INL/MIS-24-79952-Revision-0

Cybersecurity Operational Research, Experimentation, Innovation, and Integration (COREII)

October 2024

Alycia Brooke Honas

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-24-79952-Revision-0

Cybersecurity Operational Research, Experimentation, Innovation, and Integration (COREII)

Alycia Brooke Honas

October 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Cybersecurity Operational Research, Experimentation, Innovation, and Integration (COREII)

Overview

The Department of Energy's Cybersecurity, Energy Security, and Emergency Response Office (CESER) has partnered with Idaho National Laboratory (INL) and energy companies to develop COREII. This research initiative aims to align with the national cybersecurity strategy, enhance the resilience of critical energy infrastructure, facilitate efforts to improve grid-enhancing technologies (GET) and major effects from other critical and emerging technologies, and to enable discovery of innovative solutions for emerging cybersecurity challenges. COREII strives to push the boundaries of Operational Technology (OT) cybersecurity and seeks to provide a solution to the problem of aligning and integrating research efforts to effectively support the national OT cybersecurity mission in the following ways:

Sponsorship

The COREII program is sponsored by the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

- Advance the current level of publicly available OT cybersecurity knowledge to address emerging threats.
- Ensure the long-term relevance and viability of research-generated data.
- Provide a consolidated point of collection and cross-correlation of all National Lab-generated unclassified data.
- Utilize the national lab complex to merge and synergize research efforts to enable a cohesive data ecosystem.
- Enable scalable public-to-private collaboration. Contribute to the open scientific literature within the cybersecurity domain.
- Deliver practically applied solutions to energy sector industry partners.
- Create a system that converges existing and new research efforts focusing on applied research and development workforce enablement to collect data, generate reports, and avoid replication of research.

Operational Objectives

The COREII program is dedicated to advancing the cybersecurity posture of critical infrastructure by leveraging decision intelligence and cutting-edge technology. COREII's operational objectives include:

- **Create a Collaborative Platform** to unify OT cybersecurity tools developed at DOE National Labs that were funded by CESER and other DOE program offices.
- **Enhance Decision Intelligence** to continuously improve outputs to provide actionable insights.
- **Strengthen Cybersecurity Collaboration** to facilitate greater collaboration between public and private sector entities.operations.
- **Implement Advanced Cybersecurity Measures** to deploy advanced technologies and methodologies.
- **Conduct Comprehensive Training and Exercises** to provide relevant training and simulation scenarios.

Solutions and Benefits

Human Factors Engineering show limits to what an individual analyst can process. COREII empowers the human user's ability to process, correlate, sustain, or fully leverage the amount of available data generated by the DOE national lab complex through projects, programs, or activities. The COREII platform integrates multiple programs, projects, tools, and data sources to facilitate rapid data analysis, guide applied research and development, and efficiently advance the national OT cybersecurity posture.

COREII benefits include:

Reduce data aging through ongoing and consistent enrichment processes.

Quickly analyze vast volumes of data to support data-driven applied research and development (R&D).

Enhance coordination among national lab complex on R&D efforts.

Areas of Research (AoR)

The focus of the COREII program is to advance the cybersecurity capabilities of the energy sector through targeted research, development, and implementation of innovative solutions. The program focuses on the following research areas:

REQUIREMENTS GENERATION AND ALIGNMENT

Generating and aligning OT cybersecurity research requirements to ensure that research efforts meet the needs of sponsors and address the most pressing cybersecurity challenges within the energy sector.

THREAT ANALYSIS

Creating solutions that enable efficient threat analysis from diverse data sources (unclassified and open source) and convert them into actionable OT threat intelligence. The objective is to streamline the threat analysis process, ensuring the resulting intelligence is pertinent to OT environments

SCALABLE CYBER-PHYSICAL TESTING

Developing scalable cyber-physical testing environments to evaluate the resilience of energy infrastructure against cyber threats. The goal is to create comprehensive modeling, simulation, and emulation environments scalable from the component level to sector-wide applications.

KNOWLEDGE MANAGEMENT AND TRANSFER

Enhancing the collection, extraction, transformation, and updating of OT cybersecurity knowledge relevant to research conducted on behalf of DOE CESER. The objective is to ensure that each research area identifies datasets that can be integrated into a comprehensive data, information, and knowledge model.

MARKET AND SUPPLY CHAIN ANALYSIS

Analyzing market and supply chain dynamics to identify and mitigate cybersecurity risks. The key focus for Phase I is to determine the necessary market and supply chain analysis datasets and tools to enrich other research areas with relevant data.

WORKFORCE ANALYSIS

Analyzing and addressing the cybersecurity workforce needs within the energy sector, specifically targeting the OT cybersecurity workforce. Initial efforts will focus on basic exploration and discovery of data sources beneficial to researchers, with detailed plans developed post-Phase I.

Partnership Ecosystem

The vision of COREII is to create a central platform to collect applied research and development data, driving and informing advanced applied research activities. COREII seeks to integrate and harmonize data and applied research efforts across the national lab complex. Additional use cases are being considered for operational needs.

Federal Partnerships

Phase 1 (FY24):

- Idaho National Laboratory
- Sandia National Laboratories
- Lawrence Livermore National Laboratory
- Pacific Northwest National Laboratory

Phase 2 (FY25):

- Partnership exploration in progress

Industry Partnerships

COREII will leverage strategic partnerships to evaluate and address cybersecurity threats and vulnerabilities in the energy sector. These partners will work with the COREII team to identify and mitigate cybersecurity vulnerabilities related to the energy sector, ensuring the integrity and reliability of critical infrastructure systems nationwide. One of COREII's main strategic goals is to create an AI-enhanced platform that enriches federal, state, and other critical infrastructure data by provisioning near-real-time decision intelligence.

Become a partner: Speak with one of our experts to see how you can participate and benefit from our partnership network and applied research.

email: COREII@inl.gov

Revision 0, July 2024

21-50125_06