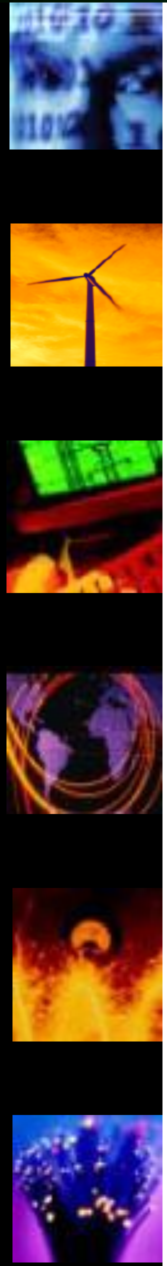


NERC Cyber Security Standards and August 14th Blackout Implications

OSI PI User Group

April 20, 2004

Joe Weiss

jweiss@kemaconsulting.com

(408) 253-7934

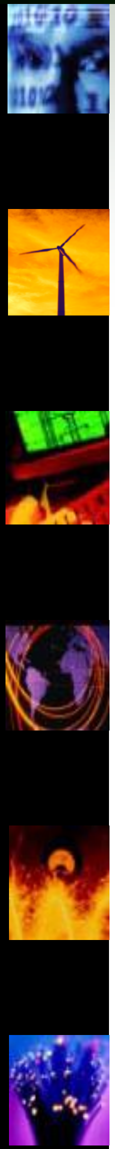
KEMA, Inc.

Control System Cyber Security Summary

- Cyber security threats are real
- Cyber security is not just a regulatory or national infrastructure issue; it makes good business sense
- Technology will continue to evolve to meet demands for productivity and reliability improvements
- Security requirements need to keep pace with technology advancements
- There are workable near-term solutions
- We need to work toward
  - Addressing the gap between IT and operations
  - Long-term technology changes

Current Status

- Government/Industry
  - NERC/FERC
  - Presidential decision directive- HSPD-7
  - DHS/DOE
  - National Strategy to Secure Cyberspace
  - Industry/standards organizations
- Solution
  - Conduct vulnerability and risk assessments
  - Develop recovery plans
  - Address IT/Operations gap
  - Provide training programs



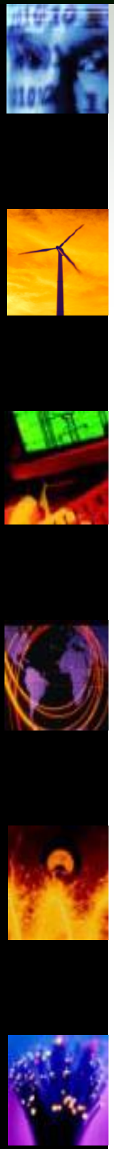
Where is the Industry

- All over the map
- Little information sharing, however….

  everyone wants to know where everyone else is
- Whatever you do will set a precedent

What does the Final Blackout Report Say

- Recommendation 32 – Implement NERC IT Standards
- Recommendation 33 – Develop and deploy IT management procedures
- Recommendation 34 – Develop corporate level IT security governance and strategies
- Recommendation 35 – Implement controls to manage system health, network monitoring, and incident management



Blackout Recommendations (Continued)

- Recommendation 36 – Initiate a US-Canada risk management study
- Recommendation 37 – Improve IT forensic and diagnostic capabilities
- Recommendation 38 – Assess IT risk and vulnerability at scheduled intervals
- Recommendation 39 – Develop capability to detect wireless and remote wireline intrusion and surveillance

Blackout Recommendations (Continued)

- Recommendation 40 – Control access to operationally sensitive equipment
- Recommendation 41 – NERC should provide guidance on employee background checks
- Recommendation 42 – Confirm NERC ES-ISAC as the central point for sharing security information and analysis
- Recommendation 43 – Establish clear authority for physical and cyber security

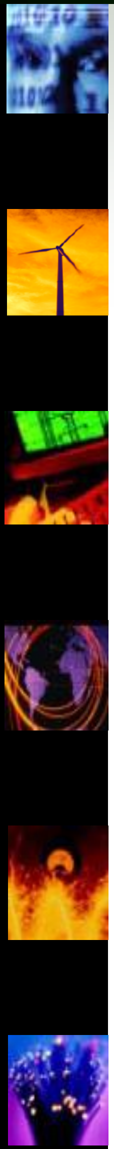
Blackout Recommendations (Continued)

- Recommendation 44 – Develop procedures to prevent or mitigate inappropriate disclosure of information

Blackout Recommendations NOT Addressed by NERC Standard 1200

Blackout Recommendations

- Recommendation 33 – Places on obligation on vendors
- Recommendation 36 – Not addressed (US-Canadian Task Force)
- Recommendation 37 – Emphasis on forensics
- Recommendation 38 – Requires periodic risk and vulnerability assessments
- Recommendation 39 – Wireless not addressed

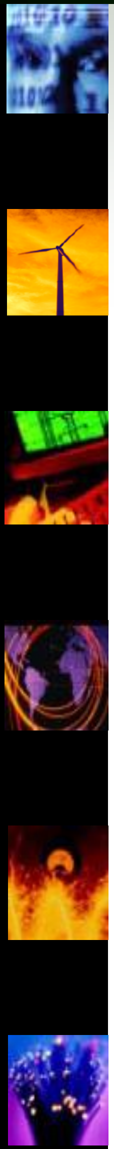


NERC Cyber Security Standards

NERC Cyber Security Standard-1200

- **Purpose**: To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets

  Standard is meant to address operational systems, not IT
- **Applicability:** These standards apply to control areas, transmission owners and operators, and generation owners and operators
- **Scope**: Control Centers
- **Implementation Schedule:**
  - Substantial by First Quarter-04
  - Complete by First Quarter-05



Scope

1201	Cyber Security Policy
1202	Critical Cyber Assets
1203	Electronic Security Perimeter
1204	Electronic Access Controls
1205	Physical Security Perimeter
1206	Physical Access Controls
1207	Personnel
1208	Monitoring Physical Access
1209	Monitoring Electronic Access
1210	Information Protection
1211	Training
1212	Systems Management
1213	Test Procedures
1214	Electronic Incident Response Actions
1215	Physical Incident Response Actions
1216	Recovery Plans

Identified Needs

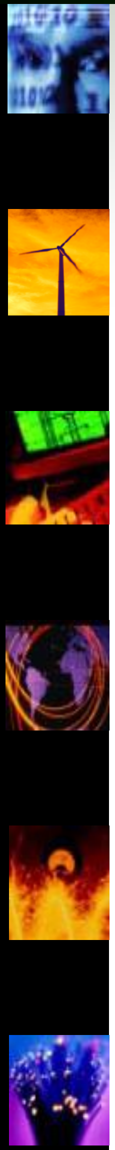
- Cyber security policy for control systems and senior management responsibility (1201)
  - Security policies for SCADA/control systems do not exist
- Define appropriate critical cyber security assets (1202)
  - See previous slides on "Issues to Consider"
- Define cyber security perimeter (1203)
  - See previous slides on "Issues to Consider"
- Methodology for identifying and controlling remote access points (1204)
  - Generic methodology in development
- Identify physical security perimeter for cyber assets (1205)

Identified Needs

- Identify physical access controls for SCADA systems (1206)
- Screening for personnel with access to critical cyber assets (1207)
- Methodology for monitoring physical access for cyber assets (1208)
- Methodology for monitoring electronic access (1209)
  - May need development of logging
- Information protection program for security (1210)
  - SCADA/control system configuration management
- Security training program (1211)
  - Address SCADA/control system specific issues not covered by IT

Identified Needs

- Management policies and identification of capabilities needed to be developed (1212)
  - Password management (special considerations for SCADA/control systems)
  - Authorization and periodic review of access rights
  - Disabling of unauthorized, invalidated, expired, or unused access rights
  - Disabling of unused services and ports (other considerations needed for SCADA/control systems)
  - Secure dial-up modem connections (procedures needed)
  - Firewall management (may not exist in substations, power plants)



Identified Needs (1212 continued)

- Management policies and identification of capabilities needed to be developed (continued)
  - Intrusion detection processes (may not exist in substations, power plants)
  - Security patch management (may not exist for SCADA/control systems)
  - Anti-virus software (could impact control system performance)
  - Retention and review of operator logs, application logs, and intrusion detection logs (may not exist for SCADA/control systems)
  - Identification of vulnerabilities and responses (may be difficult for SCADA/control systems)

Identified Needs

- Security test procedures (1213)
  - Not developed for SCADA/control systems
- Methodology for identifying and performing incident response on electronic intrusions (1214)
  - Methodology for identifying control system incidents
- Incident response for physical intrusions to a cyber asset (1215)
- Recovery plans (1216)
  - Cyber significantly changes business continuity/recovery plans

Expected Gaps

- Control system cyber security policies
- Cyber security test procedures
- Control system cyber security training program
- Configuration management program and policies for cyber security assets
- Methodology for control system cyber incident response
- Cyber impacts on business continuity planning/recovery plans

Final Standard -1300

- Expected to include power plant control systems and substation equipment
- Expected to be risk-based
- Expected to have audits with penalties
- Needs to be available by 2005 since 1200 cannot be extended

Thank You

Joe Weiss (408) 832-5396 - mobile
jweiss@kemaconsulting.com