AURORA Vulnerability Background

Southern California Edison (SCE)

September 2011

Outline

- What is AURORA?
- Your Responsibility as a Customer
- Sectors Impacted by AURORA
- Review of Regulatory Agencies
- History of AURORA
- Current State of AURORA II
- Mitigation Efforts Currently Underway

What is AURORA?

- Potential vulnerability in rotating equipment connected to the electric grid
- Equipment Potentially Impacted
  - High Value rotating equipment such as Motors and Generators
- Vulnerable Protection Devices
  - Digital Protection & Control Devices (DPCDs) such as relays & remote terminal units
- Vectors for Potential AURORA incident
  - Cyber devices with electronic access to control DPCDs
  - Communication paths to access DPCDs
  - Extensive on-board control capability with little authentication or authorization capability
- Alerts & Advisories
  - Alerts, advisories or other threat information for the AURORA vulnerability is issued by North American Electric Reliability Corporation (NERC) or Electricity Sector-Information Sharing and Analysis Center (ES-ISAC)
  - The alert or advisory notice directs Southern California Edison's (SCE) actions or responses to the vulnerability

Your Responsibility as a Customer

- ❑Review this presentation to get a better understanding of an AURORA event and its impacts
- ❑Evaluate your systems and facilities to determine if an AURORA vulnerability exists
- ❑Contact SCE at aurora@sce.com if you have any questions, concerns or if you feel you may be vulnerable.

Sectors Impacted by AURORA

Critical Infrastructure and Key Resources Sectors


Agriculture and Food


Banking and Finance


Chemical


Commercial Facilities


Communications


Critical Manufacturing


Dams


Defense Industrial Base


Emergency Services


Energy


Government Facilities


Healthcare and Public Health


Information Technology


National Monuments and Icons


Nuclear Reactors, Materials and Waste


Postal and Shipping


Transportation Systems


Water

Source Document: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Review of Regulatory Agencies

Here is a list of regulatory agencies that are involved with the AURORA vulnerability:

❑**Department of Homeland Security (DHS)** - produced a video depicting a generator exploding in a test lab during a simulated cyber attack.

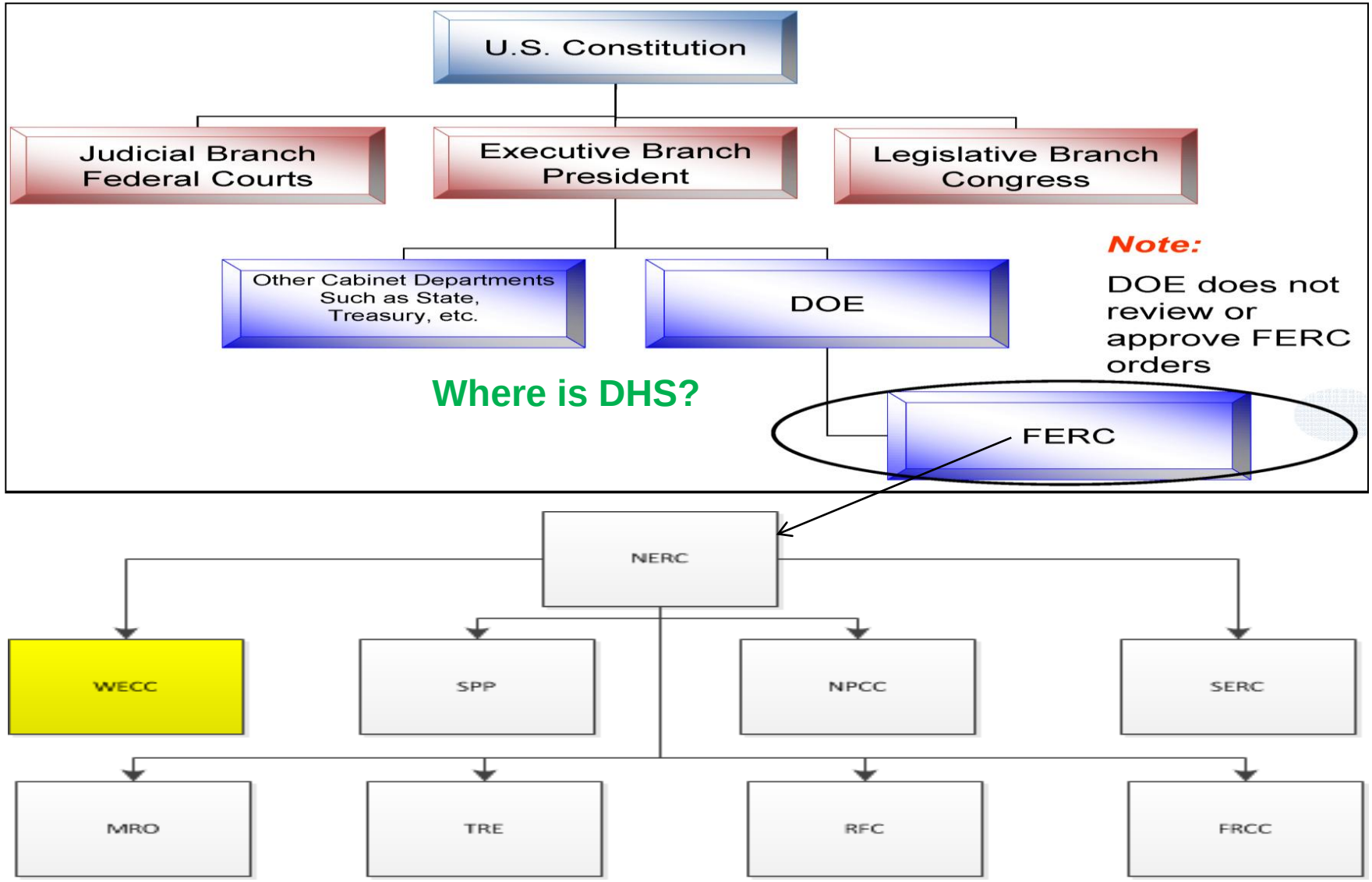
❑**Federal Energy Regulatory Commission (FERC)** - the United States federal agency with jurisdiction over interstate electricity sales, wholesale electric rates, hydroelectric licensing, natural gas pricing, and oil pipeline rates.

❑**North American Electric Reliability Corporation (NERC)** - falls under the FERC and the Department of Energy (DOE). NERC has been certified as the Electric Reliability Organization by FERC. NERC is the overall governing body who issues recommendations to industry on the AURORA vulnerabilities. Their recommendations provide sensitive and clarifying information regarding the nature of AURORA.

❑**Electric Sector Information Sharing and Analysis Center (ES-ISAC; Operated by NERC)** - ES-ISAC Advisory was meant to address what was considered a very important vulnerability, yet the Advisory did not require identification of all equipment that could be affected as critical. It also referenced NERC CIP-002 which many utilities have used to exclude power plants from being defined as critical cyber assets. The Advisory also was sent to other industries in early September 2007. Source : http://community.controlglobal.com/content/subject-aurora%E2%80%A6

❑**Western Electricity Coordinating Council (WECC)** - NERC delegates authority to enforce reliability standards to eight regional Entities including WECC. SCE is within the WECC region.

Review of Regulatory Agencies



History of AURORA

- First NERC Advisory pertaining to the Aurora vulnerability was issued June 2007 (AURORA I) – Focused on Cyber Access

- NERC Alert Recommendation issued October 2010 (AURORA II) – Focused on Physical and Cyber Access

  - NERC provided additional guidance to industry on the methodology used in the AURORA vulnerability analysis
  - Guidance on potential remediation if AURORA vulnerability is found to exist
  - Additional bibliographic material and security research documents

- Watch a demonstration of a simulated malicious exploit of the Aurora Vulnerability: http://www.youtube.com/watch?v=C2qd6xXbySk

Current State of AURORA II

- Congressional Activity
  - Multiple bills in congress for Cyber Security in the Energy Sector
  - Legislative actions to increase protected assets

- NERC Alert Recommendations
  - Mandatory response from SCE to NERC every 6 months until mitigation is complete
  - Additional documentation from NERC can be found at: http://www.nerc.com/fileUploads/File/PressReleases/PR_AURORA_14_Oct_10.pdf

Mitigation Efforts Currently Underway

- SCE is reviewing the overall recommendations and facility checklists from NERC and identifying any areas of concern.

- SCE is evaluating facilities that are owned by SCE for the presence of the AURORA vulnerability.

- SCE will take corrective action at facilities owned by SCE to remediate any discovered AURORA vulnerability.

- SCE recommends customers evaluate their systems and facilities for the AURORA vulnerability.

- Contact SCE at aurora@sce.com if you have any questions, concerns or if you feel you may be vulnerable.