

Cybersecurity Overview

House Energy and
Technology Committee

March 30, 2022



Organization Intelligence and Alerting

- Staying connected with trusted authorities
 - DHS –Department of Homeland Security
 - EISAC –Electric Information Sharing & Analysis Center
 - FBI –Federal Bureau of Investigations
 - CISA –Cybersecurity & Infrastructure Security Agency
 - SANS –Sysadmin, Audit, Network, and Security
 - NERC –North American Electric Reliability Corporation
 - NIST –National Institute of Standards and Technologies
 - 20 automated intelligence sources
 - Used for automated real-time assessments of indicators

Compliance Security Requirements

- NERC CIP Bulk Electric System Cyber Security Policies:
 - CIP-004 – Personnel & Training
 - CIP-005 – Electronic Security Perimeter
 - CIP-006 – Physical Security of BES Cyber Systems
 - CIP-007 – System Security Management
 - CIP-008 – Incident Reporting and Response Planning
 - CIP-009 – Recovery Plans for BES Cyber Systems
 - CIP-010 – Configuration Change Management and Vulnerability
 - CIP-011 – Information Protection
 - CIP-013 – Supply Chain Risk Management