RIVERSIDE PUBLIC UTILITIES' SECURITY PROGRAM

Board of Public Utilities
September 9, 2019

SECURITY REGULATION

California Public Utilities Commission

On September 25, 2014, California's governor signed into law California Senate Bill 699 which requires the Commission to develop rules for physical security of the electric distribution system.

Executive Order 13800

The EO was issued on May 11, 2017 to improve the Nation's cyber posture and capabilities in the face of intensifying cybersecurity threats to its digital and physical security.

North American Electric Reliability Corporation

The NERC Critical Infrastructure Protection Reliability Standards (CIPs) are recognized as best practices that all public power utilities should consider. NERC CIPs are a group of reliability standards included in the complete set of NERC Reliability Standards which define the reliability requirements for planning and operating the North American bulk power system and are developed using a results-based approach that focuses on performance, risk management, and entity capabilities.

American Water Works Association

AWWA guidance is based on the recommendation in ANSI/AWWA G430: Security Practices for Operations and Management and EO 13636.

MANAGEMENT RECOMMENDATIONS FROM VULNERABILITY ASSESSMENT

1. Establish security management/oversight
2. Establish security program, policies and standard operating procedures
3. Establish working group and governance oversight committee

RPU'S SECURITY PROGRAM GOVERNANCE STRUCTURE

Security Governance Committee
General Manager, Asst General Managers, City Innovation Officer

↑

Steering Committee
Cyber/Physical Security and Emergency Response Teams

↑

Divisional Working Groups

SECURITY PROGRAM ADMINISTRATION

There was no single point of management for RPU cyber security, physical security, emergency management and safety training/awareness

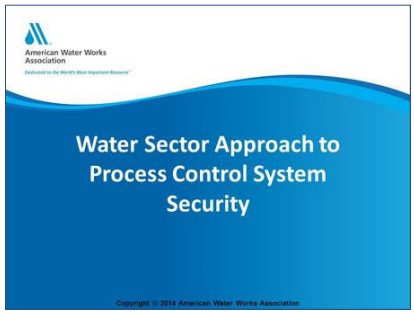
Added Security oversight and governance responsibilities under the NERC Regulatory Compliance/Energy Risk Manager:

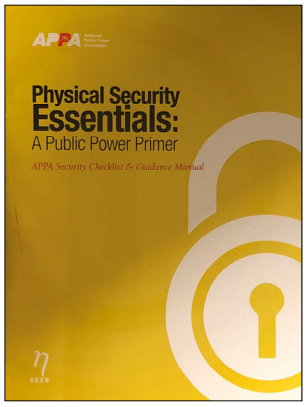
1. Existing position that reports to the RPU General Manager
2. Overlap exists in the responsibilities of NERC Reliability Standards Compliance

NERC = North American Electric Reliability Corporation

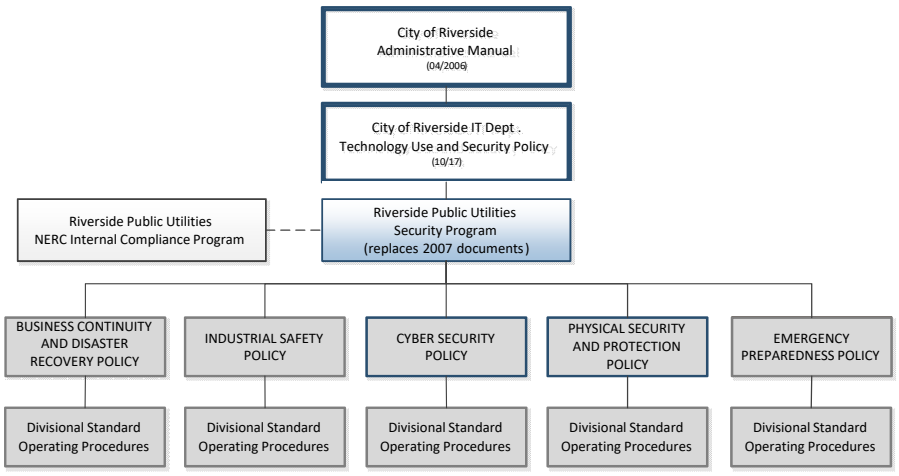
KEY REFERENCES

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION





SECURITY PROGRAM STRUCTURE



SECURITY PROGRAM ACCOMPLISHMENTS TO DATE

1. Security Program
   - A. Cyber Security Policy
     - i. Cyber Security Incident Response Plan
     - ii. Electric and Water cyber security procedures
   - B. Physical Security Policy
     - i. Customer Service Safe-Vault Security
     - ii. Administration Key Control
     - iii. Electric and Water facilities perimeter, access, lighting procedures
   - C. Emergency Preparedness (complies with City EOP)
     - i. RPU Emergency Operations Plan, April 22, 2019
     - ii. Emergency Action Plan for Mockingbird Dam
   - D. Safety and Business Continuity
     - i. HC-EMI Emergency Management and Business Continuity
     - ii. Electric and Water safety procedures
2. Security Program Share point Portal

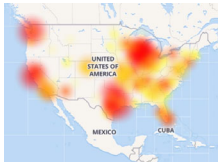
ELECTRIC SCADA CYBER SECURITY CHANGES

1. Maintain department awareness of Industry Best Practices
2. Moved from Reactive to Proactive stance by taking a Defense in Depth approach:
   A. Isolated the SCADA network – Data flow only flow out of the SCADA network – and flows both ways from DMZ to City Network to allow access to give SCADA data by the Corporate users

   B. Implemented Antivirus and Anti Malware
   C. Maintain (Update) system patching for security
   D. Log and Store events of the Electric SCADA systems
   E. Using Multi-Factor authentication (something you have, you know, or you use)
   F. Rectified findings from last Vulnerability Assessment

GRIDEX V (2019)

1. Two-day nationwide electric grid security exercise
2. Simulates a coordinated cyber and physical attack
3. "Table top" exercise November 13-14.
4. Customized scenario for RPU
   A. Targeted cyber attacks on cooperate and SCDDA networks.
   B. Simultaneous physical attacks on generation, transmission and control centers.
   C. Disruption of voice and data communications



GRIDEX V (2019)

1. **Move 0 : October 21 to November 13**
   A. Sets the stage.
2. **Move 1 and 2 November 13**
   A. Simulated national news, Facebook and twitter
   B. Attacks are likely and then start
   C. Resources are exhausted. 311 Call center overloaded.
3. **Move 3 and 4 November 14**
   A. Some recovery overnight
   B. Attacks on water facilities start
   C. Software patches issued, infrastructure being repaired

Exercise Exercise Exercise Exercise Exercise Exercise Exercise

GRIDEX V (2019)

A. RPU Planners and participants – key RPU leaders
B. After action report
C. Comprehensive analysis of our performance
D. Action items matrix with priority and cost
E. Free and confidential participation

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

GridEx V GRID SECURITY EXERCISE 2019

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

RECOMMENDATION

That the Board of Public Utilities receive and file an update on Riverside Public Utilities' Security Program which includes policies for cyber security and physical security specific to Public Utilities assets and facilities.