



# Securing the Nation's Critical Infrastructure

## Cybersecurity

### OUR NATION'S CHALLENGE

*The cyber-attacker of today has an advantage over those protecting our Nation's assets and infrastructure – they can operate inexpensively, with anonymity, and without pressure to act quickly.*

At the Pacific Northwest National Laboratory, we understand the enormity of this challenge and the need for rapid threat discovery utilizing both traditional and non-signature based cyber solutions.

### PNNL'S APPROACH

Since the late 1990s, PNNL has provided impactful cybersecurity research and solutions to protect our Nation's cyber infrastructure. Today, PNNL staffs over 300 hundred scientists and engineers, who are engaged in multi-disciplinary teams that include not only cyber professionals, but also biological, chemical, high performance computing, and software engineering expertise. Our resources and expertise are deployed in solutions for the U.S. Departments of Energy, Homeland Security, Defense and other National Security agencies.

Additionally, PNNL remains committed to significant multi-year cybersecurity research investments. Our current agenda is intended to produce the tools and technology that will not only measure the cybersecurity posture at all system levels, but provide an asymmetric advantage to the defender at reduced operational costs.

How do we know if we are on track? The evaluation, analysis, and visualization of these grand challenges and other transformational ideas happen every day at PNNL's Cyber Innovation and Operations Center—a secure prototyping and demonstration capability where we advance the analytic state-of-the-art and address emerging customer needs.

Our extensive portfolio of technology and capabilities offers tomorrow's innovative solutions today; each designed to enhance the nation's cybersecurity posture in the areas of:

- » Global Threat Intelligence
- » Electric Grid Security
- » Cyber Physical Systems
- » Bio-inspired Security
- » Component Security
- » Cyber Analytics

### CONTACTS

*For more information about Cybersecurity solutions and capabilities, contact:*

Dave Thurman — Portfolio Manager, National Security Computing  
dave.thurman@pnnl.gov

Sharon Adams — Technical Group Manager, Cyber Security  
sharon.adams@pnnl.gov



# DISCOVERY

*in action*

## Cybersecurity at PNNL

*For over two decades, Pacific Northwest National Laboratory has been developing the science and technology needed to deliver the theory, processes, methodologies, and algorithms that will enable a resilient cyber infrastructure with an asymmetric advantage to address our nation's greatest computational challenges in energy, the environment, national security, and fundamental science.*

### Integrated Cyber Physical Security

Research at PNNL examines vulnerabilities associated with cyber-physical interdependencies. Using existing facility information we can identify vulnerabilities and evaluate safeguards to enable a better defense against threats.

### Electric Grid Security

Leading the charge to secure a safer and more reliable grid, PNNL is currently developing cyber-based systems that safeguard our Nation's critical electric infrastructure.

### Bio-inspired Security

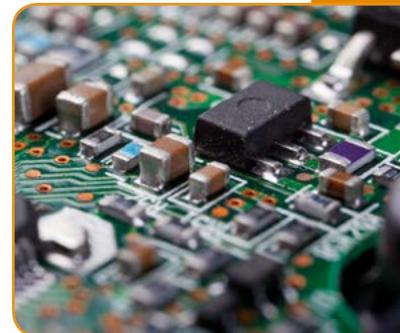
The volume of network traffic data generated has outpaced our ability to effectively analyze it fast enough to prevent many forms of network-based attacks. PNNL develops and leverages technologies and methods from biological and DNA sequencing research to discover malicious sequences of traffic in computer networks.

### Component Security

Helping to ensure the integrity of mission-critical systems, PNNL is developing specialized diagnostic and monitoring tools, identifying malicious code that is traditionally undetectable, detecting compromises in supply chains, and ensuring the integrity of computer hardware and firmware components.

### Cyber Analytics

Our innovative and distinctive methods, algorithms, and software tools, combined with large scale data management and available data tools, enable PNNL domain experts to detect anomalies and defend computer networks.



**Pacific Northwest**  
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965