SYSTEM IMPROVEMENT
Applying Public Power's Best Practices to Each Utility

Cybersecurity Check Up
Assessment of Cybersecurity Posture of Public Power Utilities

AESI-US, Inc.'s Cybersecurity Check Up focuses on three components that are fundamental for a strong cyber posture. AESI conducts a survey-based assessment; reviews a representative set of existing cybersecurity-related policies, standards, and procedures based on the survey results; and tests high-risk web applications to determine a utility's cyber posture. The outcome is a quick health check and a path to become more cyber resilient.

In partnership with Hometown Connections, AESI delivers cyber and physical security consulting for public power utilities (electric, water, gas), leaning on best practices and meeting appropriate industry standards.

AESI bases its Cybersecurity Check Up service on guidance from the American Public Power Association (APPA), the U.S. Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), the NIST Cybersecurity Framework, and accepted privacy principles (GAPP).

Assessment Approach—The Check-Up
The Cybersecurity Check Up service consists of three components:

Cybersecurity Program Survey
- A customized survey-style assessment to be completed with the utility.
- Baseline for questions includes APPA's guidance and authoritative standards such as NIST and US Department of Energy.

Policies, Standards & Procedures Review
- Review of a representative set of existing cybersecurity-related polices, standards, and procedures based on the survey results.

Remote Testing
- Remote testing of high risk web applications.

Together, these three components represent a high level assessment to ascertain efficiently the cybersecurity posture ideal for utilities requiring a starting point for a cyber program or a quick health check of an existing cyber program.

AESI

Hometown Connections

Hometown Connections staff and industry colleagues offer these integrated consulting services:

FACILITATION SERVICES
Strategic Planning
Technology Planning
Governance Training/
Board Retreats

RESEARCH SERVICES
Customer Satisfaction,
Service Preferences, & Public
Power Awareness
Employee Satisfaction
Compensation Studies

FINANCIAL SERVICES
Cost of Service Studies/Rate
Design
Energy Trading/Risk
Management

TECHNOLOGY SERVICES
Cyber & Physical Security
Consulting
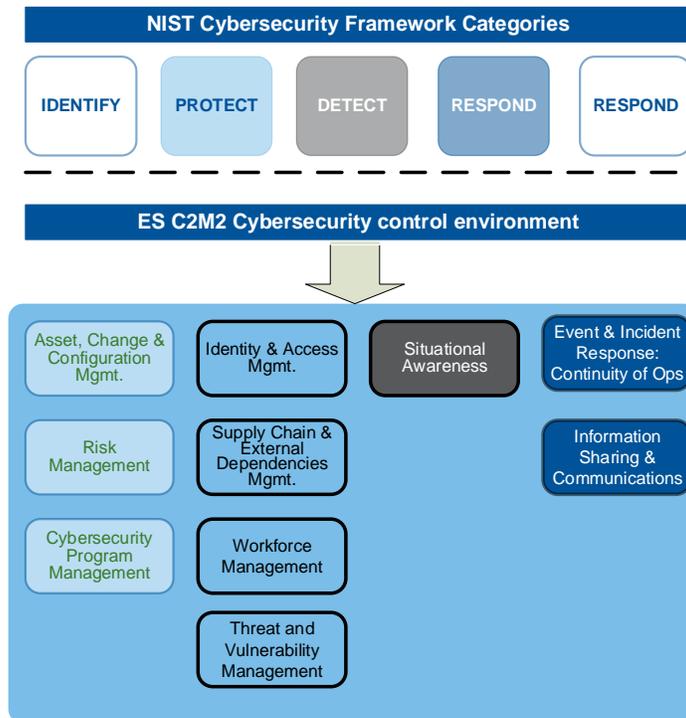Utility Technology
Consulting

SKILL SET SERVICES
Temporary Skill Sets:
Personnel and Projects

CHECK-UPS
Organization
Governance
Finance
Customer Service
Cybersecurity
Distribution System
Reliable Public Power
Program (RP3)

Cybersecurity Check Up Assessment Framework

Utilities are assessed on the ten (10) domains described in the Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model:

NIST Cybersecurity Framework Categories

| IDENTIFY | PROTECT | DETECT | RESPOND | RESPOND |

ES C2M2 Cybersecurity control environment

- Asset, Change & Configuration Mgmt.
- Identity & Access Mgmt.
- Situational Awareness
- Event & Incident Response: Continuity of Ops
- Risk Management
- Supply Chain & External Dependencies Mgmt.
- Information Sharing & Communications
- Cybersecurity Program Management
- Workforce Management
- Threat and Vulnerability Management

The AESI Cybersecurity Check Up deliverables include a dashboard view of the utility's cybersecurity posture, scan results, and high-level recommendations.

Benefits

- Based on established security frameworks and authoritative sources
- Cost effective
- Demonstration of due diligence to identify initial security posture
- Utility staff time commitment is approximately one day
- Identifies the cybersecurity maturity level of the utility
- Based on the results of the cybersecurity check-up, provides recommendations for improving the security posture and maturity level for the utility

Additional A La Carte Services

Based on the results of the Cybersecurity Check Up, the utility can tap into any of the following additional services to build/augment their cybersecurity program:

- Training for the board/executive team and IT/OT technical staff
- Develop or validate Core Policies, Procedures, and Governance:
    - Templates for a "fill in the blanks" approach to setting policies, procedures
    - Roles and Responsibilities matrix (RACI)
- Cyber Vulnerability Assessments (CVA)
- Risk Assessments
- Penetration Tests
- Cybersecurity Program Development
- Offerings of Other Hometown Connections Partners
    - **N-Dimension Solutions Free 60-Day Trial** of N-Sentinel Monitoring for 24/7 remote monitoring and detection of network issues.
    - **Wortham Power Gen Insurance** for protection from liability and recovery costs from a data breach in which customer or employee personal information is exposed or stolen. **Group purchasing premiums average 20 to 40% lower in the first year.**