NERC Critical Infrastructure Department (CID) and CIP Compliance Update

February 28, 2011
NERC is a compliance organization... we are part of NERC

HOWEVER,

We use compliance with CIP Standards to improve security for the electricity industry
CIP Compliance

CIP auditors in North America

- 33 dedicated CIP auditors
- 25 CIP auditor vacancies
- ~ 25 additional Regional or contractor auditors available for augmentation

CIP audits completed in 2010

- Approximately 140 (audits & spot checks)
Recurring Issues

Identification of Critical Assets

• Analysis tools not adequate
• Adjacent entity collaboration/dependency
• Black-start resources

User account management

• Individual logon for SCADA apps but shared O/S accounts
• Passwords not changed for overlooked accounts.
• Incomplete revocation of access
And More Recurring Issues…

Physical Security
- Written policy and Critical Asset configuration discrepancies
- Visitors logged into building but not when entering PSP

Logical Security
- Wandering laptops between the ESP and external networks
- Inadequate security to address risks of open ports, malware and access provisioning
Some of the **Industry** challenges?

Industry struggling with adopting CIP Standards

- Traditional understanding of “security” as “reliability”
- Pressure to manage to compliance vs. security
- CIP Standards compliance may not be adequate to secure the BPS (requirements within standards that are simply documentation)
- Adopting standards rigorous enough to satisfy regulatory authorities yet flexible enough to maintain traditional levels of service at reasonable cost
Some of the **Entity** challenges?

Entities struggling with implementing CIP Standards
- Producing quality evidence in readily auditable form
- Obtaining and sharing “lessons learned” is complicated by need to protect sensitive information
- Applying consistent measures to third parties despite contract limitation and vendor reluctance
- Misunderstanding CIP Standards by entity SME’s
Some of the **Regional** challenges?

Regions struggling with auditing CIP Standards

- Access to evidence prior to audit team arrival
- Auditing strictly to the Standard and nothing more
  - despite real or perceived shortcomings
- Entity SMEs who have limited availability
Some of the **ERO** challenges?

ERO compliance struggling with CIP Standards

- Interpreting the meaning and implementation of CIP Standards in a consistent manner across Regions
- Balancing “arms length” relationship between auditors and entities while working together to improve reliability
General CIP Auditing Issues

- Consistency in interpretation of standards
- Maintaining qualified/experienced CIP auditors
- Auditor workload
- External entities impact on RE compliance
- Lack of vendor incentives to comply with standards
- CIP standards developing at a slow rate and not publicly perceived as being as comprehensive or as mature as other cybersecurity standards
CIP Auditor Training

- CCWG/NERC workshops
  - 2 CIP specific Auditor Workshops
  - 2 “piggybacks” with 693 Auditors
- MRO contracted for Auditor Training
- Security+ certification required in one region
- ICS cybersecurity professional certification?
- Training and CE’s to maintain certifications
  - GIAC, CISA, CISM, CISSP, etc.
- INL Advanced Cybersecurity training
  - Red/Blue team exercise
Sufficiency Review Program (SRP)

- Pilot Sufficiency Review Program (SRP) in 2010
- Sufficiency of CIP-002 V3 Risk Based Methodology
- Three Entities selected - final report issued
- 2011 SRP will continue 12 Registered Entities
- Regions notified and NERC is soliciting volunteers
Technical Feasibility Exceptions (TFE)

- TFE process is complex and confusing
- TFE submissions require extensive resources
- Approximately 8000 TFE’s submitted
- Technologies and systems requiring TFEs are frequently well-known limitations that standards should or could address by (e.g., anti-malware protections on integrated devices, procedural controls around passwords)
NERC is a compliance organization... we are part of NERC

HOWEVER,

We use compliance with CIP Standards to improve security for the electricity industry
Manage Threat, & Consequence component

Operational Zone

Research, develop, deploy technical solutions

NERC Standards (fully implemented)

ES-ISAC Alerts and Notifications
CRPA's
NERC Monitoring

Network Isolation
New protective measures
New Architectures

Secure

Compliant

Nascent Company Capability’s
A conversation…

• We’ve been actively listening
• Reorganized CID to meet needs we heard
• Goals are focused and worth pursuing
• This is the start of a conversation…the dialogue is ripe for change
CID Functional Organization

**Mission**
- **Risk Management**
- **Standards Support**
- **Policy & Coordination**

**Programs**
1. Risk Analysis and Security Guidelines
2. Incident Response
3. Information Sharing and Analysis
4. Industry and Laboratory Coordination
5. Standards Development
6. Exception Processing
7. Training & Exercises
8. Readiness Support
9. CIPC Coordination
10. CIP Audit Support
11. Planning and Coordination
12. CMEP Liaison
Understanding the issues

- The electricity sector is facing rapidly emerging threats with escalating potential impact...just like everyone else!
- Communications must be improved to both enhance security program adoption and overall perception
- Perception of low industry acceptance of CIP standards translates to complexities in relationships, policy development and security readiness
2011 Objectives

1. Refresh ES-ISAC to enhance intelligence gathering, secure communications and information sharing.
2. Expand Cyber Risk Preparedness Assessment (CRPA) program
3. Develop public Internet monitoring capability for enterprise visibility
4. Conduct NERC Grid Security Conference (NERC GridSecCon) and establish cybersecurity technical training program
5. Develop and conduct cybersecurity exercise (NERC GridEx)
6. Leverage DOE National Laboratory cybersecurity research and expertise
7. Streamline CIP standards development and TFE processing
8. In coordination with NIST and DOE, develop electricity sector enterprise-wide risk management process
He didn’t think cybersecurity was a big issue either.

How can NERC support industry better?