AMERICAN
PUBLIC
POWER™
ASSOCIATION

Powering Strong Communities

American Public Power Association's Cybersecurity Services Program

Midwest Regional Cybersecurity Summit

Kearney, NE

July 24, 2019

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

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. Move each utility from its existing state to a public power target profile.

Tasks:

1. Cybersecurity risk assessments (Cybersecurity Scorecard)
2. Onsite cyber vulnerability assessments
3. Pilot existing and emerging security technologies
4. Information sharing between utilities and APPA, E-ISAC, MS-ISAC, other partners

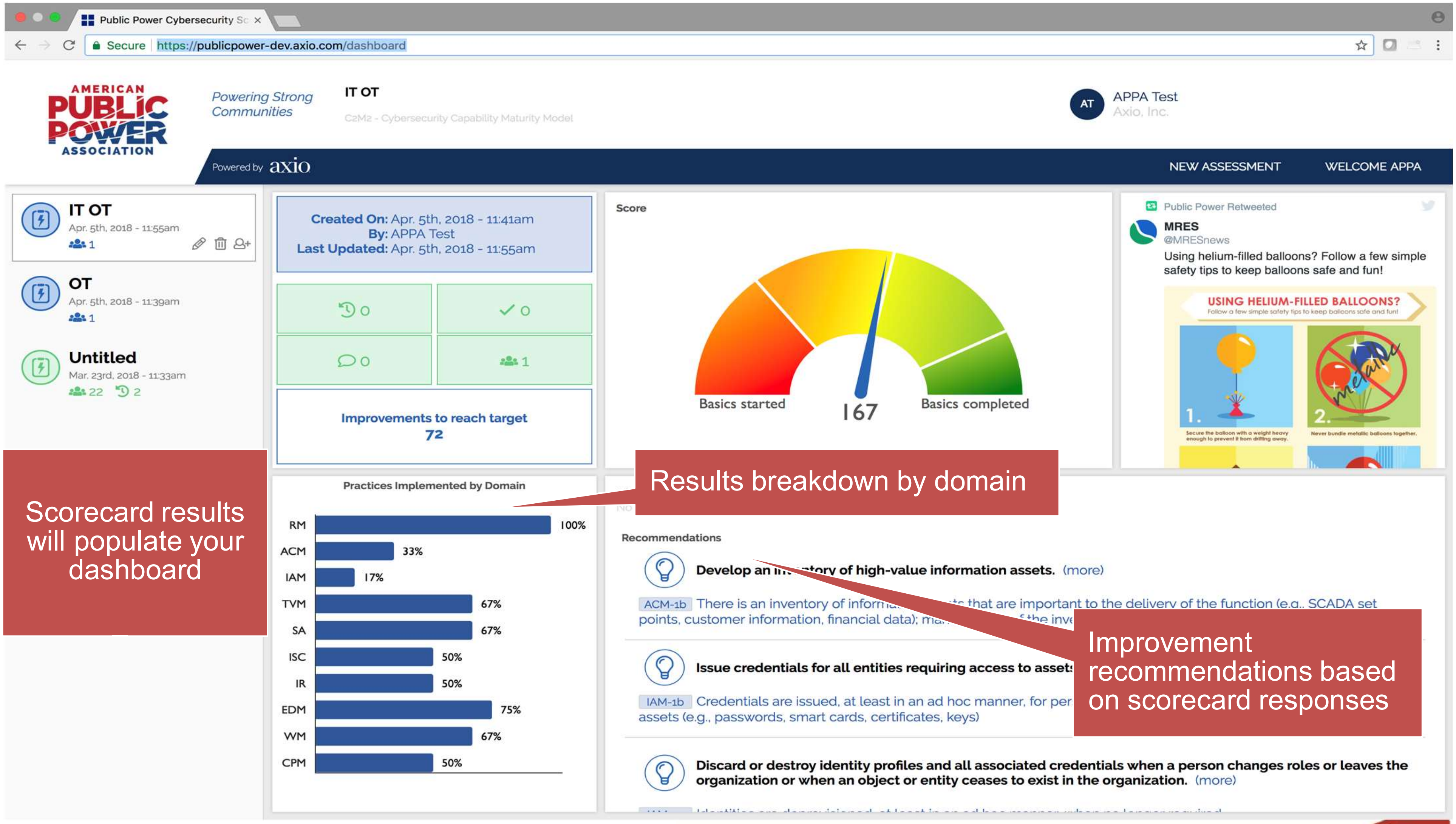
Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

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.*


Public Power Cybersecurity Sc ×
Secure https://publicpower-dev.axio.com/dashboard
AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities
Powered by axio
NEW ASSESSMENT
WELCOME APPA
AT
Score
Basics started
167
Basics completed
Practices Implemented by Domain
RM 100%
ACM 33%
IAM 17%
TVM 67%
SA 67%
ISC 50%
IR 50%
EDM 75%
WM 67%
CPM 50%
USING HELIUM-FILLED BALLOONS?
Follow a few simple safety tips to keep balloons safe and fun!
1.
Secure the balloon with a weight heavy enough to prevent it from drifting away.
2.
Never bundle metallic balloons together.

IT OT

C2M2 - Cybersecurity Capability Maturity Model

APPA Test
Axio, Inc.

IT OT
Apr. 5th, 2018 - 11:55am
1

OT
Apr. 5th, 2018 - 11:39am
1

Untitled
Mar. 23rd, 2018 - 11:33am
22 2

Created On: Apr. 5th, 2018 - 11:41am
By: APPA Test
Last Updated: Apr. 5th, 2018 - 11:55am

0	✓ 0
0	1

Improvements to reach target
72

Public Power Retweeted
MRES
@MRESnews
Using helium-filled balloons? Follow a few simple safety tips to keep balloons safe and fun!

Recommendations

Develop an in tory of high-value information assets. (more)

ACM-1b There is an inventory of inform ts that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); ma f the inve

Issue credentials for all entities requiring access to assets

IAM-1b Credentials are issued, at least in an ad hoc manner, for per assets (e.g., passwords, smart cards, certificates, keys)

Discard or destroy identity profiles and all associated credentials when a person changes roles or leaves the organization or when an object or entity ceases to exist in the organization. (more)

IAM Identities are deprovisioned, at least in an ad hoc manner, when no longer required.

Scorecard results will populate your dashboard

Results breakdown by domain

Improvement recommendations based on scorecard responses

Scorecard Activity

- 261 public power utilities participating
  - (2019 Goal is to reach 400 utilities)
- 502 foundational cybersecurity self assessments at the 244 utilities
  - (14 Questions – 45 minutes)

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

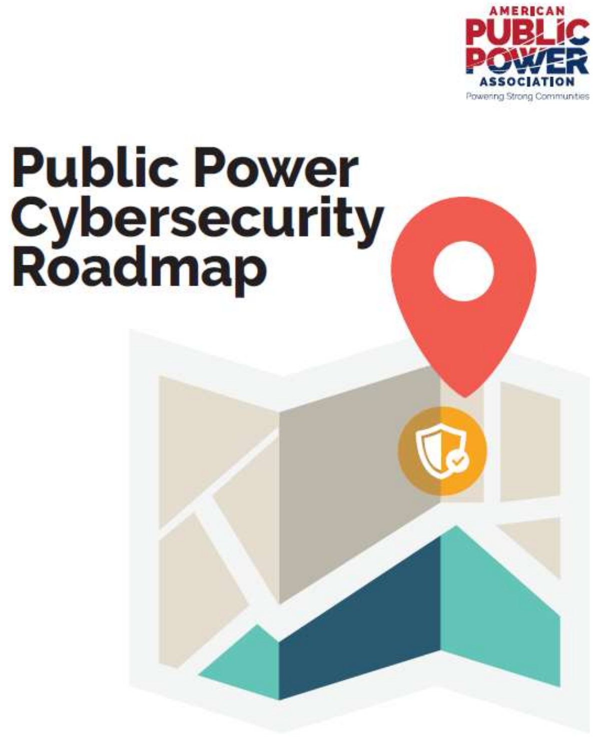
- Utilities who have taken the assessment have reported that the Scorecard is helping to **“take the guesswork out of what they should be striving to achieve”**

Cybersecurity Roadmap

Cybersecurity Roadmap

- Using the Scorecard output, provide public power utilities with clear actions to improve their cybersecurity program

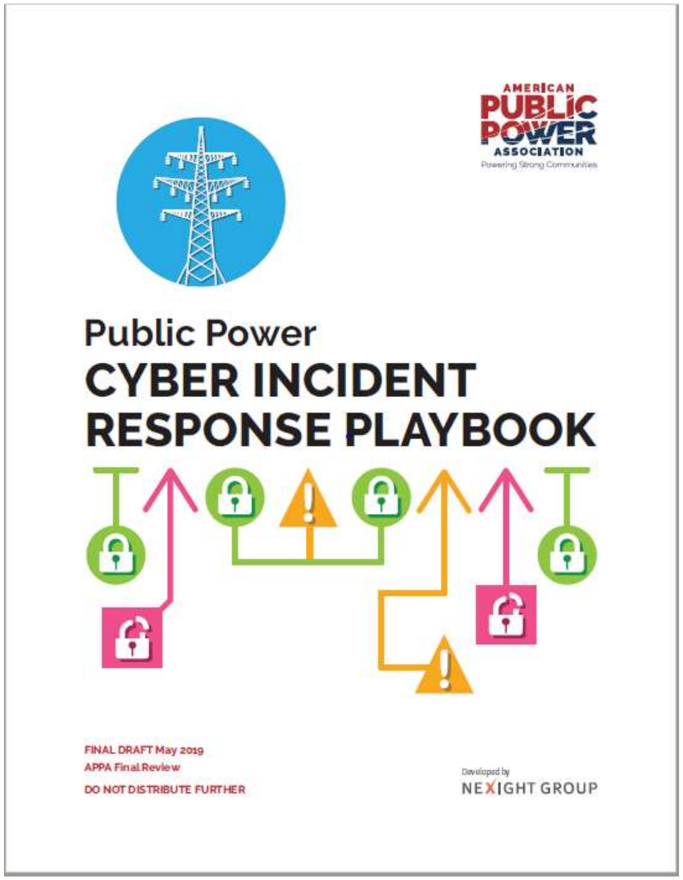
- Provide information that creates a compelling business case for security investments.


AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities
Public Power Cybersecurity Roadmap

Incident Response Playbook

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



AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

Public Power
CYBER INCIDENT
RESPONSE PLAYBOOK

FINAL DRAFT May 2019
APPA Final Review
DO NOT DISTRIBUTE FURTHER

Developed by
NEXIGHT GROUP

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

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
  - Orlando July 10-11
  - Kearney Nebraska July 24-25
  - Los Angeles California August 22
- Hosting a year end public power **cybersecurity summit (November 18-20, 2019 Nashville TN)**

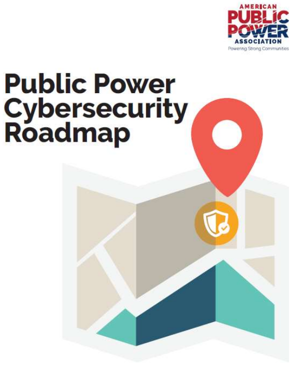
Secure Information Sharing

- Sign up for the E-ISAC at www.eisac.com
- Sign up for the MS-ISAC at www.cisecurity.org
- We continue to recommend the E-ISAC as the trusted source of public power utility's ICS threat information.
- Developing a program for **Shared Cybersecurity Services**
  - Joint Action Agency model as a framework to possibly provide a shared cyber analyst
  - Mature organizations mentoring others
  - Concise threat feed in our Secure Trusted Community (STC) network

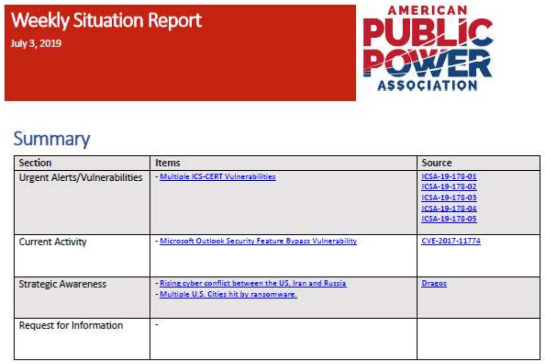
Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

Additional Cybersecurity Resources

- **Cybersecurity Scorecard**
  - 261 public power utilities
- **Cybersecurity Roadmap**
  - Helps you develop an action plan
- **Incident Response Playbook**
  - Cyber Mutual Aid
  - Shared cyber resources
- **Cybersecurity Training**
  - We bring training to you
- **Secure Information Sharing**
  - Weekly Situation Report (new)



Public Power Cybersecurity Roadmap

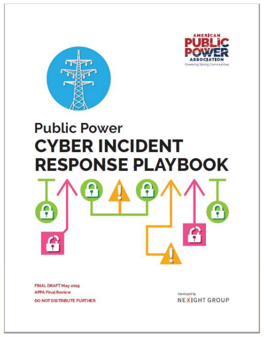


Weekly Situation Report

July 3, 2019

Summary

Section	Items	Source
Urgent Alerts/Vulnerabilities	- Multiple ICS-CERT Vulnerabilities	ICSA-19-178-01 ICSA-19-178-02 ICSA-19-178-03 ICSA-19-178-04 ICSA-19-178-05
Current Activity	- Microsoft Outlook Security Feature Bypass Vulnerability	CVE-2017-11774
Strategic Awareness	- Rising cyber conflict between the US, Iran and Russia - Multiple U.S. Cities hit by ransomware.	Dragos
Request for Information	-	

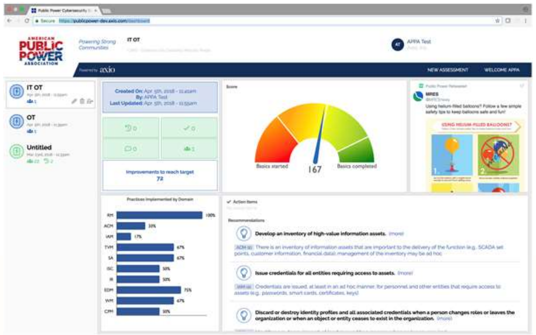


Public Power
CYBER INCIDENT
RESPONSE PLAYBOOK

Powering Strong Communities

FINAL DRAFT May 2019
APPA Final Review
DO NOT DISTRIBUTE FURTHER

Developed by NEXIGHT GROUP



Created On: Apr 5th, 2018 - 11:41am
By: APPA Test
Last Updated: Apr 5th, 2018 - 11:55am

Improvements to reach target
72

MRES
Using helium-filled balloons? Follow a few simple safety tips to keep balloons safe and fun!

Develop an inventory of high-value information assets. (more)

ACM-1a There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc

Issue credentials for all entities requiring access to assets. (more)

IAM-1a Credentials are issued, at least in an ad hoc manner, for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)

Discard or destroy identity profiles and all associated credentials when a person changes roles or leaves the organization or when an object or entity ceases to exist in the organization. (more)

Resources page: www.publicpower.org/gridsecurity

Sam Rozenberg
Engineering Services Security Director
American Public Power Association
2451 Crystal Dr., Suite 1000,
Arlington, VA 22202

Direct: 202.467.2985
Srozenberg@PublicPower.org

cybersecurity@publicpower.org