U.S. DEPARTMENT OF
ENERGY
Office of Electricity
Delivery and Energy
Reliability

PEER REVIEW

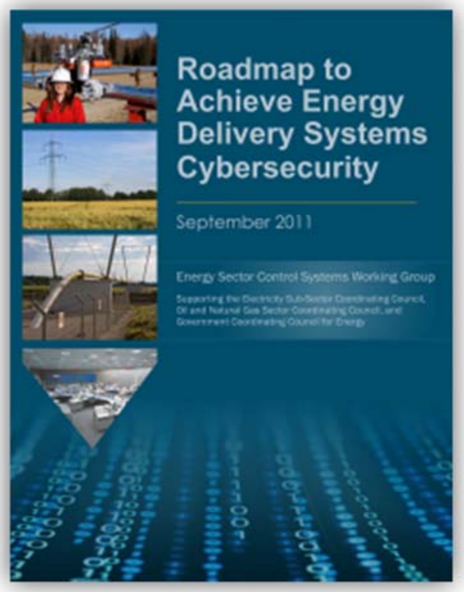
CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS(CEDS)

2016

December 7-9, 2016
Arlington, VA

Welcome to the 2016 CEDS Peer Review!

The Cybersecurity for Energy Delivery Systems (CEDS) program supports the Office of Electricity Delivery and Energy Reliability's (OE) key mission to enhance the reliability and resilience of the nation's energy infrastructure. OE designed the CEDS program to assist the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS supports research partnerships to make advances in cybersecurity capabilities for energy delivery systems, and fosters collaborations among the energy sector, government, national laboratories, and universities.


Roadmap to Achieve Energy Delivery Systems Cybersecurity

September 2011

Energy Sector Control Systems Working Group

Supporting the Electricity Sub-Sector Coordinating Council, Oil and Natural Gas Sector Coordinating Council, and Government Coordinating Council for Energy

The peer review provides CEDS projects, stakeholders, and management with an expert, unbiased assessment of strengths, weaknesses, and specific recommendations for improvement. The CEDS program will receive high-quality technical input to assist in making decisions and setting priorities. The event offers a networking opportunity for energy sector stakeholders, national laboratories, and the academic community. Importantly, the peer review process provides public accountability for the use of public funds. Presentations from the 2016 Peer Review will be available on the ieRoadmap website (www.controlsystemsroadmap.net).

The CEDS program aligns all activities with federal priorities as well as the strategy and milestones articulated in the energy sector's 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity that envisions resilient energy delivery control systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

This year's event includes formal peer review presentations, information sharing sessions and the opportunity to participate in networking/poster sessions. We welcome your participation in this peer review and look forward to your valuable feedback.

Dr. Carol Hawk

WEDNESDAY—DECEMBER 7, 2016		
Poster Set-Up	7:30-8:30am	Potomac I-II
Registration & Breakfast	8-8:45am	Washington Foyer
Instructions— ❖ Mr. Ryan Egidi, CEDS Project Office, National Energy Technology Laboratory	8:45-9am	Washington Room
Welcome Messages— ❖ Ms. Patricia Hoffman, Assistant Secretary – Office of Electricity Delivery & Energy Reliability	9-9:10am	
❖ Dr. Carol Hawk, Program Manager—Cybersecurity for Energy Delivery Systems	9:10-9:20am	
❖ Ms. Jetta Wong, Director—Office of Technology Transitions	9:20-9:30am	
Argonne National Laboratory – Peer Review ❑ A Resilient Self-Healing Cyber Security Framework for Power Grid ❑ A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications ❑ Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters	9:30-10am	
Brookhaven National Laboratory – Peer Review ❑ Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI)	10-10:30am	
Poster Session/Morning Break	10:30-11:15am	Potomac I-II & Washington Foyer
Electric Power Research Institute – Peer Review ❑ Secure Policy Based Configuration Framework (PBCONF)	11:15-11:45am	Washington Room
Schweitzer Engineering Laboratories – Information Sharing ❑ Watchdog and SDN Projects	11:45-12:15pm	
Lunch	12:15-1:30am	Potomac III – IV
Georgia Tech Research Institute – Peer Review ❑ Cyber-Physical Modeling & Simulation for Situational Awareness (CYMSA)	1:30-2pm	Washington Room
Idaho National Laboratory – Peer Review ❑ Validation and Measuring Automated Response (VMAR) Project	2-2:30pm	
Poster Session/Afternoon Break	2:30-3:15pm	Potomac I-II & Washington Foyer
ABB, Inc. – Information Sharing ❑ Collaborative Defense of Transmission and Distribution and Protection and Control Device against Cyber Attacks (CODEF)	3:15-3:35pm	Washington Room
Grid Protection Alliance – Information Sharing ❑ ARMORE: Applied Resiliency for More Trustworthy Grid Operation	3:35 – 3:55pm	
National Rural Electric Cooperative Association – Information Sharing ❑ Energy Sector Security Appliances in a System for Intelligent, Learning Network Configuration Management and Monitoring (ESSENCE)	3:55 – 4:15pm	

THURSDAY – DECEMBER 8, 2016		
Breakfast	8-8:30am	Washington Foyer
Los Alamos National Laboratory – Peer Review □ Quantum Security Modules for the Power Grid	8:30-9am	Washington Room
Lawrence Berkeley National Laboratory – Peer Review □ Supporting Cyber Security of Power Distribution Systems by Detecting Differences Between Real-time Micro-Synchrophasor Measurements and Cyber-Reported SCADA	9-9:30am	
Oak Ridge National Laboratory – Peer Review □ Timing Authentication Secured by Quantum Correlations (TASQC) □ Cliques: CRL-less Revocation and Anonymous Authentication for the Smart Grid	9:30-10am	
Lawrence Livermore National Laboratory – Peer Review □ Safe Active Scanning for Energy Delivery Systems (SASEDS)	10-10:30am	
Poster Session/Morning Break	10:30-11:15am	Potomac I-II & Washington Foyer
Pacific Northwest National Laboratory– Peer Review □ Automated, Disruption Tolerant Key Management (ADTKM) □ Enabling Situation Assessment/Awareness for Utility Operators and Cybersecurity Professionals □ EDS Digital Evidence □ Multispeak Secure Protocol Enterprise Access Kit (MS-SPEAK)	11:15-11:55am	Washington Room
Lunch	11:55-1:15pm	Chesapeake View
University of Arkansas – Peer Review □ Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)	1:15-2:15pm	Washington Room
Sandia National Laboratory – Peer Review □ Artificial Diversity and Defense Security (ADDSec)	2:15-2:45pm	
Afternoon Break	2:45-3:30pm	
Poster Session/Networking Session	3:30-5:30	Potomac I-II

FRIDAY – DECEMBER 9, 2016

Breakfast	8-8:30am	Washington Foyer
Schweitzer Engineering Laboratories – Peer Review ❑ Secure SW Defined Radio	8:30-9am	Washington Room
Foxguard Solutions – Peer Review ❑ Patch and Update Management Program for EDS	9-9:30am	
POSTER SESSION/MORNING BREAK	9:30-10am	Potomac I-II & Washington Foyer
University of Illinois– Peer Review ❑ Cyber Resilient Energy Delivery Consortium (CREDC)	10-11am	Washington Room
CEDS Multi-Year Program Plan Discussion	11-11:30am	

Argonne National Laboratory

A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications

- **Primary Roadmap Milestone:** 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented.
- **Project Description:** Development of a holistic security and cloud outsourcing framework for power grid applications such that infrastructure security, data confidentiality, and time criticality are considered.
- **Significance:** This project lays out a scientific foundation and develops validating fundamental building blocks for cloud-based power grid applications, transforming the "fault-resilient grid" (N-1 contingency) of today to an "attack-resilient grid" of the future.

Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters

- **Primary Roadmap Milestone:** 3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions.
- **Project Description:** Development of a holistic attack-resilient architecture and layered cyber-physical solution portfolio to protect the integrated distributed energy resources (DER) and the critical power grid infrastructure from malicious cyber attacks.
- **Significance:** The outcome of this project is the significantly enhanced ability to maintain resilience during cyber-attacks targeted at dispersed renewables, DER and smart inverters while sustaining critical energy delivery functions.

A Resilient Self-Healing Cyber Security Framework for Power Grid

- **Primary Roadmap Milestone:** 2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available.
- **Project Description:** Development of an attack-resilient Wide-Area Monitoring, Protection, and Control (WAMPAC) framework, with associated computational algorithms and software tools, to prevent and mitigate cyber attacks.
- **Significance:** This project will develop tools to prevent and mitigate cyber-attacks and enhance the resilience of the bulk power system.

Brookhaven National Laboratory

Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI)

- **Primary Roadmap Milestone:** 4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available.
- **Project Description:** Development of an online tool (AIERCI) that utilities can use to detect, mitigate, and evaluate the potential impact of various cyberattack scenarios to reduce the risk that malicious compromise of essential forecasting data used for grid scheduling and operation might result in disruption of energy delivery.
- **Significance:** Energy delivery systems are increasingly dependent on sophisticated forecasting data for efficient operations. Weather data, load profiles and forecasting information about renewable generation are used for scheduling functionalities for both transmission and distribution operations.

ELECTRIC POWER RESEARCH INSTITUTE

Secure Policy Based Configuration Framework (PBCONF)

- **Primary Roadmap Milestone:** 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented.
- **Project Description:** The project team led by EPRI is developing a framework that allows utilities to centrally manage the remote configuration of their energy delivery system devices – regardless of vendor or age – more securely.
- **Significance:** This effort will provide an open-source framework with a single, organization-wide view of field device security configurations and a policy engine to address the interoperability challenges of various remote access control methods.

GEORGIA TECH RESEARCH INSTITUTE

Cyber-Physical Modeling & Simulation for Situational Awareness (CYMSA)

- **Primary Roadmap Milestone:** 2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available.
- **Project Description:** The project team led by GTRI is developing a cybersecurity situational awareness technology suite that evaluates energy delivery system control commands to anticipate their impact on power grid operations and, if needed, implements cybersecurity responses to prevent disruptions.
- **Significance:** This technology will offer asset owner's and operator's enhanced situational awareness that helps to detect adversarial manipulation of energy delivery components in a real-time operational environment informed by modeling and simulation technologies based on co-simulation of cyber and physical grid operations, and distributed state estimation.

IDAHO NATIONAL LABORATORY

Validation and Measuring Automated Response (VMAR) Project

- **Primary Roadmap Milestone:** 4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available.
- **Project Description:** The Validation and Measuring Automated Response (VMAR) project is providing a cyber-incident response comparison capability and enabling industry to select response technologies best suited to each energy sector entity's particular needs.
- **Significance:** This effort is working towards automated response to a cyber-incident and measuring the efficacy of automated response to drive future improvements.

LOS ALAMOS NATIONAL LABORATORY

Quantum Hardware Security Modules for the Power Grid

- **Primary Roadmap Milestone:** 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented.
- **Project Description:** Development of dedicated devices called Quantum Security Modules (QSMs) that receive data from grid control devices, encrypt that data with quantum keys, and then transmit and receive that data over computer networks.
- **Significance:** This project is unique in that it leverages the groundbreaking capabilities of quantum communications to generate and manage the encryption keys that guarantee data integrity. This research uses quantum physics principles to reveal in real-time an adversarial attempt to intercept the key exchange. Unlike traditional cryptography solutions, quantum keys enjoy the twin benefits of higher security and lower computational complexity.

LAWRENCE BERKLEY NATIONAL LABORATORY

Supporting Cyber Security of Power Distribution Systems by Detecting Differences Between Real-time Micro-Synchrophasor Measurements and Cyber-Reported SCADA

- **Primary Roadmap Milestone:** 2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available.
- **Project Description:** This effort utilizes μPMUs and SCADA in the distribution grid to measure physical/electrical power system parameters and detect cyber-attacks against substation equipment. Specifically, the project has developed data-driven models to identify key classes that help distinguish cyber-attacks from physical events, and equipment malfunction.
- **Significance:** This research aims to give a more reliable, robust, scalable, and cost-effective means of detecting key classes of cyber-attack scenarios against the power distribution grid compared to traditional approaches.

OAK RIDGE NATIONAL LABORATORY

Cliques – CRL-less Revocation and (Anonymous) Authentication for the Smart Grid

- **Primary Roadmap Milestone:** 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented.
- **Project Description:** This technology seeks to enable rapid and secure revocation and provisioning of cryptographically secured authorizations in a publish-subscribe controlled micro-grid. The Cliques project separates long-lived node identity ("serial number") from the attestation of a node's authorized actions.
- **Significance:** This project will result in a scalable cryptographic key management system that can be used with smart grid devices.

Timing Authentication Secured by Quantum Correlations (TASQC)

- **Primary Roadmap Milestone:** 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented.
- **Project Description:** Develop and demonstrate a transformative system of ground-based timing and communication beacons featuring security that is enhanced by geographically distributed quantum correlations and that takes full advantage of the direction of information flow for power systems management.
- **Significance:** The system will offer the improved security afforded by the techniques of quantum communication to authenticate timing signals, power systems data such as those sent from a phasor measurement unit (PMU) to a substation, and other communications tasks.

Lawrence Livermore National Laboratory

Safe Active Scanning for Energy Delivery Systems (SASEDS)

- **Primary Roadmap Milestone:** 2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings.
- **Project Description:** This research team performed a detailed literature survey and interviews with industry partners to characterize and understand whether active scanning techniques may be safely applied to energy delivery systems.
- **Significance:** Initial experimentation results show that running aggressive active scans showed very little impact on ICS devices. These preliminary results imply that, properly configured, active scans could potentially be used in EDS environments.

Pacific Northwest National Laboratory

Automated, Disruption Tolerant Key Management (ADTKM)

- **Primary Roadmap Milestone:** 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented.
- **Project Description:** The project is working to design a standards compliant and interoperable system, implement a prototype key management and field device services, and evaluate and compare the performance and effectiveness of the prototype against existing key management systems for the energy sector.
- **Significance:** This effort is improving security and the efficiency of operations by providing a new key management architecture suited to the unique requirements of EDS.

Enabling Situation Assessment/Awareness for Utility Operators and Cybersecurity Professionals

- **Primary Roadmap Milestone:** 2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available.
- **Project Description:** This project will develop visualizations that power system operators and/or cybersecurity professionals can use to make fast, accurate assessments of situations, enabling them to maintain situation awareness during unfolding events.
- **Significance:** The visualization tool will reduce the cognitive burden on the operators and enable them to make faster decisions and maintain cybersecurity situational awareness.

EDS Digital Evidence

- **Primary Roadmap Milestone:** 4.4 Real-time forensics capabilities commercially available.
- **Project Description:** In digital forensics forums, the idea of Live analysis is gaining momentum. This project is evaluating existing Live Analysis monitoring and detection tools for energy delivery systems (EDS) use.
- **Significance:** The research seeks to develop a tool that could provide evidence of anomalous cyber behavior on a live EDS without interrupting energy delivery.

"Multispeak Secure Protocol Enterprise Access Kit (MS-SPEAK)"

- **Primary Roadmap Milestone:** 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented.
- **Project Description:** The project team is creating an innovative ESB+ (enterprise service bus) for MultiSpeak. The ESB+ will support increased interoperability and cybersecurity of the MultiSpeak standard and reduce costs in utilities that depend on MultiSpeak.
- **Significance:** This effort is improving cybersecurity of the Multispeak standard for the energy sector.

UNIVERSITY OF ARKANSAS

Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)

- **Primary Roadmap Milestone:** 5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining.
- **Project Description:** This multi-disciplinary team of university and industry partners will conduct mid-term and long-term research and development (R&D) of cybersecurity technologies for energy delivery systems organized under the following five (5) focus areas: a) protecting core power grid controls and operations; b) building cyber security into components and services including microgrid assets, demand-side management, smart metering, as well as electric vehicles; c) protecting energy sector communications infrastructure; d) providing cyber security management capabilities to address complex cyber security operation beyond human capacity; and e) provisioning cyber security testing and validation to evaluate the efficacy of protective measures.
- **Significance:** SEEDS will develop cyber technologies and transition them to practice in the energy sector, become a member-based self-sustaining consortium to continue industry relevant cybersecurity R&D, and propagate a highly qualified student workforce to be industry-ready in the area of cybersecurity for energy delivery systems.

SANDIA NATIONAL LABORATORY

Artificial Diversity and Defense Security (ADDSec)

- **Primary Roadmap Milestone:** 3.4 - Self-configuring energy delivery system network architectures widely available.
- **Project Description:** The ADDSec project is developing defensive technologies that randomly and automatically reconfigure energy delivery operational network parameters moment-by-moment to impede reconnaissance and cyber attack planning.
- **Significance:** ADDSEC will increase the security of both legacy and modern energy delivery systems by converting these traditionally static systems into moving targets.

SCHWEITZER ENGINEERING LABORATORIES

Secure SW Defined Radio (SDR)

- **Primary Roadmap Milestone:** 3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented.
- **Project Description:** The project team is developing a configurable radio platform with integrated security features for more secure "last mile" wireless communications for electric utility distribution automation.
- **Significance:** This project will provide a cyber-secured wireless network with capabilities to secure firmware updates, data retrieval, configuration, authentication and logging. In addition the, SDR is a flexible and configurable radio platform that can be extended in the future to address other aspects of distribution automation data collection and control through the development of additional radio, and time distribution technology.

FOXGUARD SOLUTIONS

Patch and Update Management Program for Energy Delivery Systems

- **Primary Roadmap Milestone:** 1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available.
- **Project Description:** The project team is developing a cybersecure patch and update management service/system that will simplify the asset owners and operators' process of keeping up-to-date with the most current firmware and software patches and updates.
- **Significance:** This project will help reduce the risk that a known vulnerability could remain unpatched and consequently be exploited, as well as reduce the burden associated with patching and updating energy delivery devices. It will also provide a means for asset owners/operators to verify the integrity and authenticity of patches and updates. Likewise, it will offer a methodology and services for asset owners/operators to validate patches and updates to avoid related system down time.

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Cyber Resilient Energy Delivery Consortium (CREDC)

- **Primary Roadmap Milestone:** 5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining.
- **Project Description:** Research and development of cybersecurity for energy delivery system technologies organized under the following tracks: a) long-term research to address foundational issues; (b) mid-term research and development leading towards deployable technology; (c) verification and validation to demonstrate correctness and efficacy of developed solutions in realistic settings, and (d) outreach activity to promote a culture of EDS cybersecurity in the workforce as well as among the public. The CREDC model will explicitly create a pipeline that generates research results and takes them through to evaluation and demonstration of prototypes in industrial settings (i.e., field testing), with a handoff to the energy sector through licensing, startups, and open-source mechanisms.
- **Significance:** CREDC will impact the foundational science and engineering approaches to Energy Delivery Systems (EDS) cyber security and resiliency as well as propagate a highly qualified student workforce to be industry-ready in the area of cybersecurity for energy delivery systems. Project results will include solutions that enhance resiliency as EDS systems encompass evolving cyber-technologies and changing EDS markets, a business case to build a culture of security in EDS sectors, and a self-sustaining consortium to maintain and advance improvements in EDS resiliency.

Schweitzer Engineering Laboratories

Watchdog and SDN Projects

- Primary Roadmap Milestone: 3.4 Self-configuring energy delivery system network architectures widely available.
- Project Description: The SEL projects establish deny-by-default whitelisted Ethernet communications at every hop and switch in the network. The projects included applied SDN architectures and multi-layer inspection to enable a programmable network infrastructure and then tested deployment with proactive traffic engineering that realized stronger cybersecurity, better performance, and enhanced situational awareness.
- Significance: SEL's projects have resulted in the world's first SDN solution for energy delivery control systems, which was commercially released under these two projects in 2016.

ABB, Inc.

Collaborative Defense of Transmission and Distribution and Protection and Control Device against Cyber Attacks (CODEF)

- Primary Roadmap Milestone: 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented.
- Project Description: The CODEF project is developing a distributed security domain layer that enables transmission and distribution grid protection and control devices to collaboratively defend against cyber-attacks. Leveraging distributed security extensions of the IEC 61850 communications protocol will allow protection and control relays to collaboratively validate that inputs, configuration changes, or power system data make sense for reliable grid operation.
- Significance: CODEF enhances utility network cybersecurity by enabling protection and control devices, both between and within substations, to verify that received communications support the current operational state of the power grid.

GRID PROTECTION ALLIANCE

ARMORE: Applied Resiliency for More Trustworthy Grid Operation

- **Primary Roadmap Milestone:** 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented.
- **Project Description:** The ARMORE project enables higher-speed secure peer-based communications while honoring current regulatory requirements for establishment of Electronic Security Perimeters (ESPs) for each critical substation.
- **Significance:** The project provides for greater overall security through enhancement of legacy energy sector protocols, with augmented security functionality to cover aspects like encryption, authentication, and access control throughout the utility infrastructure.

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

Energy Sector Security Appliances in a System for Intelligent, Learning Network Configuration Management and Monitoring (ESSENCE)

- **Primary Roadmap Milestone:** 4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available.
- **Project Description:** The ESSENCE project develops tools that facilitate more secure operational network management. Software defined networking (SDN) provides a solution to assist cooperatives with mapping their operational networks, analyzing traffic, and learning expected traffic flow to better inform human operators.
- **Significance:** As the electric industry increasingly migrates utility operational technology (OT) systems to virtualization and cloud-managed services, small utilities and electric cooperatives with limited resources could benefit from emerging software defined networking capabilities to automate the operational network response to a cyber compromise.

POSTER SESSIONS

ABB

- Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF)
- Cyber Attack Resilient HVDC System
- Multi-layered Resilient Microgrid Networks

Argonne National Laboratory

- A Resilient Self-Healing Cyber Security Framework for Power Grid

Brookhaven National Laboratory

- AIERCI Tool to Ensure Uninterrupted Energy Flow from Cyber Attacks Targeting Essential Forecasting Data for Grid Operations

Cybati

- A Metamorphic Cybersecurity Educational Platform

Electric Power Research Institute

- Secure Policy-Based Configuration Framework (PBCONF)

Foxguard Solutions

- Patch and Update Management Program for EDS

GE Global Research

- Cyber-Attack Detection & Accommodation for EDS

Grid Protection Alliance

- ARMORE: Applied Resiliency for More Trustworthy Grid Operation

Idaho National Laboratory

- Validation and Measuring Automated Response (VMAR)

Intel Federal

- Enhanced Security in Power System Edge

Iowa State University

- Autonomous Tools for Attack Surface Reduction

Los Alamos National Laboratory

- Quantum Security Modules for the Power Grid

Lawrence Berkeley National Laboratory

- Supporting Cyber Security of Power Distribution Systems by Detecting Differences Between Real-time Micro-Synchrophasor Measurements and Cyber-Reported SCADA

National Rural Electric Cooperative Association

- NRECA REACT Project
- Energy Sector Security Appliances in a System for Intelligent, Learning Network Configuration Management and Monitoring (ESSENCE)

Oak Ridge National Laboratory

- Cliques: CRL-less Revocation and Anonymous Authentication for the Smart Grid
- Timing Authentication Secured by Quantum Correlations (TASQC)

Pacific Northwest National Laboratory

- Automated, Disruption Tolerant Key Management System

Qubitekk, Inc.

- Automated, Disruption Tolerant Key Management System

Schweitzer Engineering Laboratories

- Secure SW Defined Radio
- Chess Master Project

Sandia National Laboratory

- Artificial Diversity and Defense Security (ADDSec)

United Technologies Research Center

- INGRESS, Integration of Renewables with Building & Electric Power

University of Arkansas

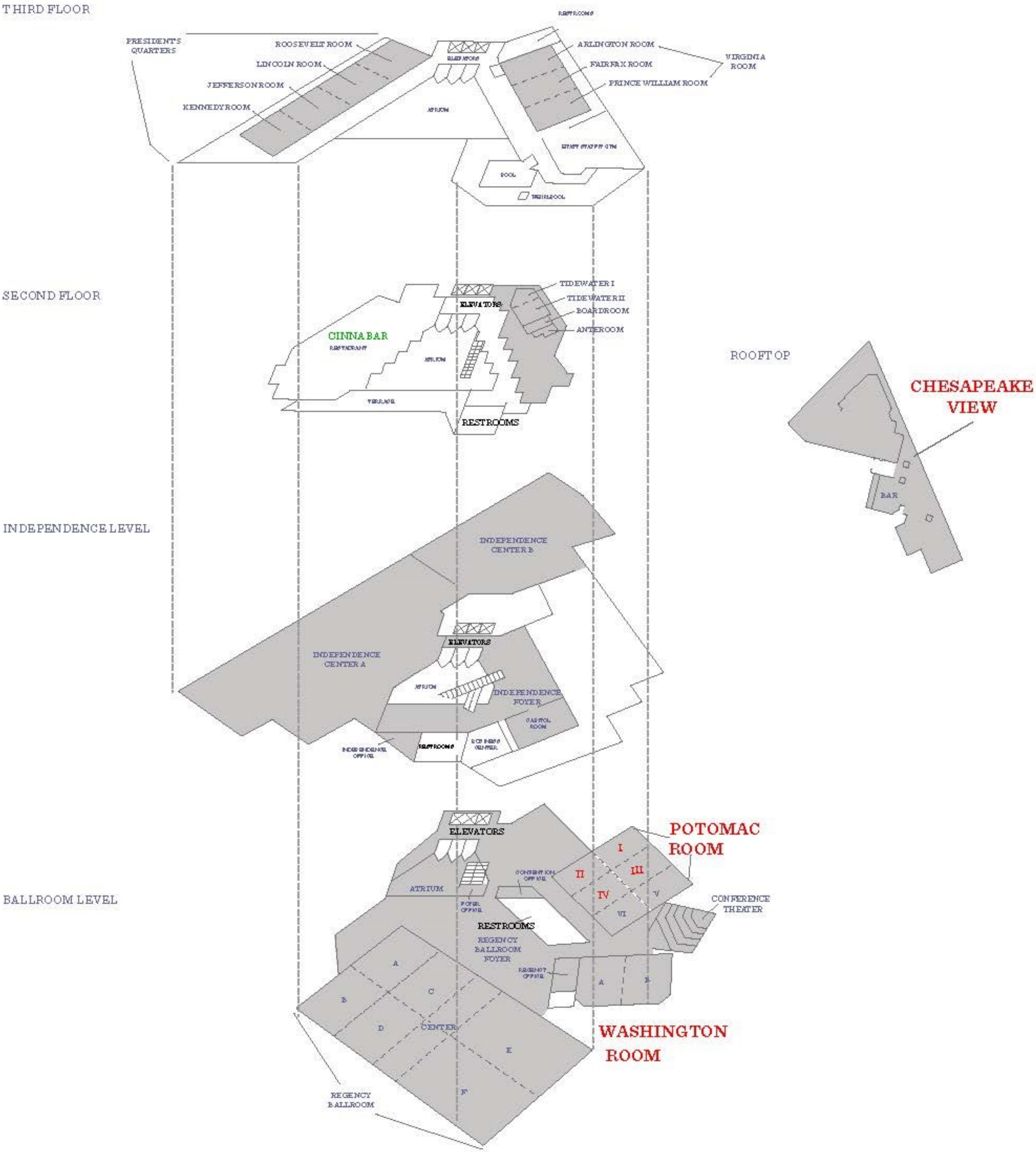
- Cybersecurity Center for Securing Electric Energy Delivery Systems (SEEDS)

University of Illinois at Urbana-Champaign

- Cyber Resilient Energy Delivery Consortium (CREDC)

Be sure to visit the poster sessions in Potomac I-II each day during the morning/afternoon breaks, and the networking event on Thursday evening.

HOTEL MAP


THIRD FLOOR
RESTROOMS
PRESIDENT'S QUARTERS
ROOSEVELT ROOM
LINCOLN ROOM
JEFFERSON ROOM
KENNEDY ROOM
ELEVATORS
ATRIUM
ARLINGTON ROOM
FAIRFAX ROOM
PRINCE WILLIAM ROOM
VIRGINIA ROOM
HYATT STAY FIT GYM
POOL
WHIRLPOOL
SECOND FLOOR
ELEVATORS
TIDEWATER I
TIDEWATER II
BOARDROOM
ANTEROOM
CINNABAR
RESTAURANT
ATRIUM
TERRACE
RESTROOMS
ROOFTOP
CHESAPEAKE VIEW
BAR
INDEPENDENCE LEVEL
INDEPENDENCE CENTER B
ELEVATORS
INDEPENDENCE CENTER A
ATRIUM
INDEPENDENCE FOYER
CAPITOL ROOM
INDEPENDENCE OFFICE
RESTROOMS
BUSINESS CENTER
BALLROOM LEVEL
ELEVATORS
POTOMAC ROOM
I
II
III
IV
V
VI
CONVENTION OFFICE
ATRIUM
FOYER OFFICE
CONFERENCE THEATER
RESTROOMS
REGENCY BALLROOM FOYER
REGENCY OFFICE
A
B
C
D
CENTER
E
F
A
B
WASHINGTON ROOM
REGENCY BALLROOM

For more information about the CEDS Program, please visit:
www.controlsystemsroadmap.net
Short URL: goo.gl/TWifTQ

ie Roadmap
interactive energy Roadmap to Achieve
Energy Delivery Systems Cybersecurity