CSWG

FERC Technical Conference, Atlanta November 14, 2010

Cyber Security Review

Daniel Thanos (daniel.thanos@ge.com),
Co-Chair of Cryptography, BU, R&D,
Chief Cyber Security Architect, GE Digital Energy

Security Drivers for Adoption

- Adoption of the IEC Standards will enable better security models as well as existing and new tools to leverage them

- Open standards for inter-exchange of data that represents critical devices and system state/configurations can enable deeper forms of security intrusion detection and prevention

- Open systems enable better and wider analysis by the security community as compared to proprietary ones

Review Process of IEC 62351

- CSWG Standards group mandate
- Open and voluntary review process
- Provides a good initial step for the industry towards better functional notions of stronger security
- CSWG Standards group IEC 62351 report section highlights points where further revision is needed
- Examples: Erroneous security definition and terms, referencing of older crypto protocol versions, use of crypto primitives that are not well aligned to NISTIR
- All parties are aware and will work to continue evolution of work but adoption should acknowledge the need for some revisions
- TC57/WG15 is also starting development of a more detailed standard for key management and crypto that will offer more optimal methods

Security Guidance for Adoption

- More widely open and formal review process with comments for a final validation
- Posting and announcing alone is not enough, active outreach to broader security community is needed
- Any adopted standards should not preclude the use of more updated and secure referenced standards

NISTIR 7628

- Key to strategy and roadmap
- Requirements for Product and system development
- Security framework for projects
- Informing cyber security training and education
- Needed further development and/or supporting work (Start of Design Principles Group)