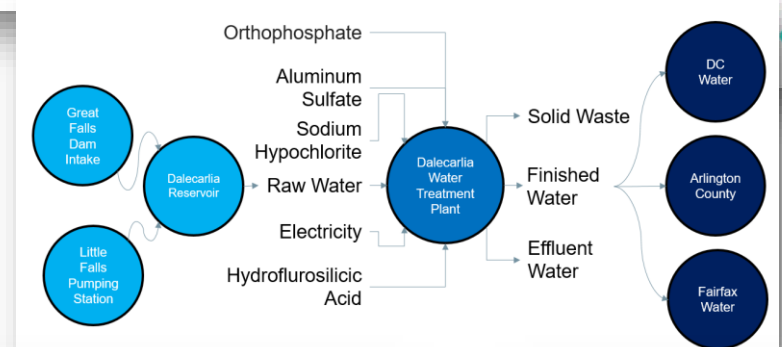
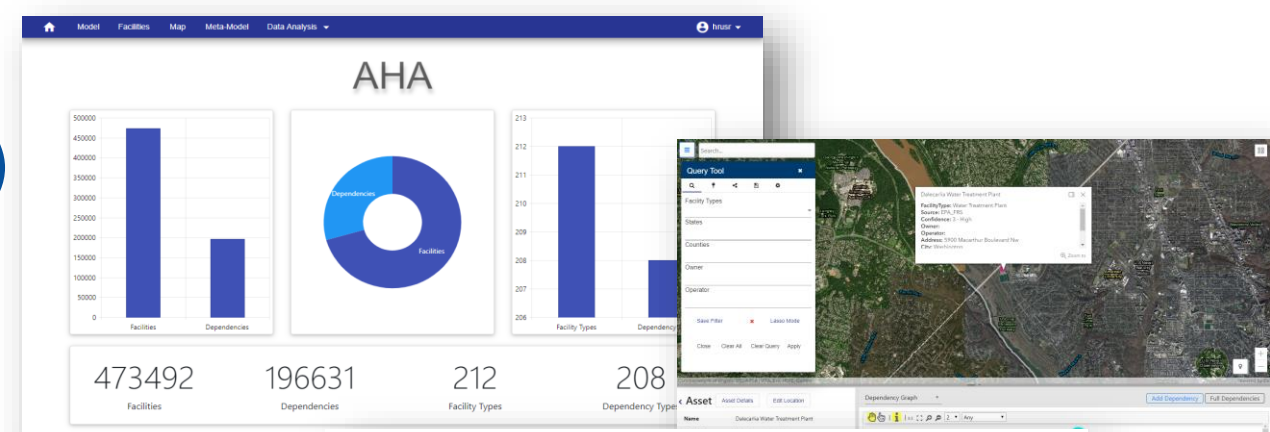
- Understand the consequence of infrastructure failure
- Enable collection and documentation of dependency information
- Provide a framework and capability for both analysts and decision makers
- Enhance the continuity of operations across sectors

## Use Case

- National Response Framework
  - Disruption Modeling (TTX)
- Mission Assurance (COOP)
- Resilience Planning
- Supply Chain Modeling
- Knowledge Management and Transfer

## Availability

- Analytic support for Federal and State Partners (DHS, USAF, US Army)
- State and Local Deployment Pilot
  - No-cost License (2 states)





# Regional Infrastructure Guidebook

## Idaho State Infrastructure Guidebook

In times of growing cyber threats and severe weather, resilience – the ability to continue providing emergency services while damaged infrastructure is restored – has emerged as a growing concern among leaders at state and local levels. The world is held together with strands far more fragile than most people realize.  
-Kelly Wilson

Infrastructure Assurance & Analysis



## Focus on knowledge building and a framework for how to perform infrastructure analysis

**Priorities and capabilities will be different Region-to-Region**

- Identifying and prioritizing regional infrastructure
- Understanding lifeline systems and critical nodes
- Analytic tradecraft and business intelligence
- Multi-source research
- Resources

**Allows flexibility for different ways a critical infrastructure analyst may support a host of operational missions**

- DHS Taxonomy, Critical Lifelines, Capabilities-focused, ESF-14
- Dependency Profiles
- Special Event Support
- Incident Support
- Risk Management and Mitigation Strategies

**Critical questions help to translate guidebook information into analytic inquiries and actions**

- What can I do with this (guidebook) information?

**Keeping abreast of key infrastructure industry drivers of changes, threats, and trends**

- Infrastructure portfolios and risk profiles will change over time

# Securing U.S. Election Infrastructure

- Participated in 4 task areas related to election systems aimed at pre- and post-attack defense
  - **All efforts uncovered issues ranging from minor to significant**
    - Provided stakeholders mitigative solutions to better harden systems against attack
- Evaluated large percentage of national election system vendors
- CISA plans on continuing election research at INL

**THE HILL** Top voting machine manufacturer urges Congress to make paper records required  
BY MAGGIE MILLER · 06/10/19 04:48 PM EDT 219 COMMENTS

This is the latest step by ES&S to ensure customers of the security of its machines, coming after the company submitted its machines to the Idaho National Laboratory for testing in April, which was done to ensure the "strength of equipment deemed critical infrastructure," according to ES&S.

**ES&S Sets High Standard in Elections Industry with Independent Third-Party Testing**

Internationally Renowned Re-Test on Critical Infrastructure |



NEWS PROVIDED BY Election Systems & Software → Apr 30, 2019, 13:14 ET

"The new testing by INL, which also performs testing for the U.S. Department of Defense, complements the thousands of hours of independent security testing already performed on ES&S equipment and systems," said ES&S Vice President of Systems Security Chris Wlaschin. "This additional round of penetration testing and vulnerability assessment furthers our never-ending effort to strengthen our nation's voting infrastructure."

Researchers at INL are internationally known for their contributions in the area of national and homeland security. INL scientists and engineers are internationally recognized for their capabilities in critical infrastructure protection and nuclear nonproliferation. In addition to their energy and national security work, INL penetration testers are also known for winning the DEFCON 18 Capture the Flag event in 2010.

"INL is widely respected for its expertise, and that's why we proactively began this work," Wlaschin said. "We believe this kind of collaboration between election system providers, the Department of Homeland Security and national test labs should be the way of the future for the testing of election systems."

**POLITICO**

**Weekly Cyberse**  
Delivered every Monday by 10 o'clock  
Cybersecurity examines the latest cybersecurity policy and politics

**The CEOs of Election Systems & Software (Tom Burt) and Hart InterCivic (Julie Mathis) both said their companies had submitted equipment to Idaho National Laboratory, which conducts vulnerability tests with DHS. Overall, Burt said he**

**Hitches in a voting vendor vulnerability disclosure program**  
By TIM STARKS | 01/10/2020 10:00 AM EST  
With help from Eric Geller, Mary Lee, Martin Mattishak and Alexandra S. Levine

**ABOUT THE AUTHOR**  
Tim Starks has written about cybersecurity since 2003, when he began at Congressional



# Operation Warp Speed (OWS)

## OWS Mission Statement:

Using the resources of the federal government and the U.S. private sector, OWS will accelerate the testing, supply, development, and distribution of safe and effective vaccines, therapeutics, and diagnostics to counter COVID-19 by January 2021



- INL support to OWS:
  - Proactive assessments of critical infrastructure systems and networks across the vaccine supply chain
    - Help manufacturers and distributors better architect their environments against attacks
      - INL has performed 4 Assessments to date (additional scheduled)
  - Continuous monitoring and network defense support for OWS stakeholders
    - Focused on detecting advanced intrusions when they happen
    - Multiple customers in different stages of deployment



# Questions?

Ron Fisher

Director, Infrastructure Assurance and Analysis Division  
National and Homeland Security  
[ron.fisher@inl.gov](mailto:ron.fisher@inl.gov)