
AMERICAN
PUBLIC
POWER™
ASSOCIATION
Powering Strong Communities

American Public Power Association's Cybersecurity Services Program

MPUA Annual Meeting 2018

Tan-Tar-A Resort

October 4, 2018

APPA Members

- 1400+ public power utilities
- Retail service in 49 states
- Very large to very small systems
- *Median* size: 1,977 meters
- 14.4% of sales to electric consumers

Cyber & Physical Preparedness

- Help members develop “all-hazards” approach to disaster preparation and response
- Show federal policymakers public power’s commitment to security and mutual aid
- Strengthen government/industry partnerships
- Minimize new federal regulation

DHS open source alerts: HIDDEN COBRA - North Korean Malicious Cyber Activity

- **August 9, 2018: North Korean Trojan: KEYMARBLE**
- **June 14, 2018: North Korean Trojan: TYPEFRAME**
- **May 29, 2018: HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm**
- **May 29, 2018: HIDDEN COBRA RAT/Worm**
- **March 28, 2018: North Korean Trojan: SHARPKNOT**
- **February 13, 2018: North Korean Trojan: HARDRAIN**
- **February 13, 2018: North Korean Trojan: BADCALL**
- **December 21, 2017: North Korean Trojan: BANKSHOT**
- **November 14, 2017: North Korean Remote Admin Tool: FALLCHILL**
- **November 14, 2017: North Korean Trojan: Volgmer**
- **August 23, 2017: Analysis of Delta Charlie Attack Malware**
- **June 13, 2017: HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure**
- **May 12, 2017: WannaCry Ransomware (300,000 computers affected)**

DOE Cooperative Agreement Overview

- In 2016 APPA partnered with the Department of Energy
- 3-year, $7.5M Cooperative Agreement;

- 2016-17 – Analysis and Data Collection
- 2017-18 – Deployment and Resource Development
- 2018-19 – Sustainability

Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

DOE Cooperative Agreement Overview

Goal:
Develop a culture of cyber security within public power utilities.

Objective:
Engage with public power distribution utilities to understand their cyber security awareness, capabilities and risks.

Year 1 Tasks:
1. Cyber security risk assessments
2. Onsite cyber vulnerability assessments
3. Pilot existing and emerging security technologies
4. Improve how we communicate cyber threats

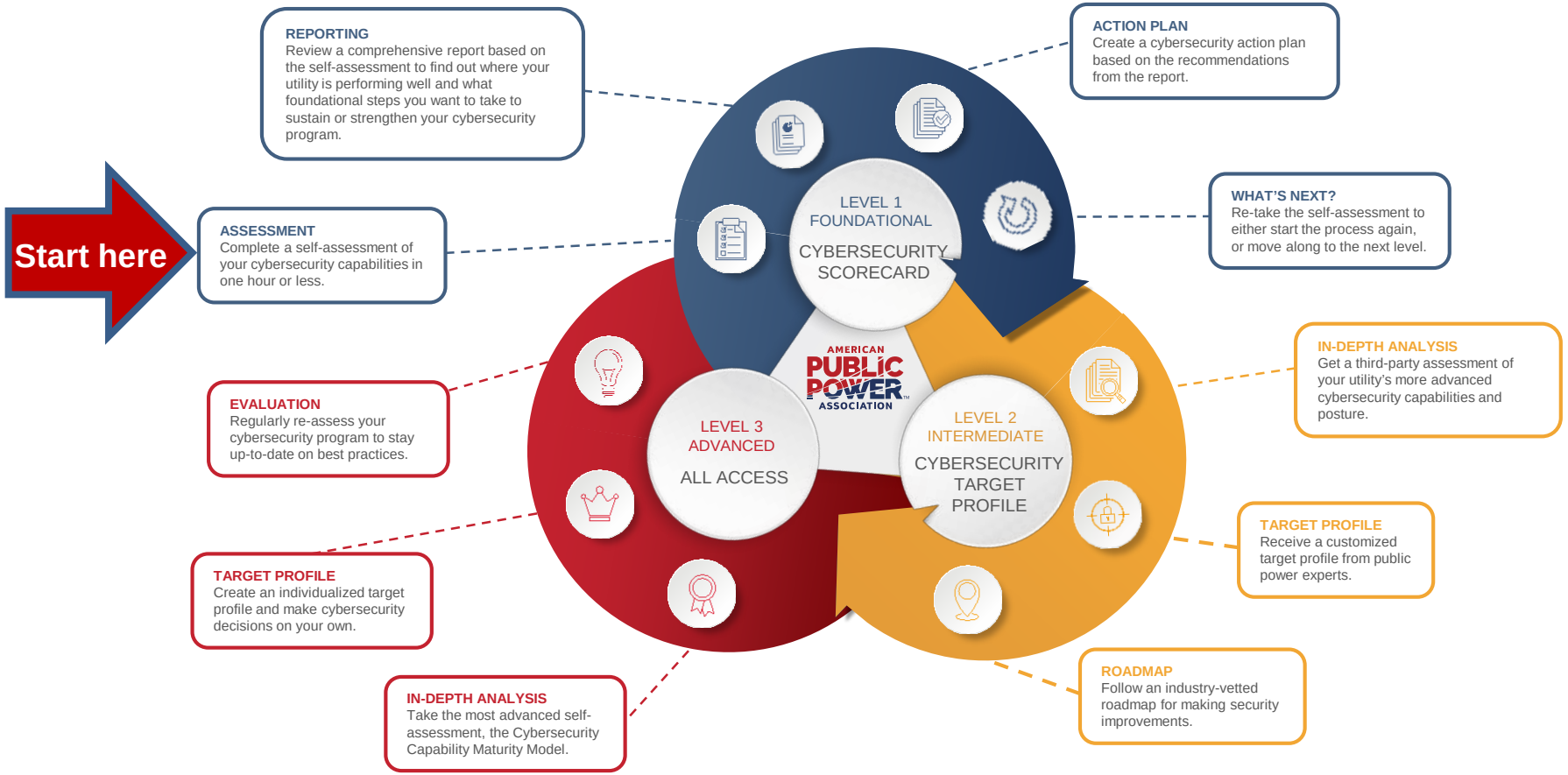
Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

Cybersecurity Risk Assessments
Cybersecurity Scorecard

- Use existing cybersecurity models to inform a product that is useable by all public power utilities
- Developed a self-assessment tool called the public power **Cybersecurity Scorecard,**
- Usable by small to mid-sized public power utilities to start evaluating their cybersecurity program.
- Also scalable so all public power utilities will find it useful.

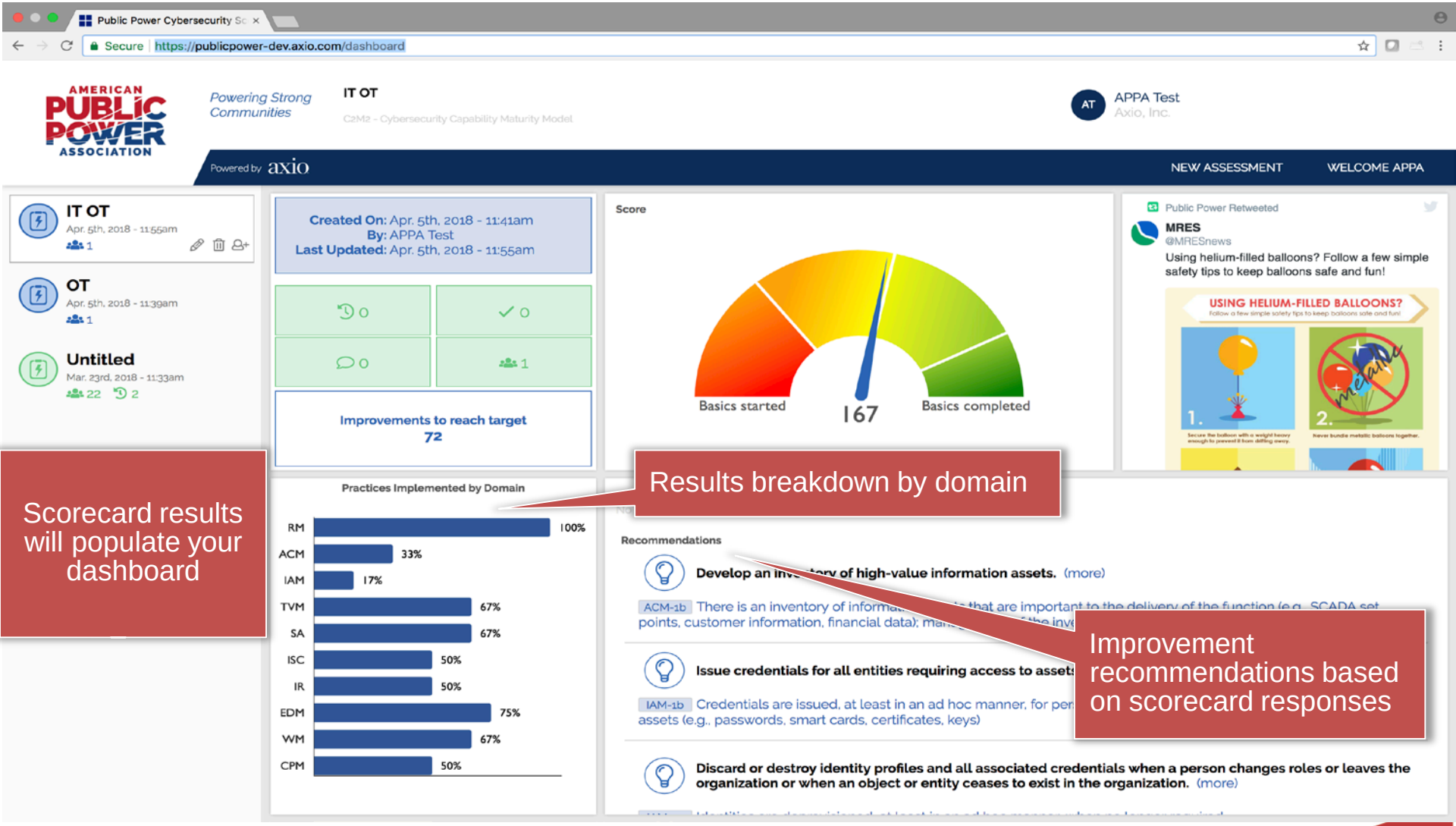
Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

The Public Power Cybersecurity Scorecard



Foundational Cybersecurity Practices

1. Cyber Asset Inventory
2. Configuration Baseline
3. Access Control
4. Vulnerability Management
5. Threat Management
6. Cyber Risk Management
7. Cyber Event Detection
8. Cyber Incident Response
9. Operational Resiliency
10. Monitoring Cyber System Activity
11. Cyber Threat and Event Information Sharing
12. Supply Chain Risk
13. Workforce Management and Cybersecurity Training
14. Cybersecurity Program Management



Scorecard results will populate your dashboard

Results breakdown by domain

Improvement recommendations based on scorecard responses

Public Power Scorecard Activity

- 116 public power utilities participating
  - (2019 Goal is to reach 700 utilities)
- 158 foundational cybersecurity self assessments
  - (14 Questions – 45 minutes)
- 39 completed a full self assessment
  - (312 Questions – 2-3 days)

- All public power utilities have **FREE** access to the Scorecard portal

- Utilities who have taken the assessment have reported that the Scorecard is helping to **“take the guesswork out of what they should be striving to achieve”**

Cybersecurity Resources

- Developing a **Cybersecurity Roadmap**
  - Using the Scorecard output, provide public power utilities with clear actions to improve their cybersecurity program
  - provide information that creates a compelling business case for security investments.
- Developing a **Cyber Asset Tracking** system to provide public power utilities with an online tool for:
    - Cyber Asset Inventory
    - Configuration Baseline
    - Vulnerability and Threat Management
    - Cyber Event Logging
    - Supply Chain tracking

Cybersecurity Resources

- Developing a program for **Shared Cybersecurity Services**
  - Joint Action Agency model as a framework
  - More mature organizations mentoring others
  - Joint training sessions
  - Investigating a shared cyber analyst

- Developing a **Cyber Incident Response Playbook**
  - Modeled after mutual aid response network
  - Cyber Mutual Assistance (CMA) being developed nationally
  - Utilities sharing cyber resources and expertise in a crisis
  - Exercising the playbook to be prepared

Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

Cybersecurity Resources

You can find published material on our website at:
www.publicpower.org/gridsecurity

- Cybersecurity Information Engagement Plan,
- Cybersecurity Information Sharing Report,
- Cybersecurity Essentials: A Public Power Primer,
- Managed Cybersecurity Service Providers Guide,
- Physical Security Essentials.
- Cybersecurity Awareness Videos

Cybersecurity Training

- Signing up JAAs to be host sites for training
  - Cybersecurity@publicpower.org
- Deliver low cost **cybersecurity training and exercises** that align with the Scorecard
- Conduct Regional facilitated workshops **(JAA/State Association sites)**
- Hosting a year end public power **cybersecurity summit (November 13-14, 2018 Austin, TX)**

Cybersecurity Technology Assistance Program

- After completing the Scorecard, utilities may be ready to reduce risk by investing in cybersecurity technologies from managed security service providers or other vendors.
- The Association's new Cybersecurity Technology Assistance Program (CTAP) can support that investment first by connecting public power utilities to cybersecurity technology solution providers.
- Next, the Association can contribute partial funding through our cooperative agreement with the Department of Energy to qualified utilities.
- Interested utilities should contact us at: cybersecurity@publicpower.org

Future Sustainability Model

- APPA will continue to provide the platform to conduct cybersecurity self assessments
- APPA will encourage members to mature their cybersecurity program over time to fill the gaps identified in the self assessments
- Partner with Joint Action Agencies, Regional Agencies and State Associations across the country to provide services and resources to help utilities sustain their cybersecurity program

Resources page:
www.publicpower.org/gridsecurity

Nathan Mitchell
Sr. Director of Cyber and Physical Security Services
American Public Power Association
2451 Crystal Dr., Suite 1000,
Arlington, VA 22202

Direct: 202.467.2925
nmitchell@publicpower.org

cybersecurity@publicpower.org