U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Research Exploring Malware in Energy DeliverY Systems (REMEDYS)

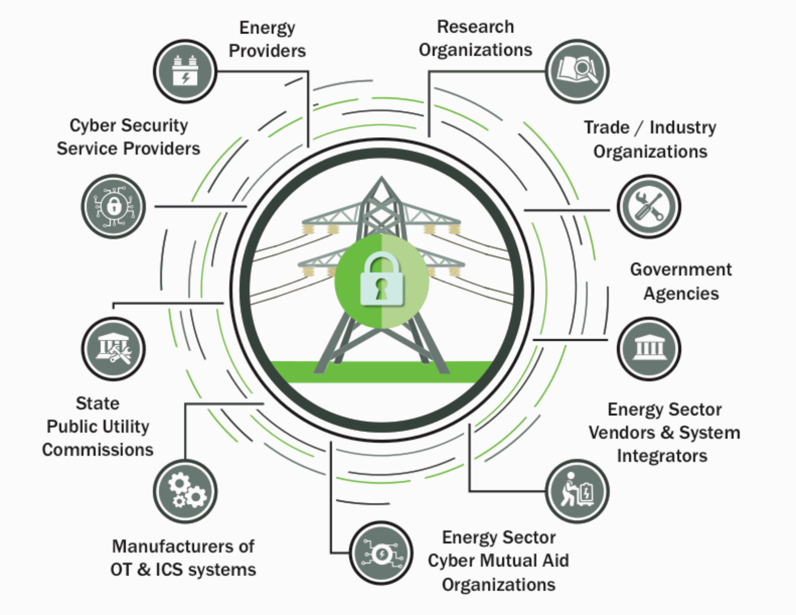
ORNL/PNNL

Marissa Morales-Rodriguez/Jess Smith

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: REMEDYS



Energy Providers
Research Organizations
Cyber Security Service Providers
Trade / Industry Organizations
Government Agencies
State Public Utility Commissions
Energy Sector Vendors & System Integrators
Manufacturers of OT & ICS systems
Energy Sector Cyber Mutual Aid Organizations

Objective

- Research, develop, and evaluate, the optimum organizational structures for the coordination the nation’s multiple energy sector stakeholders in the rapid research, development and distribution of mitigations solutions.

Phase 1 Schedule

- October 2017 – September 2020
- Industry Workshop/Nov 2017
- Landscape Evaluation/July 2018
- Initial Organizational Models Developed & Evaluated/ Aug-Nov 2018

Total Value of Award:	**$5M**
Funds Expended to Date:	**23.64%**
Performer:	**PNNL/ORNL**
Partners:	**Jim Fama, CREDC-MIT, FoxGuard, Brixon, LLNL, CURENT, EPB, Duke Energy, EPRI, Schneider Electric, Exxon Mobile, U of Illinois, NRECA, Avista, WAPA, Siemens, SEL, Cisco Talos, ANG Consulting, Nevermore Security, WSU**

Advancing the State of the Art (SOA)

Describe current "state of the art"

- Currently, stakeholders work in isolation to develop appropriate mitigation when malware is discovered

Describe the feasibility of your approach

- This project enables an ecosystem of trust within stakeholders and an optimum structure to promote team work to develop mitigation solutions utilizing the Nation's public-private resources

Describe why your approach is better than the SOA

- This approach engages subject matter experts across the energy sector including, but not limited to, industry, asset owners & operators, academia, national laboratories

Describe how the end user of your approach will benefit

- The end user will receive effective mitigation solutions quicker reducing the window of opportunity for the adversary

Advancing the State of the Art (SOA)

Describe how your approach will advance the cybersecurity of energy delivery systems

We are identifying and validating organization structures and approaches that will:

- Decrease the time it takes to develop and make available mitigations to newly discovered malware
- Bring together public and private sector entities in a collaborative partnership
- Create and test organizational hypotheses upon which to build a sustainable organization

Progress to Date

Major Accomplishments

- Hosted a Roadmap Exercise with over 30 Industry Partners – November 2017
- Established a Working Group & Industry Advisory Board – June 2018
- Evaluation of the Current Organizational Landscape – July 2018
- Develop a Value Proposition & Flyers for stakeholder engagement – May 2018
- Engagement with ESCC's CMA Working Group – August 2018
- Presentation at the ICS Joint Working Group – August 2018
- Initial Organizational Models Hypothesis Developed and Evaluated – November 2018
- Coordinated research and deliverables between ORNL, PNNL, and MIT

Challenges to Success

Challenge 1: Coordination

- Discovering and coordinating the many sector partners required to achieve a unified vision and make this future organization a success

Challenge 2: Technical

- Understanding how to construct organizational models based on literature survey and analytics approach to fit the needs of the target audience
- Leverage the capabilities of existing organizations rather than duplication
- Design and develop an evaluation criteria for the selection of organizational models that will research, develop, and make mitigation available
- Repeatable method for evaluating potential organization structures using existing malware incidents as use case scenarios

Challenge 3: Process

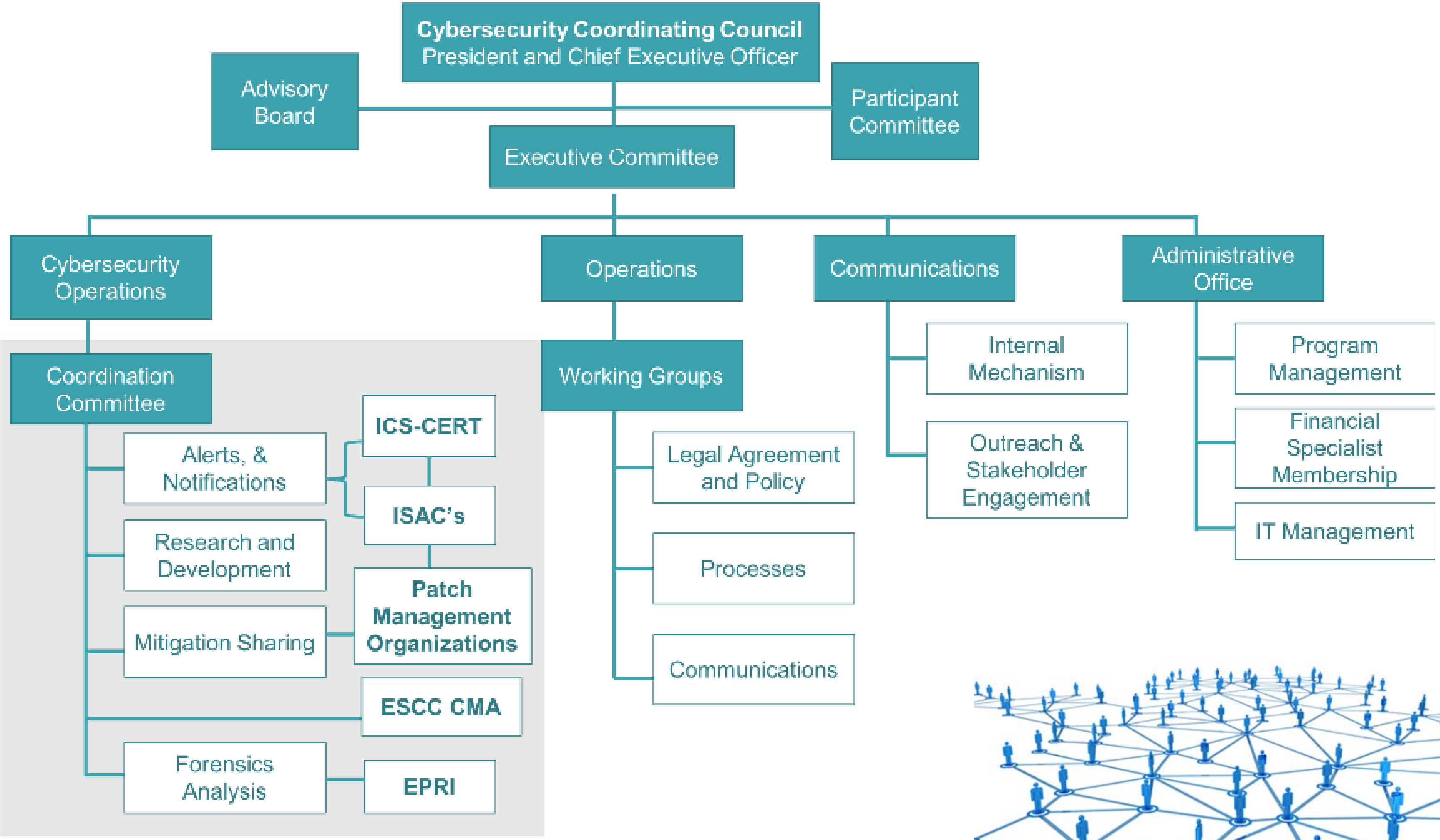
- Identification of the legal mechanisms and data protection to enable the process for mitigation sharing between the different energy stakeholders

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- What category is the targeted end user for the technology or knowledge? (e.g., Asset Owner, Vendor, OEM)
  - This project targets all energy stakeholders, but initially the project was focused on private sector engagement. Research showed that in order to achieve this, the larger utilities must support this initiative
- What are your plans to gain industry acceptance?
  - Outreach strategy was developed and implementation is ongoing
  - Engagement with the ESCC CMA will allow the team to gain access to industry and understand details of the current needs
  - Results from the ICS JWG presentation were generally positive

Initial Organizational Models



Cybersecurity Coordinating Council
President and Chief Executive Officer

Advisory Board

Participant Committee

Executive Committee

Cybersecurity Operations

Coordination Committee

- Alerts, & Notifications
- Research and Development
- Mitigation Sharing
- Forensics Analysis

ICS-CERT

ISAC's

Patch Management Organizations

ESCC CMA

EPRI

Operations

Working Groups

- Legal Agreement and Policy
- Processes
- Communications

Communications

- Internal Mechanism
- Outreach & Stakeholder Engagement

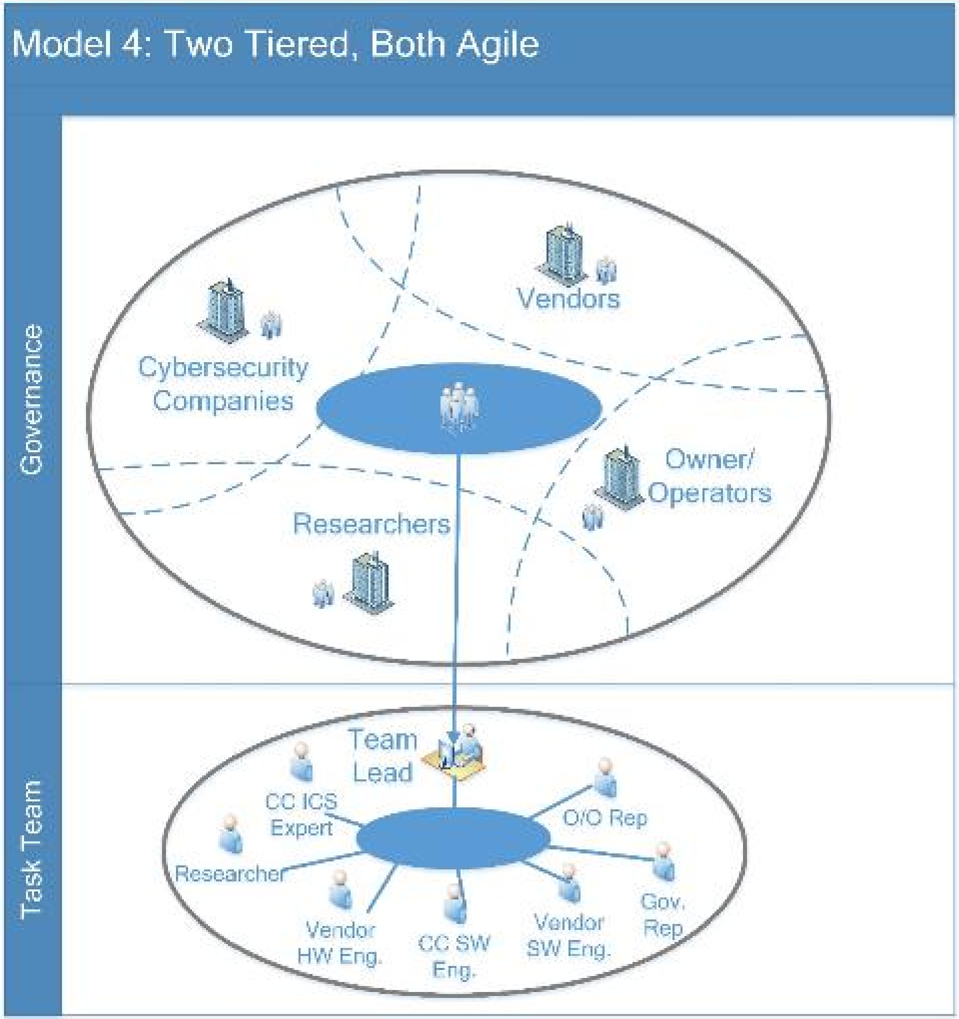
Administrative Office

- Program Management
- Financial Specialist Membership
- IT Management

DRAFT

Initial Organizational Models (Cont’d)

- Two tiered, fully agile
- Minimal financial overhead
- Takes advantage of existing ESCC CMA while also offering task teams
- Response times may be slowed at Governance level



U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Next Steps for REMEDYS

Task

PHASE 1: Project Initiation

- Working Groups and Industry Advisory Board
- Value proposition
- Initial organizational analysis
- Outreach

PHASE 2: Organizational Research & Analysis

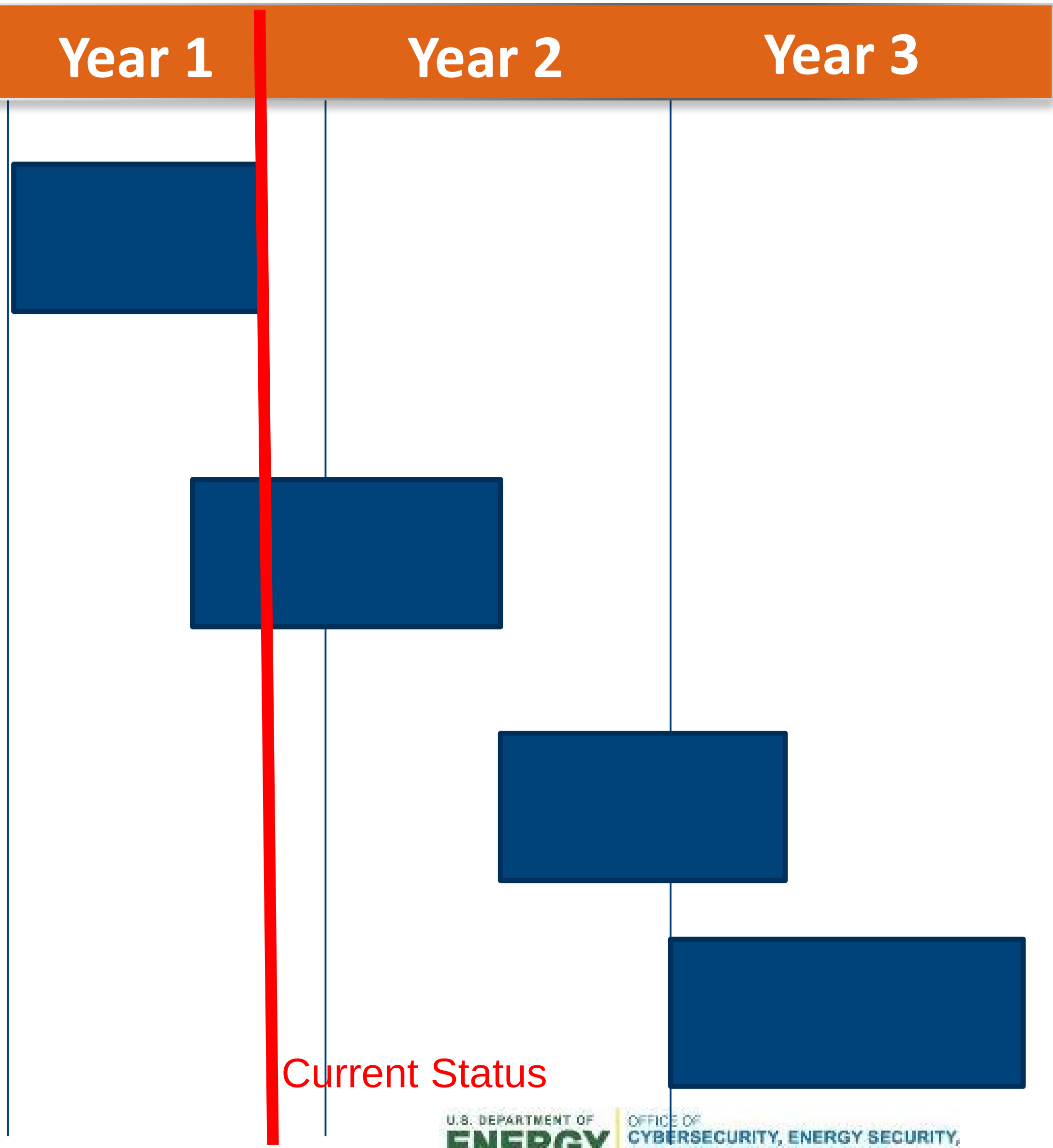
- Continued organizations landscape analysis
- Organizational requirements and use cases
- Organizational hypothesis
- Test and validation of hypothesis

PHASE 3: Organizational Models Hypothesis

- New hypothesis or refinements of existing ones
- Establish a secure communication framework
- Case studies: Test and Validation
- Technology transfer plan, CONOPS, Charter, Value Proposition

PHASE 4: Project Completion

- Final Organization Structure
- Transition to Practice



Thank You

Pacific Northwest
NATIONAL LABORATORY

Bary Elison
Project Manager
Bary.Elison@PNNL.gov

Jess Smith
Principal Investigator
Jess.Smith@PNNL.gov

OAK RIDGE
National Laboratory

Peter Fuhr
Project Manager
fuhrpl@ornl.gov

Marissa Morales-Rodriguez
Principal Investigator
moralesme@ornl.gov

MIT MANAGEMENT
SLOAN SCHOOL

Keri Pearlson
Principal Investigator
KeriP@mit.edu

U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE