



# CYBERSECURITY RISK INFORMATION SHARING PROGRAM (CRISP)

The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership to facilitate the timely sharing of cyber threat information and develop situational awareness tools to better protect against and respond to cybersecurity threats. The capability enhances the Energy Sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, reducing the risk of energy disruptions due to cyber events.

CRISP uses technical expertise and technologies developed at the Pacific Northwest National Laboratory (PNNL) and machine speed information sharing technologies developed by Argonne National Laboratory, leverages access to government cybersecurity information, and collaborates with industry subject matter experts at the North American Electric Reliability Corporation's (NERC) Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

## Approach

CRISP is a collaborative effort between critical electric power utilities and the U.S. government (USG). Partici-

pating critical infrastructure owners and operators provide cybersecurity data in near-real-time to PNNL and the ES-ISAC, and in return, receive automated analytics and analysis from a team of cybersecurity specialists. The program also allows participants to receive machine-to-machine threat information and mitigation measures. CRISP represents a maturation of the private-public partnership established under the National Infrastructure Protection Plan, and benefits both industry and government. No other program shares cyber intelligence information fused with industry information in a collaborative sharing framework in the same way as CRISP.

Key to CRISP's approach is information sharing across a broad and diverse group of utilities supported by the Information Sharing Device (ISD), a network device that resides at an entities' network border just outside the firewall. Once activated, the ISD data is encrypted and transmitted to the CRISP Analysis Center at PNNL where analysts investigate the data for advanced sector-specific threats. The completely passive ISD is an intrusion scoping system; CRISP leverages ISD data and all-source intelligence to support

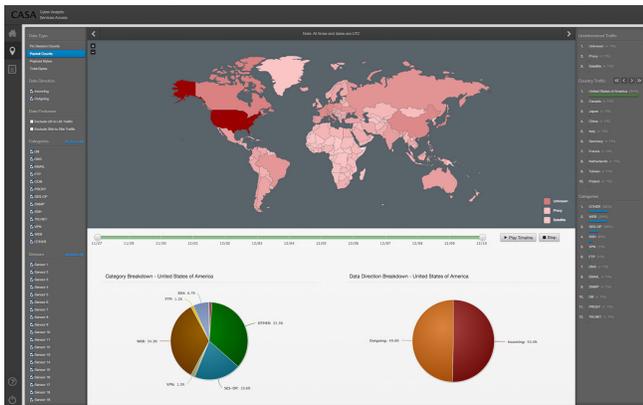
*“The reports sent were corroborated by alerts we also received via our ... monitoring service, but your team’s analysis provided more detail on the tools being used.”*

operations across the CRISP community and to inform the USG of advanced threats impacting the Energy Sector.

## Impact

Insight derived via CRISP is delivered to the Energy Sector via both a sector-wide view of network activity and blended cyber/human/physical threat analysis capability. Automated threat identification analytics delivered to CRISP partner companies—including enhanced cyber defense analysis with continual queries for high threat indicators, strategic trend analysis, and investigations of new alerts—enable enhanced situational awareness across the entire Energy Sector.

CRISP is an industry owned and operated capability and advances the Energy Sector’s cybersecurity posture by combining cybersecurity information from across a large and diverse group of companies. Participating companies leverage USG cybersecurity



research and development to collectively address cybersecurity challenges and build a foundation for future capabilities. This unique public-private partnership enhances industry’s ability to prevent cyber-attacks and improve response to events that do occur.

## About PNNL

Interdisciplinary teams at PNNL address many of America’s most pressing issues in energy, the environment and national security through advances in basic and applied science. Founded in 1965, PNNL employs 4,300 staff and has an annual budget of about \$950 million. It is managed by Battelle for the U.S. Department of Energy’s Office of Science. As the single largest supporter of basic research in the physical sciences in the United States, the Office of Science is working to address some of the most pressing challenges of our time.

## About ES-ISAC

The ES-ISAC, operated by NERC, establishes situational awareness, incident management, coordination, and communication capabilities within the Energy Sector through timely, reliable, and secure information exchange. The ES-ISAC, in collaboration with the Department of Energy and the Electricity Sector Coordinating Council, serves as the primary security communications channel for the Energy Sector and enhances the ability of the sector to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

For more information contact

**Matthew Light, Program Manager**  
ES-ISAC | NERC  
202.809.3079 | [matthew.light@nerc.net](mailto:matthew.light@nerc.net)

**Jeffery Mauth, Program Manager**  
Pacific Northwest National Laboratory  
509.375.2511 | [jeff.mauth@pnnl.gov](mailto:jeff.mauth@pnnl.gov)

