ESRI First Annual Homeland Security Summit

Homeland Security Issues for the Electric Utility Industry: Actions, Priorities and Challenges

September 12, 2005
Denver, CO

Barry R. Lawson
National Rural Electric Cooperative Associaton (NRECA)

National Rural Electric Cooperative Association
A Touchstone Energy® Cooperative

Overview

- Background
- Industry and Government Actions
- Guidelines, Best Practices and Regulations
- Actions Utilities Should Take
- Final Thoughts

NRECA Information

- Trade association representing the 930 rural electric cooperatives in the U.S.
- They provide electricity to 37 million people in 47 states, and in 2,500 of the 3,100 counties
- Own and operate nearly half of the nation's electric distribution lines
- Employ approximately 63,000 people

Historical Reliability and Security

- Primary job – keep the lights on
- One of the most reliable industries in the world
- Electric system is designed to withstand certain incidents
- Public safety and system recovery is critical focus
- Security is an ongoing aspect of reliability

Familiar Incidents

- Natural disasters – e.g., weather related
- Vandalism
- Transmission tower bolts loosened and tower collapse
- Bomb threats at buildings/facilities
- Picture taking and videotaping of facilities
- Cyber/IT system intrusions
- Theft – vehicles, uniforms and $$
- Manmade disasters, e.g., natural gas leak, train accident, etc.

Post 9/11 Security

- New threat environment
- Need to evaluate if current emergency/security plans are adequate or if revisions are needed
- Expectations and existence of industry guidelines, standards and best practices
- Government and insurance requirements
- Legal liability issues

DOE & DHS Post 9/11 Actions

- Encouraged states and industry to undertake security and vulnerability reviews
- Pushed energy industry to develop security guidelines/standards in light of new threat environment
- If no action by industry, would pursue federal legislative solution

Industry Actions

- Federal legislative solution not desired
- Through the North American Electric Reliability Council (NERC) Critical Infrastructure Protection Committee (CIPC)
  - Cyber and physical security guidelines for protecting critical assets were developed and approved by industry in June 2002
- DOE and DHS expressed satisfaction with new guidelines
- NERC cyber security standard approved August 2003

NERC Security Guidelines

- These are the industry best practices for **physical** and **cyber** security
- These voluntary guidelines serve as a tool/framework for developing/revising security/emergency plans
- Applicability will depend on facilities, customers and location for each utility
- Weblink to Security Guidelines
  - http://www.esisac.com/library-guidelines.htm

NERC Security Guidelines

- Designed to protect the bulk power system
- Focused on protection and restoration of most critical assets
- Guidelines are useful and beneficial to all electric utilities regardless of size

NERC Physical Security Guidelines

- Vulnerability and Risk Assessment
- Emergency Plans
- Continuity of Business Practices
- Communication
- Threat Alert System and Physical Response for Electricity Sector

NERC Physical Security Guidelines

- Physical Security
- Employment Background Screening
- Protecting Potentially Sensitive Information
- Threat and Incident Reporting
- Substations
- Others and revisions as needed

NERC Cyber Security Guidelines

- Risk Management
- Access Controls
- IT Firewalls
- Intrusion Detection
- Securing Remote Access to Electronic Control and Protection Systems

NERC Cyber Security Guidelines

- Threat Alert System for Cyber Response for Electricity Sector
- Patch Management for Control Systems
- Control System – Business Network Electronic Connectivity

NERC Cyber Security Standard

- Sets out cyber security practices that are <u>mandatory</u> for Control Area Operators and NERC Reliability Coordinators
- These are also industry best practices
- Regardless of applicability, all should review for background and possible usefulness
- Permanent standard approval possible in early/mid 2006
  - Will impact more utilities and IT systems

NERC Cyber Security Standard Elements

- Critical Cyber Assets
- Electronic Security Perimeter
- Physical Security Perimeter
- Electronic Access Controls
- Physical Access Controls
- Personnel
- Monitoring Physical Access
- Monitoring Electronic Access
- Information Protection
- Training
- Systems Management

NERC Cyber Security Standard Elements

- Test Procedures
- Electronic Incident Response Actions
- Physical Incident Response Actions
- Recovery Plans

NERC workshops

- Early 2003 held numerous workshops in U.S. and Canada to educate the industry on the new security guidelines
- Strong attendance at workshops
- Industry representatives and physical and cyber security experts provided workshop content

Homeland Security Presidential Directive (HSPD) 7

- Issued by President on Dec. 17, 2003
- Entitled “Critical Infrastructure Identification, Prioritization and Protection”
- Policy for federal departments on protecting the nation’s critical infrastructure
  - 85% of critical infrastructure privately owned
- Industry and government are working on these issues

Rural Utilities Service (RUS) Emergency Restoration Plan (ERP) Final Rule

- Issued October 12, 2004
- Applies only to RUS borrowers
- To receive RUS funds, you must comply
- Weblink to final rule:
  - http://www.usda.gov/rus/electric/fr2004/fr12oc04-2.htm

Primary Elements of RUS ERP Final Rule

- For **Cyber** and **Physical** security requires:
  - Completion of a vulnerability and risk assessment and related mitigation plan by July 2005
  - Modification of or creation of an ERP by January 2006
  - Development of a business continuity/disaster recovery plan by January 2006
  - Annual exercise of plan – first exercise by January 2007

NRECA/RUS Workshops

- 8 workshops focused on two primary areas:
  - Content of and compliance with the RUS ERP Final Rule
  - Electric utility industry best practices for cyber and physical security
    - North American Electric Reliability Council's (NERC's) Cyber and Physical Security Guidelines
- Workshops provided the tools and guidance needed to comply with RUS requirements and to adhere to applicable industry best practices

What Should Utilities Do?

- Some suggested steps:
  - Comply with security regulations and utilize applicable industry security best practices
  - Perform vulnerability and risk assessment
  - Undertake mitigation review
  - Increase senior management awareness
  - Review insurance coverage and contracts
  - Develop short and long-term security plans

What Should Utilities Do?

- Some suggested steps (cont.):
  - Periodically reevaluate plans and procedures on basis of new information, future guidelines and best practices
  - Attend security-related workshops and conferences; network with other security professionals
  - Work with other utilities
  - Establish and maintain effective relationships with law enforcement and state emergency operations center staff
  - Evaluate interdependencies

Important Tools and Information

- NERC's Threat Advisory Listserv (TAL)
  - Provides timely threat information to utility industry representatives
- NRECA listservs for electric cooperatives
- ES-ISAC – Electricity Sector Information Sharing and Analysis Center
  - Primary location for electric utility industry security information
  - http://www.esisac.com

Important Tools and Information

- DHS website dedicated to security needs for smaller businesses
  - http://www.ready.gov/business/index.html
- FBI's Infragard program
  - http://www.infragard.net

Final Thoughts

- No critical infrastructure owner can mitigate all threats and vulnerabilities
- Some can be mitigated, and for others need to ensure that a vigorous response and restoration plan is in place
- Utilities need to work with customers, other utilities and applicable government entities to ensure that appropriate security-related steps are taken

Questions?

My contact information:

Barry Lawson
NRECA Manager, Power Delivery
703.907.5781
barry.lawson@nreca.coop