Grid Security & Modernization Webinar - Cyber Security

MGA

America's Smartland

Midwestern Governors Association

June 27, 2018

U.S. DEPARTMENT OF ENERGY

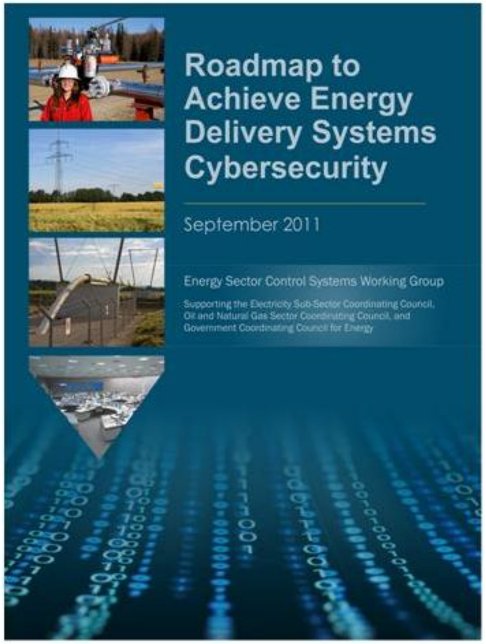
Office of Cybersecurity, Energy Security and Emergency Response

U.S. Department of Energy Cybersecurity for Energy Delivery Systems Research Partnerships

James Briones, CISSP

June 27, 2018

Roadmap – Framework for Collaboration



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

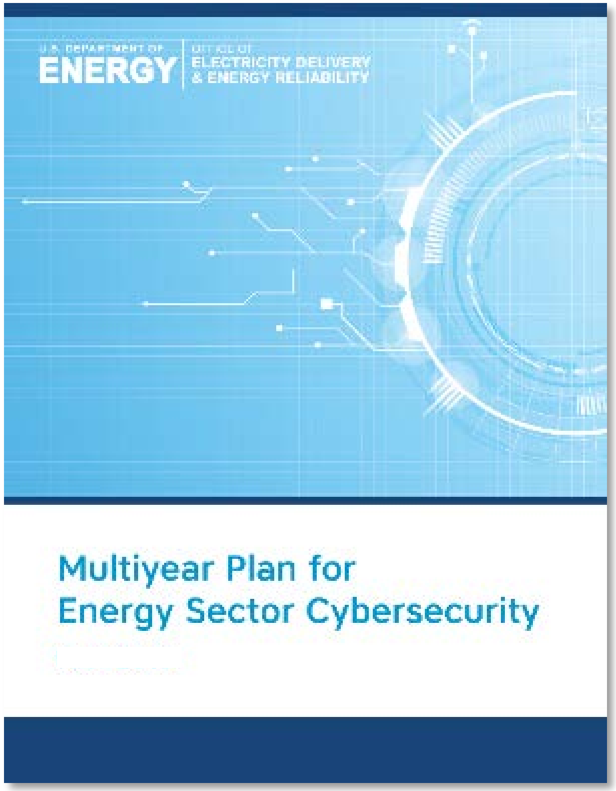
- *Energy Sector's* synthesis of energy delivery systems security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in energy delivery systems security

Roadmap Vision

Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

For more information go to: https://energy.gov/oe/cybersecurity-critical-energy-infrastructure

DOE Multi-Year Plan for Energy Sector Cybersecurity

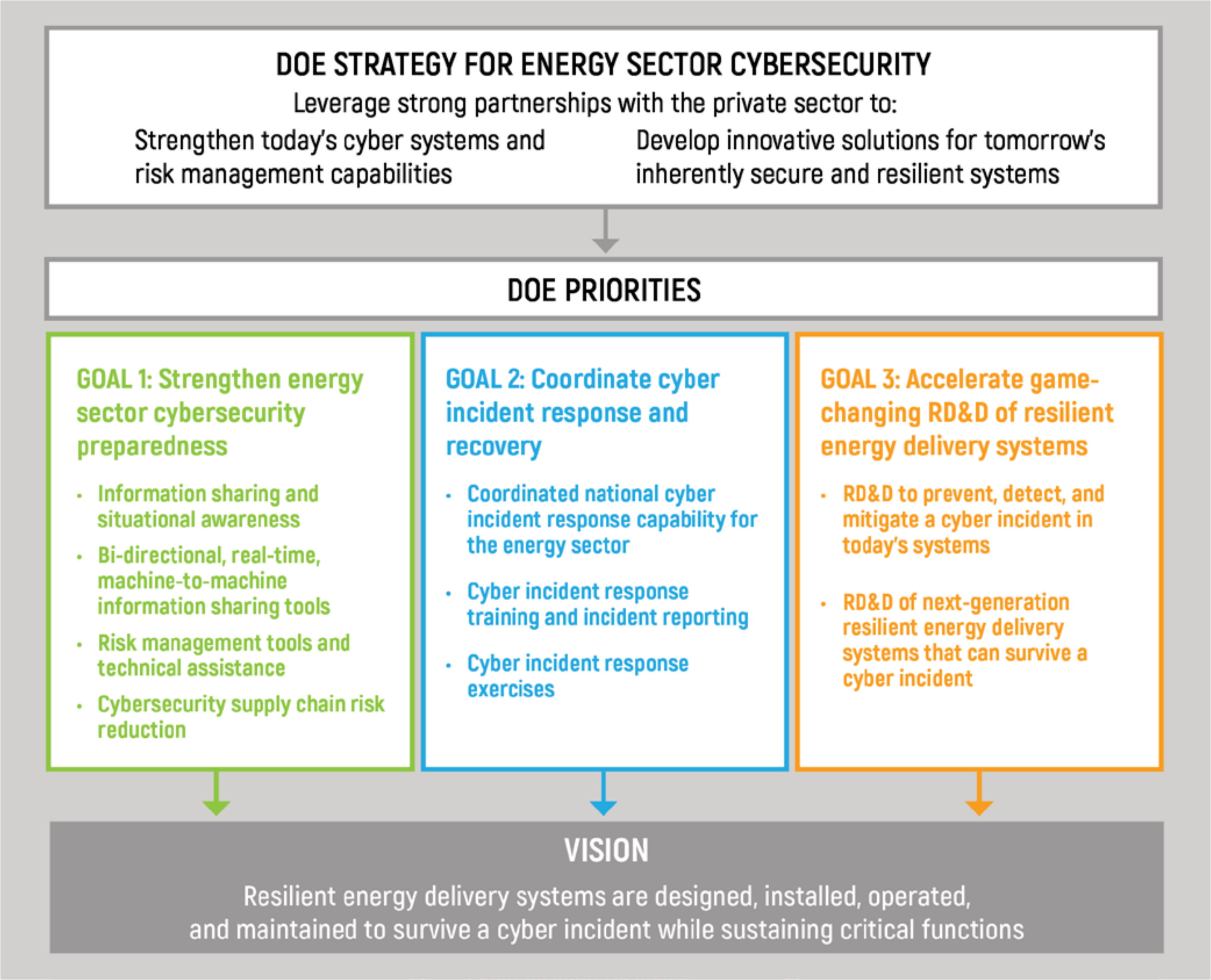


U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

Multiyear Plan for Energy Sector Cybersecurity

- **DOE's strategy** for partnering with industry to protect U.S. energy system from cyber risks
- **Guided by direct industry input** on cybersecurity needs and priorities
- **Market-based approach** encourages investment and cost-sharing of promising technologies and practices
- **Establishes goals, objectives, and performance targets** to improve both near- and long-term energy cybersecurity

DOE Strategy for Energy Sector Cybersecurity



DOE STRATEGY FOR ENERGY SECTOR CYBERSECURITY

Leverage strong partnerships with the private sector to:

Strengthen today's cyber systems and risk management capabilities

Develop innovative solutions for tomorrow's inherently secure and resilient systems

DOE PRIORITIES

GOAL 1: Strengthen energy sector cybersecurity preparedness

- Information sharing and situational awareness
- Bi-directional, real-time, machine-to-machine information sharing tools
- Risk management tools and technical assistance
- Cybersecurity supply chain risk reduction

GOAL 2: Coordinate cyber incident response and recovery

- Coordinated national cyber incident response capability for the energy sector
- Cyber incident response training and incident reporting
- Cyber incident response exercises

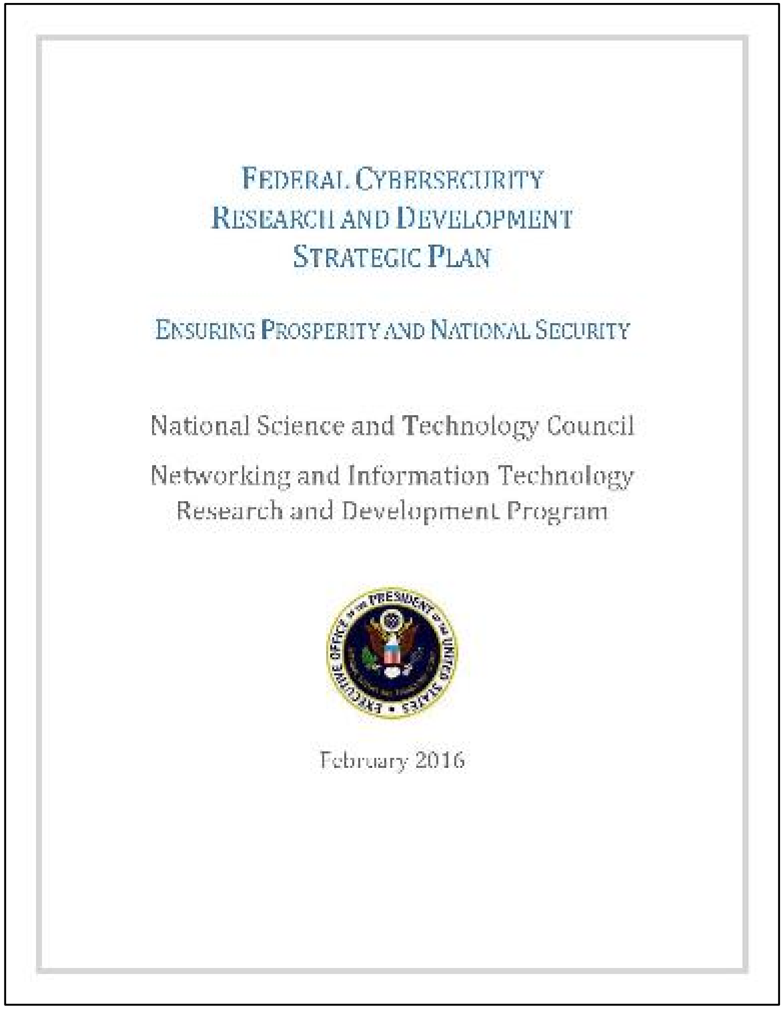
GOAL 3: Accelerate game-changing RD&D of resilient energy delivery systems

- RD&D to prevent, detect, and mitigate a cyber incident in today's systems
- RD&D of next-generation resilient energy delivery systems that can survive a cyber incident

VISION

Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions

Federal Cybersecurity Research and Development Strategic Plan



Federal Cybersecurity Research and Development Strategic Plan

Ensuring Prosperity and National Security

National Science and Technology Council

Networking and Information Technology Research and Development Program

February 2016

- ✓ **Deter.** The ability to efficiently discourage malicious cyber activities by measuring and increasing costs to adversaries carrying out such activities, diminishing the spoils, and increasing risks and uncertainty for potential adversaries.

- ✓ **Protect.** The ability of components, systems, users, and critical infrastructure to efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability, and accountability.

- ✓ **Detect.** The ability to efficiently detect, and even anticipate, adversary decisions and activities, given that perfect security is not possible and systems should be assumed to be vulnerable to malicious cyber activities.

- ✓ **Adapt.** The ability of defenders, defenses, and infrastructure to dynamically adapt to malicious cyber activities, by efficiently reacting to disruption, recovering from damage, maintaining operations while completing restoration, and adjusting to thwart similar future activity.

Coordination with Other Federal Cybersecurity R&D Programs

- Primary mechanism for U.S. Government, unclassified Networking and IT R&D (NITRD) coordination
- Supports Networking and Information Technology policy making in the White House Office of Science and Technology Policy (OSTP)

DARPA
U.S. Department of Homeland Security
Department of Energy · United States of America
NNSA
National Nuclear Security Administration
United States Environmental Protection Agency
National Institutes of Health
NASA
NIST
The Office of the National Coordinator for Health Information Technology
NOAA
National Oceanic and Atmospheric Administration · U.S. Department of Commerce
AHRQ
NSF
National Archives
National Security Agency · United States of America
National Reconnaissance Office · United States of America
Department of Defense · United States of America

CEDS Encourages Partnerships

Asset Owners/Operators

- Ameren
- Arkansas Electric Cooperatives Corporation
- Avista
- Burbank Water and Power
- BPA
- CenterPoint Energy
- Chevron
- ComEd
- Dominion
- Duke Energy
- Electric Reliability Council of Texas
- Entergy
- FirstEnergy
- FP&L
- HECO
- Idaho Falls Power
- Inland Empire Energy
- NIPSCO
- Omaha Public Power District
- Orange & Rockland Utility
- Pacific Gas & Electric
- PacifiCorp
- Peak RC
- PJM Interconnection
- Rochester Public Utilities
- Sacramento Municipal Utilities District
- San Diego Gas and Electric
- Sempra
- Snohomish PUD
- Southern Company
- Southern California Edison
- TVA
- Virgin Islands Water and Power Authority
- WAPA
- Westar Energy
- WGES

Solution Providers

- ABB
- Alstom Grid
- Applied Communication Services
- Applied Control Solutions
- Cigital, Inc.
- Critical Intelligence
- Cybati
- Eaton
- Enernex
- EPRI
- Foxguard Solutions
- GE
- Grid Protection Alliance
- Grimm
- Honeywell
- ID Quantique
- Intel
- NexDefense
- OPAL-RT
- Open Information Security Foundation
- OSIsoft
- Parsons
- Power Standards Laboratory
- Qubitekk
- RTDS Technologies Inc.
- Schneider Electric
- SEL
- Siemens
- Telvent
- Tenable Network Security
- Utility Advisors
- Utility Integration Solutions
- UTRC
- Veracity
- ViaSat

Academia

- Arizona State University
- Carnegie Mellon University
- Dartmouth College
- Florida International University
- Georgia Institute of Technology
- Illinois Institute of Technology
- Iowa State University
- Lehigh University
- Massachusetts Institute of Technology
- Oregon State University
- Rutgers University
- Tennessee State University
- Texas A&M EES
- University of Arkansas
- University of Arkansas-Little Rock
- University of Buffalo - SUNY
- University of Illinois
- UC Davis
- UC Berkeley
- University of Houston
- University of Tennessee-Knoxville
- University of Texas at Austin
- Washington State

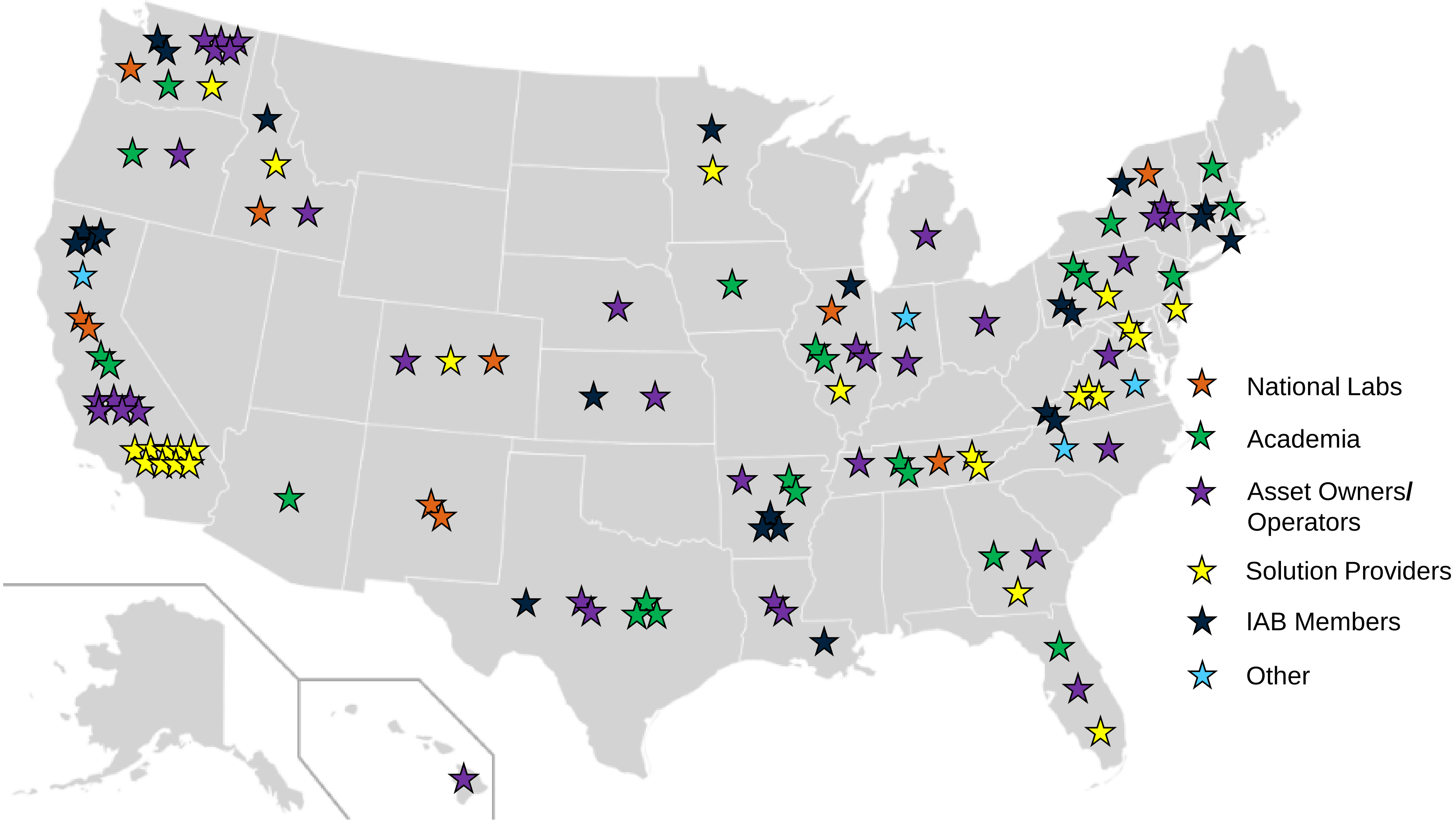
National Labs

- Argonne National Laboratory
- Brookhaven National Laboratory
- Idaho National Laboratory
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Laboratory
- Los Alamos National Laboratory
- National Renewable Energy Laboratory
- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories

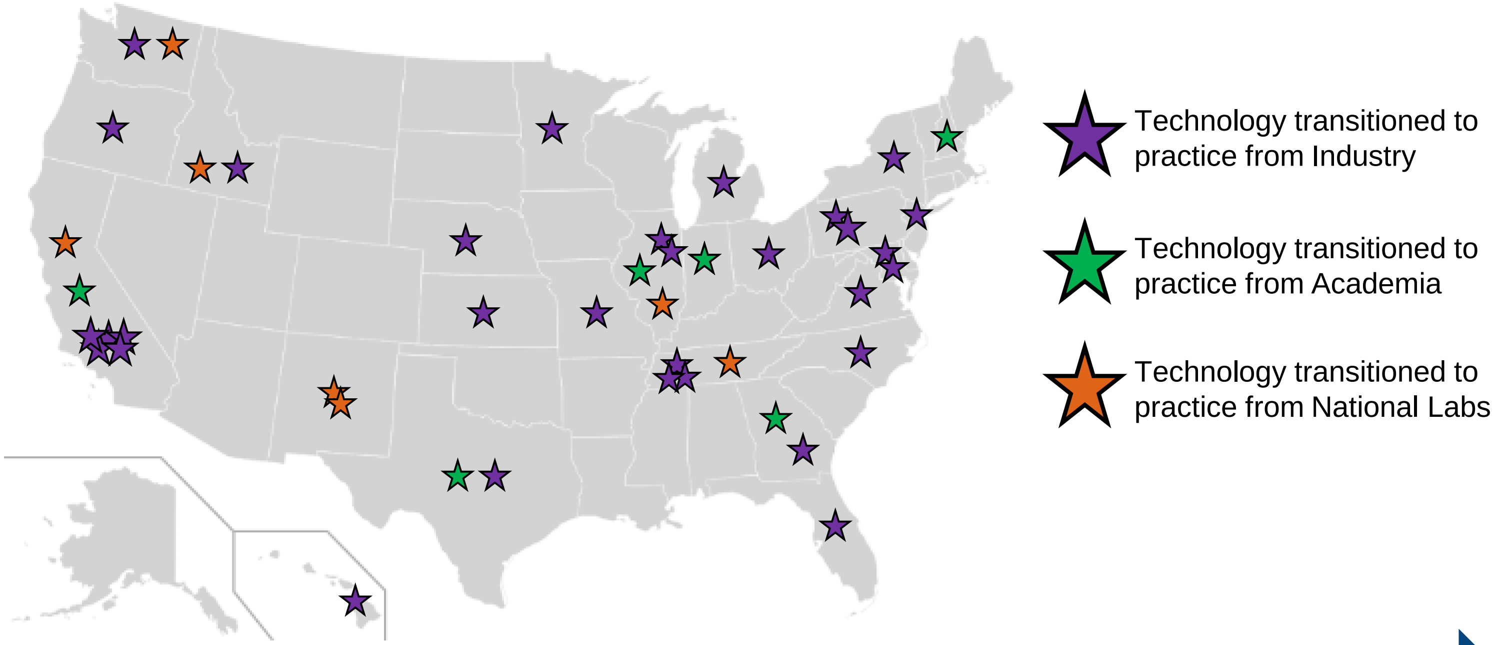
Other

- Energy Sector Control Systems Working Group
- International Society of Automation
- NESCOR
- NRECA
- Open Information Security Foundation

CEDS Encourages Partnerships



CEDS Technologies Transitioned to Practice


Technology transitioned to practice from Industry
Technology transitioned to practice from Academia
Technology transitioned to practice from National Labs

DOE PIPELINE: Transition R&D to Practice in the Energy Sector

- CEDS R&D supports advanced technologies in the earlier, high-risk/high-reward research stages, for which a business case cannot readily be established by a private sector company and yet are needed to address a national security imperative

- Builds R&D pipeline through partnerships with energy sector utilities, vendors, universities, national laboratories, and providers of cybersecurity services to the energy sector

Results

- **Successfully transitioned more than 35 tools and technologies used TODAY** to help critical energy infrastructure survive a cyber incident

- **Approximately 1,000 utilities in 50 states have purchased technologies developed by CEDS**

Cybersecurity that Improves Energy Delivery System Performance

- Quantum Key Distribution (QKD) system that provides cutting-edge security while greatly simplifying the generation, maintenance, and distribution of encryption keys used in energy delivery systems. Uses quantum entangled photons to guarantee tamper detection and provide encryption to secure against even a quantum computing attack. http://qubitekk.com/security/

- Securing advanced metering infrastructure (AMI) and distribution automation (DA) wireless mesh networks with continuous monitoring, anomaly and intrusion detection and prevention. https://www.vencorelabs.com/smartgrid/

- Securing field devices using strong anti-malware and whitelist protection that ensures only approved applications/services/executable are ran and executed and all others all blocked. https://goo.gl/zvL5GF

Cybersecurity that Improves Energy Delivery System Performance

- A solution to streamline the challenging task of patching/updating devices used in energy delivery control systems. This is particularly important in cases when patches and updates mitigates security vulnerabilities that may be exploited by the adversary. https://www.icsupdate.com/

- Technology that enhances the cyber/physical security that protects both electronic and physical perimeter by monitoring and controlling device assess. https://goo.gl/YTA88J

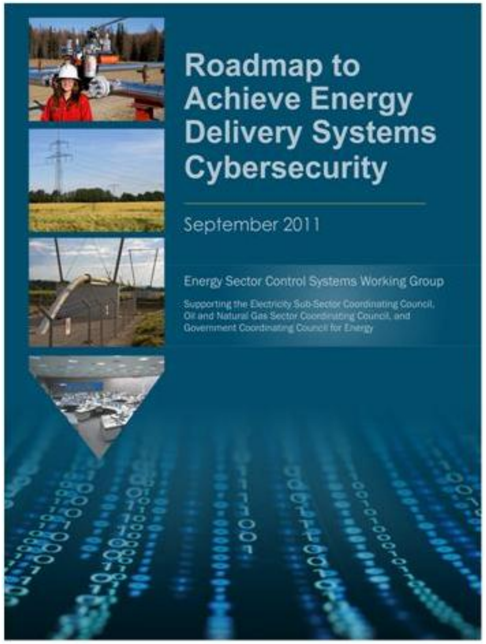
- Software Defined Networking technology for Energy delivery network that keeps working, even during a cyber-attack, by automatically redirecting communications along a pre-selected, pre-engineered alternative path. https://selinc.com/solutions/p/software-defined-network/

For More Information, Please Contact:

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security and Emergency Response

Carol Hawk
Deputy Assistant Secretary (Acting)
Cybersecurity for Energy Delivery Systems
Carol.Hawk@hq.doe.gov
202-586-3247

James Briones, CISSP
Engineer – Energy Systems Security Specialist
Cybersecurity for Energy Delivery Systems (R&D)
James.Briones@netl.doe.gov
304-285-5229



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

Visit:

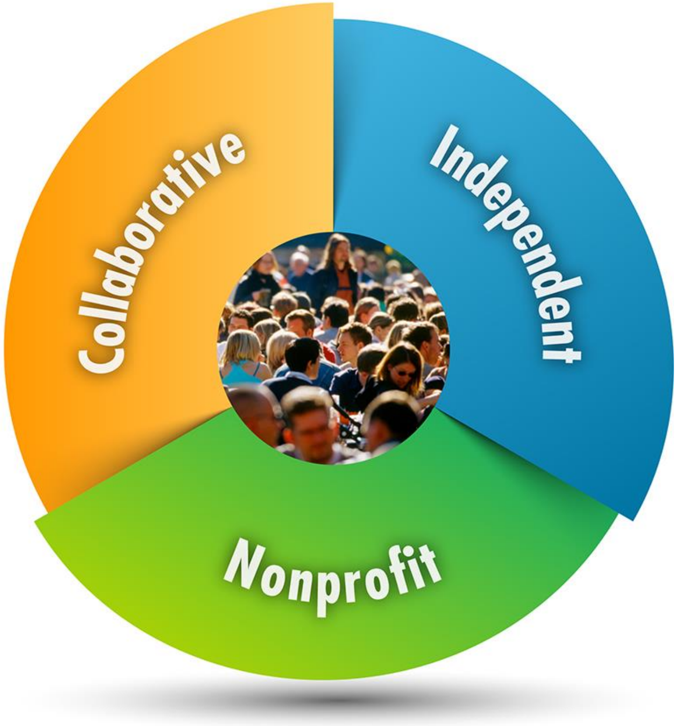
https://energy.gov/oe/cybersecurity-critical-energy-infrastructure

EPRI Security Metrics for the Electric Sector

Candace Suh-Lee, CISSP, CISA
Principal Technical Leader – Cyber Security
csuh-lee@epri.com

MGA Webinar
June 5, 2018

About the Electric Power Research Institute



Independent

Objective, scientifically based results address reliability, efficiency, affordability, health, safety, and the environment

Nonprofit

Chartered to serve the public benefit

Collaborative

Bring together scientists, engineers, academic researchers, and industry experts

Industry Trends Impacting Cyber Security Risk

Generation, Transmission & Distribution

- Real-time situational awareness
- Dynamic supply / demand balancing with DER (DERMS)
- Mobile workforce
- Increased automation and communications

Customer

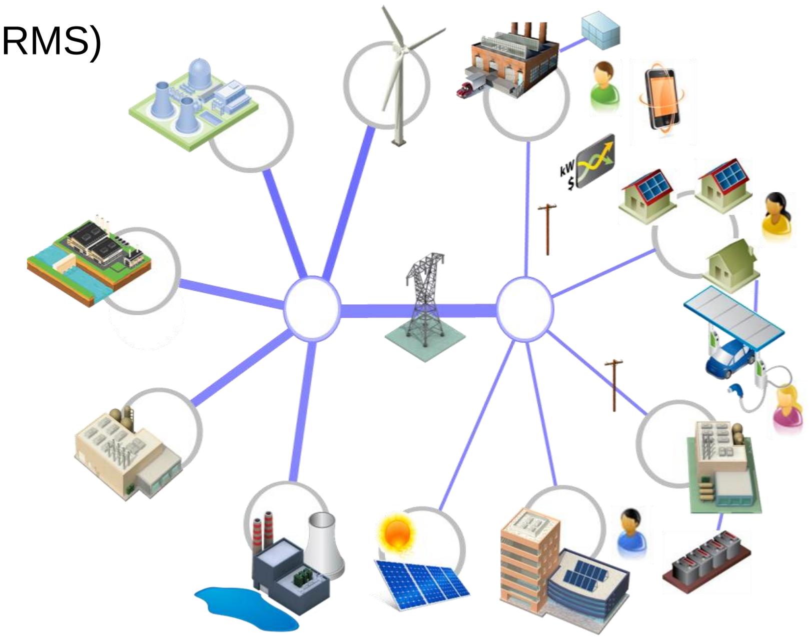
- Self generation (Solar PV, Storage,..)
- Electric vehicles
- IoT devices

Third Parties

- DER and DR aggregators

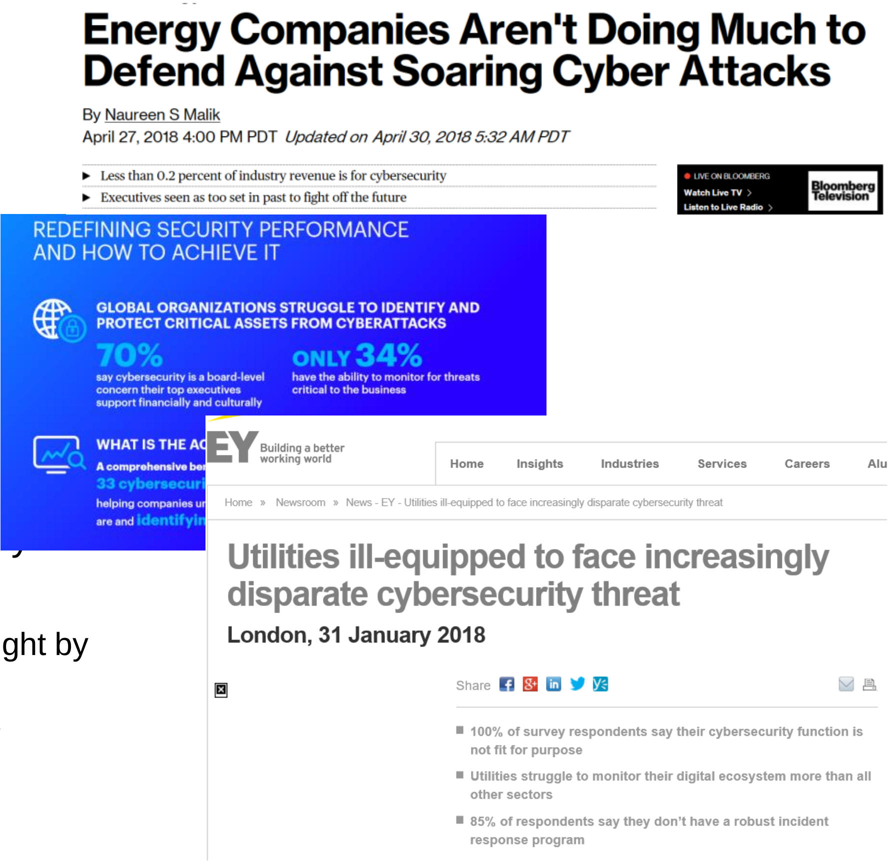
National Security/Resiliency Mindset

- Malicious attack or natural catastrophe



Cyber Security Investment in Electric Utilities

- Unmet Need by Electric Utilities in Cyber Security
  - Congressional Testimony of Aaron T. Ford, PSEG
  - PG&E State of the Grid Report 2017
- Cyber Security Investment by Utilities Lagging
  - Bloomsburg News, April 2018
  - E&Y News Release, Jan 2018
  - 2017 Accenture Security Index
- Why there is not enough investment in cyber security
  - Not clear return
  - No standard methodology to quantify risk reduction brought by the investment
  - Unclear how to prioritize - Which one is most important?
  - Concerns for technology debt



Energy Companies Aren't Doing Much to Defend Against Soaring Cyber Attacks

By Naureen S Malik

April 27, 2018 4:00 PM PDT *Updated on April 30, 2018 5:32 AM PDT*

- Less than 0.2 percent of industry revenue is for cybersecurity
- Executives seen as too set in past to fight off the future

REDEFINING SECURITY PERFORMANCE AND HOW TO ACHIEVE IT

GLOBAL ORGANIZATIONS STRUGGLE TO IDENTIFY AND PROTECT CRITICAL ASSETS FROM CYBERATTACKS

70% say cybersecurity is a board-level concern their top executives support financially and culturally

ONLY 34% have the ability to monitor for threats critical to the business

WHAT IS THE AC

A comprehensive be

33 cybersecuri

helping companies u

are and identifyin

Home » Newsroom » News - EY - Utilities ill-equipped to face increasingly disparate cybersecurity threat

Utilities ill-equipped to face increasingly disparate cybersecurity threat

London, 31 January 2018

- 100% of survey respondents say their cybersecurity function is not fit for purpose
- Utilities struggle to monitor their digital ecosystem more than all other sectors
- 85% of respondents say they don't have a robust incident response program

EPRI Cyber Security Metrics for the Electric Sector

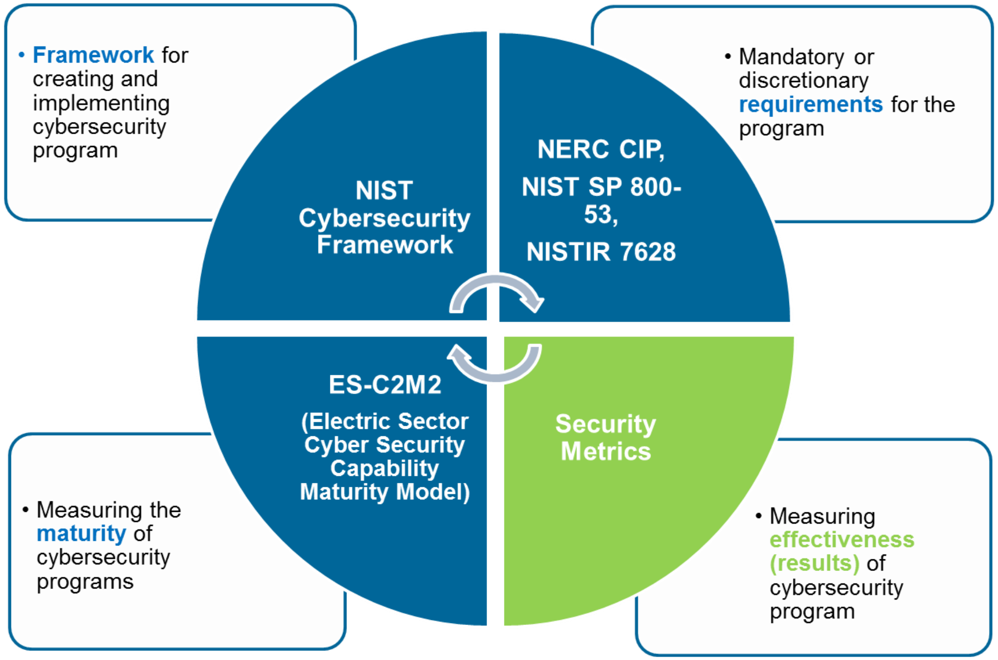
Project Objective

Create meaningful and engineering-based security metrics for the electric sector. These metrics must:

1. Be based on **quantitative, repeatable data**
2. Be **independent of compliance** to mandatory standards
3. Allow for **tailoring across the utility**, including various business units, functions, and ownership structures
4. Consider **differences between IT and OT** architectures
5. Communicate the **state of cyber security** to different stakeholders

Advantages of Security Metrics

- Accurate and clear reporting of security posture
- Support continuous improvement beyond the compliance
- Accumulation of knowledge for the data-driven security operations

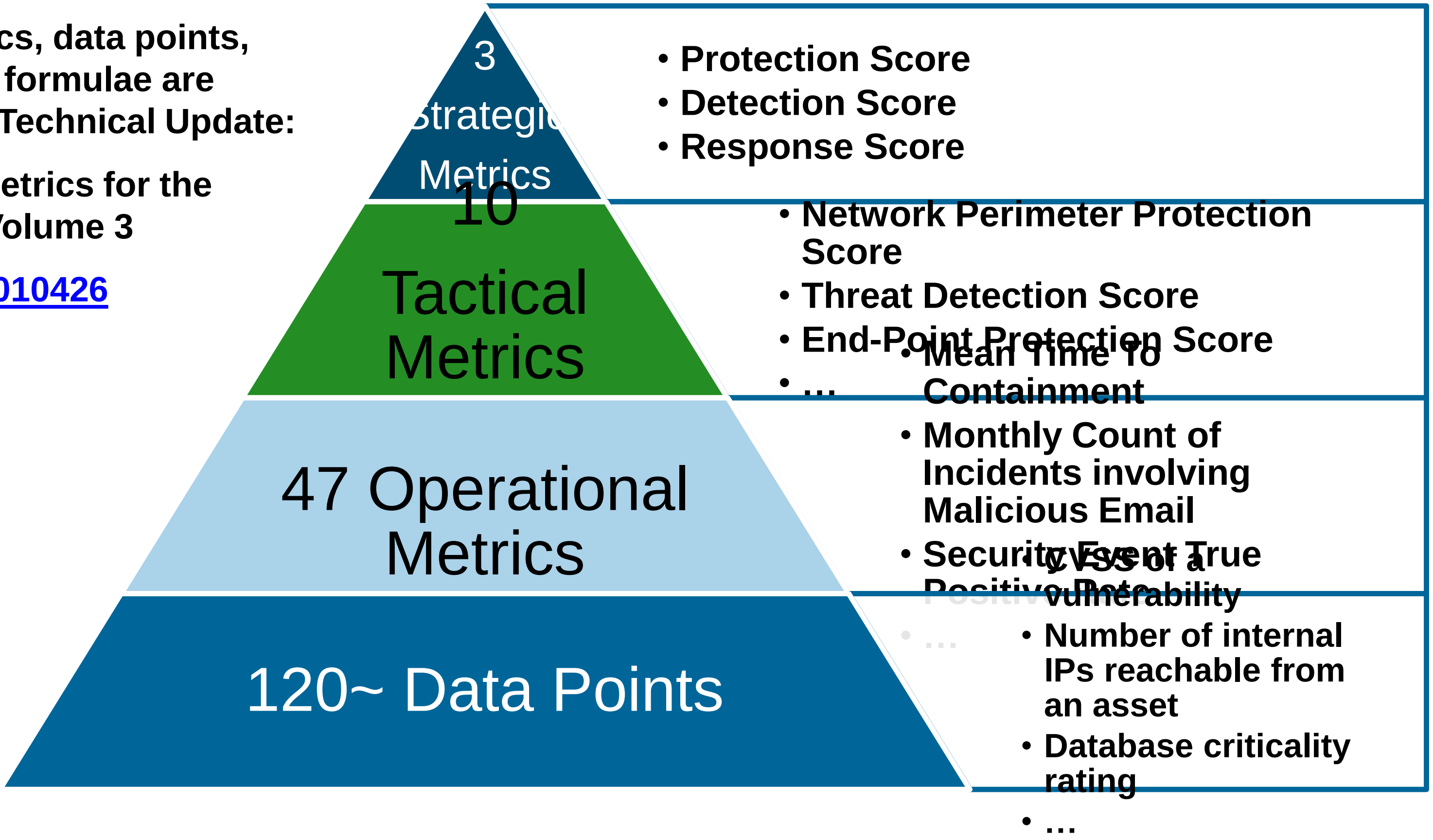

• Framework for creating and implementing cybersecurity program
NIST Cybersecurity Framework
• Mandatory or discretionary requirements for the program
NERC CIP,
NIST SP 800-53,
NISTIR 7628
• Measuring the maturity of cybersecurity programs
ES-C2M2
(Electric Sector Cyber Security Capability Maturity Model)
Security Metrics
• Measuring effectiveness (results) of cybersecurity program

EPRI’s Security Metrics

Full lists of metrics, data points, descriptions and formulae are included in 2017 Technical Update:

Cyber Security Metrics for the Electric Sector: Volume 3

Product ID: 3002010426 (www.epri.com)



3 Strategic Metrics

- **Protection Score**
- **Detection Score**
- **Response Score**

10 Tactical Metrics

- **Network Perimeter Protection Score**
- **Threat Detection Score**
- **End-Point Protection Score**
- **…**

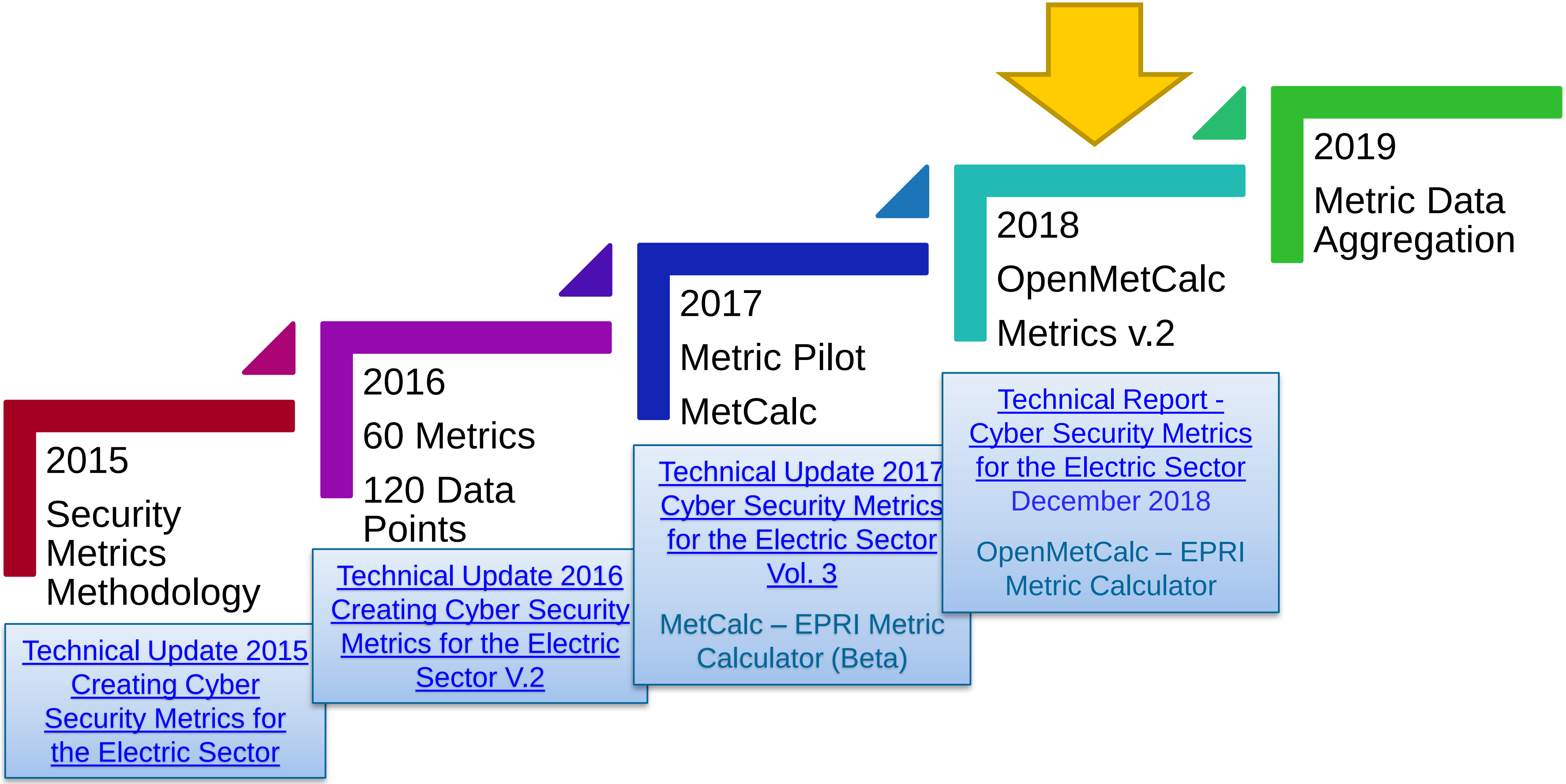
47 Operational Metrics

- **Mean Time To Containment**
- **Monthly Count of Incidents involving Malicious Email**
- **Security Event True Positive Rate**
- **…**

120~ Data Points

- **CVSS of a Vulnerability**
- **Number of internal IPs reachable from an asset**
- **Database criticality rating**
- **…**

Multi-year Project Plan / Deliverables



2015

Security Metrics Methodology

Technical Update 2015 Creating Cyber Security Metrics for the Electric Sector

2016

60 Metrics

120 Data Points

Technical Update 2016 Creating Cyber Security Metrics for the Electric Sector V.2

2017

Metric Pilot

MetCalc

Technical Update 2017 Cyber Security Metrics for the Electric Sector Vol. 3

MetCalc – EPRI Metric Calculator (Beta)

2018

OpenMetCalc

Metrics v.2

Technical Report - Cyber Security Metrics for the Electric Sector

December 2018

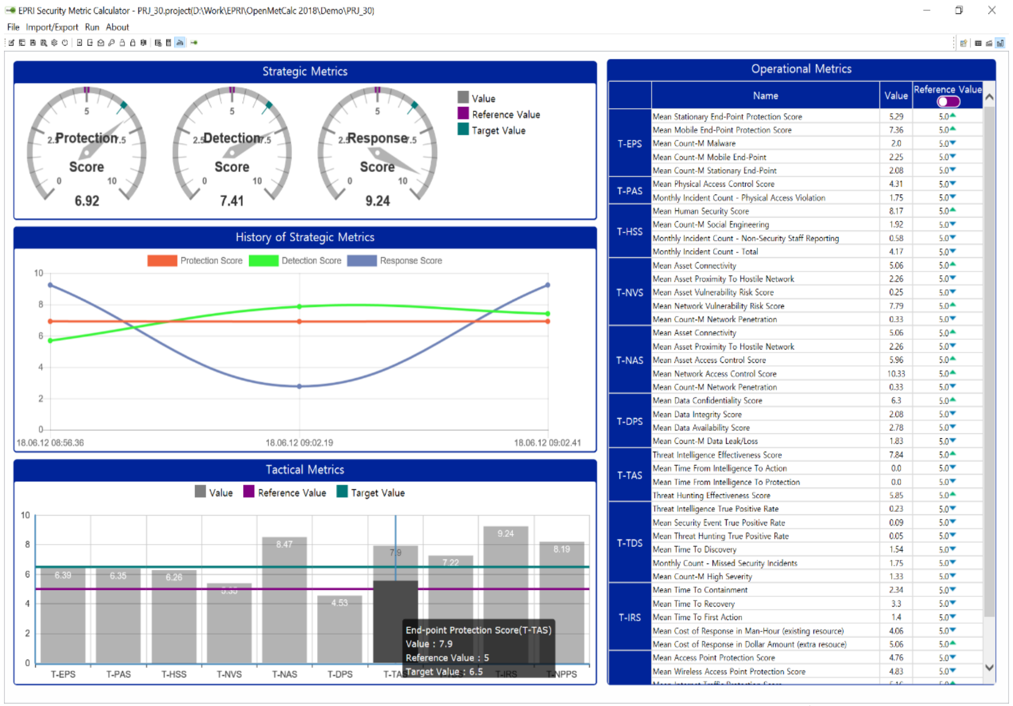
OpenMetCalc – EPRI Metric Calculator

2019

Metric Data Aggregation

EPRI OpenMetCalc

- Open-source Metric Calculator Tool
- Stand-alone Windows Application
- Functionalities
  - Load data
  - Calculate EPRI security metrics
  - Load EPRI provided reference values
  - Set your own target values
  - Generate a dashboard
  - Compare your metric with target and reference values
  - Export metrics to an Excel file
  - Customizable metric scripts and parameters
- October 2018 – public release

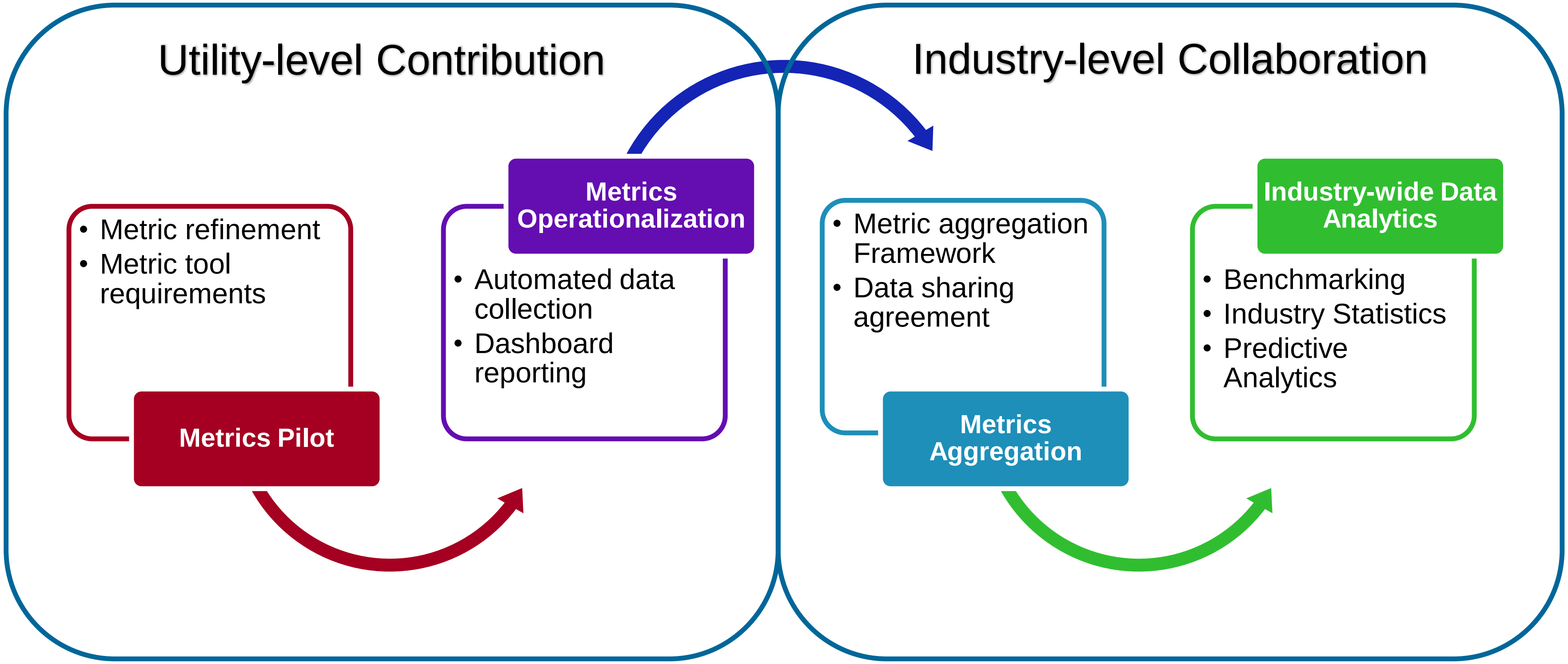


End-point Protection Score(T-TAS)
Value : 7.9
Reference Value : 5
Target Value : 6.5

Operational Metrics

	Name	Value	Reference Value
T-EPS	Mean Stationary End-Point Protection Score	5.29	5.0▲
	Mean Mobile End-Point Protection Score	7.36	5.0▲
	Mean Count-M Malware	2.0	5.0▼
	Mean Count-M Mobile End-Point	2.25	5.0▼
	Mean Count-M Stationary End-Point	2.08	5.0▼
T-PAS	Mean Physical Access Control Score	4.31	5.0▼
	Monthly Incident Count - Physical Access Violation	1.75	5.0▼
T-HSS	Mean Human Security Score	8.17	5.0▲
	Mean Count-M Social Engineering	1.92	5.0▼
	Monthly Incident Count - Non-Security Staff Reporting	0.58	5.0▼
	Monthly Incident Count - Total	4.17	5.0▼
T-NVS	Mean Asset Connectivity	5.06	5.0▲
	Mean Asset Proximity To Hostile Network	2.26	5.0▼
	Mean Asset Vulnerability Risk Score	0.25	5.0▼
	Mean Network Vulnerability Risk Score	7.79	5.0▲
	Mean Count-M Network Penetration	0.33	5.0▼
T-NAS	Mean Asset Connectivity	5.06	5.0▲
	Mean Asset Proximity To Hostile Network	2.26	5.0▼
	Mean Asset Access Control Score	5.96	5.0▲
	Mean Network Access Control Score	10.33	5.0▲
	Mean Count-M Network Penetration	0.33	5.0▼
T-DPS	Mean Data Confidentiality Score	6.3	5.0▲
	Mean Data Integrity Score	2.08	5.0▼
	Mean Data Availability Score	2.78	5.0▼
	Mean Count-M Data Leak/Loss	1.83	5.0▼
T-TAS	Threat Intelligence Effectiveness Score	7.84	5.0▲
	Mean Time From Intelligence To Action	0.0	5.0▼
	Mean Time From Intelligence To Protection	0.0	5.0▼
	Threat Hunting Effectiveness Score	5.85	5.0▲
T-TDS	Threat Intelligence True Positive Rate	0.23	5.0▼
	Mean Security Event True Positive Rate	0.09	5.0▼
	Mean Threat Hunting True Positive Rate	0.05	5.0▼
	Mean Time To Discovery	1.54	5.0▼
	Monthly Count - Missed Security Incidents	1.75	5.0▼
	Mean Count-M High Severity	1.33	5.0▼
T-IRS	Mean Time To Containment	2.34	5.0▼
	Mean Time To Recovery	3.3	5.0▼
	Mean Time To First Action	1.4	5.0▼
	Mean Cost of Response in Man-Hour (existing resource)	4.06	5.0▼
	Mean Cost of Response in Dollar Amount (extra resouce)	5.06	5.0▲
	Mean Access Point Protection Score	4.76	5.0▼
	Mean Wireless Access Point Protection Score	4.83	5.0▼

Our Vision



Utility-level Contribution

Metrics Pilot

- Metric refinement
- Metric tool requirements

Metrics Operationalization

- Automated data collection
- Dashboard reporting

Industry-level Collaboration

Metrics Aggregation

- Metric aggregation Framework
- Data sharing agreement

Industry-wide Data Analytics

- Benchmarking
- Industry Statistics
- Predictive Analytics

Resources (www.epri.com)

- 2018 Cyber Security Program Research Portfolio
- CEO Cybersecurity Checklist: A Companion Document to the Electricity Subsector Coordinating Council CEO Cybersecurity Checklist, 3002011549
- 2017 Annual Review and Looking Ahead to 2018 – Cyber Security (P183), 3002012578
- Information, Communication, and Cyber Security Roadmap, 2018, 3002011698
- Technical Update 2017 – Cyber Security Metrics for the Electric Sector, 3002010426
- Electricity Subsector-Cybersecurity Capability Maturity Model (ES-C2M2)
- Technical Results 2015 - Electric Sector Failure Scenarios and Impact Analyses – Version 3.0
- Substation Security Architecture Reference Diagrams Version 2.0, 3002012484
- Guidelines for Planning an Integrated Security Operations Center, 3002000374
- Guidelines for Integrating Control Center Systems Into an Integrated Security Operations Center, 3002003739

Together…Shaping the Future of Electricity

Questions & Answers

Upcoming Webinars

June 27 -	*Cyber Security*
July 25 -	Wholesale *Market Evolution*
September 26 -	Evolving Customer Needs

For more information, and to register, please visit www.midwesterngovernors.org/GridMod.htm.

MGA

America's Smartland

Midwestern Governors Association