SPP RE Trustees
Critical Infrastructure Protection Committee Update

Robert McClanahan
Arkansas Electric Cooperative Corporation

October 25, 2010

Overview

- ESCC Roadmap
- Changes in NERC CIP Program
- CIPC Guideline Work
- Recent CIP-Related NERC Advisories
- CIP Standards

ESCC Roadmap

- ESCC's plan to address HILF risks
  - Includes CIP Coordinated Action Plan
- CIPC has the lead role in two elements of the Coordinated Cyber Attack scenario
  - Assessment of current capabilities
  - Isolate critical cyber systems
- CIPC will be assessing existing standards and updating/developing guidelines in support of these efforts

CIP Changes at NERC

- Mark Weatherford chosen as new NERC Chief Security Officer (CSO)
  - Comes from outside the electric industry
- Numerous changes in the works
  - Will be reviewing ES-ISAC operation
  - “Reliability through Security” a part of “Culture of Reliability Excellence”
  - Expressed desire to separate CIP compliance from rest of CIP Program to encourage open dialogue with industry

CIPC Guideline Work

- Business Continuity Guideline Task Force
- Protecting Sensitive Information Guideline Task Force
- Substation Guideline Task Force
- Control System Security Working Group (CSSWG)
  - Cyber Security Guidelines
  - Coordinated Action Plan work
- None are “guidelines in support of standards”

Recent CIP-Related Advisories

- NERC recently issued two CIP-related alerts through its FERC-approved process
  - Stuxnet malware advisory
  - Aurora vulnerability advisory
- While issued at the “Recommendation to Industry” level, both have mandatory responses in the form of surveys
  - Surveys seek to determine level of industry response and mitigation of vulnerability

Stuxnet

- Stuxnet worm was originally identified in 2009, but was determined earlier this year to specifically target Siemens control systems
  - Authors had a great deal of inside knowledge of Siemens systems and equipment
- There is concern that subsequent versions may target other systems
  - Excellent delivery system for other payloads

Stuxnet (cont.)

- NERC survey questions:
  - Have all control systems been scanned?
  - Were infections identified?
  - Have ALL unnecessary ports and devices been identified and disabled?
  - Have ALL unnecessary network shares been disconnected?
  - Does organization have a policy on use of removable media (e.g. USB sticks)?
- Responses were due to NERC by October 15th

Aurora

- Originally demonstrated in 2007 by DHS
- Industry received advisory in June 2007
  - However, few engineering details provided
- Has been subject of much discussion at FERC and in Congress
- Technical details were not made available to the industry until early 2010
  - Difficult to understand and address issues without information

Aurora(cont.)

- NERC survey questions:
  - Does your organization fully understand AURORA, especially given the new information?
  - Has your organization assembled an AURORA project team?
  - What is your plan to respond to customer inquiries regarding AURORA?
  - Have you taken steps to mitigate the risk of an AURORA event or attack, as both a consumer and provider of electric power?
  - Is your project plan for mitigation complete?
  - Are your mitigation efforts complete?
- Responses are due to NERC by 12/13

CIP Standards

- Version 4 revisions to CIP Standards are out for initial ballot until November 3rd
- Major change in identification of Critical Assets
  - Removes risk-based methodology
  - Adds “bright line” criteria for identification
- Removes exemption for nuclear plants
- SDT will be responding to a mountain of comments before next ballot

Questions?