NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Webcast on Proposed Cyber Security Standard 1300

October 18, 2004

Summary of Question and Answer Session

Questions on Definitions

Q) How did the drafting team develop its definition of bulk electric system facilities, and will NERC develop a glossary of terms to prevent the creation of conflicting definitions?

A) The drafting team used the definition of bulk electric system facilities created by CIPC's Risk Assessment Working Group. The RAWG formulated its definition after reviewing existing definitions in various NERC documents.

NERC will create a glossary of terms from its reliability standards, but only one such standard exists at present.

Q) Does the definition of bulk electric system facilities belong in a cyber security standard?

A) The drafting team believes that identifying bulk electric system facilities is the first step to drilling down to the identification of critical cyber assets, and, therefore, belongs in this standard.

Q) Some stand-alone bulk electric system facilities that alone are not critical, may become critical when considered together with other bulk electric system facilities. Are these stand-alone facilities critical?

A) The determination of criticality is up to the individual entity.

Q) Urgent Action Cyber Security Standard 1200 explicitly excludes process control systems. Does 1300 also exclude these systems?

A) No, 1300 does not specifically exclude process control systems. However, networked systems that do not use a routable protocol or cannot be accessed via dial-up modem are excluded.

Q) Are cyber assets that communicate via serial protocol excluded? Are cyber assets on a closed IP network excluded?

A) Devices that communicate via a serial protocol cannot be compromised and used to control other devices. If assets on an isolated IP network are not susceptible to malicious access or abuse then they would be excluded. The FAQ provided by the drafting team helps define context of exclusion.

Q) Are nuclear units excluded?

A) Yes. This exclusion is documented in the Standards Authorization Request for 1300, but will be added to the standard itself.

Q) By definition, do critical cyber assets include E-Tag, OASIS, or Market Systems?

A) No. This standard includes critical cyber assets that support reliability functions, not business functions.

Q) Some market systems are tightly integrated into reliability systems. Are those market systems excluded?

A) It is up to individual entities to perform their risk analysis and determine which cyber assets are critical. If a market system resides on the same network as a critical cyber asset that supports reliability, it also would be considered a critical cyber asset.

Q) Standard 1300 defines types of critical cyber assets. How does that meet the intent of basing criticality on risk assessments?

A) The assets described in 1300 will almost always meet the definition of critical cyber asset. If an asset does not meet the definitional criteria, then entities can exclude them.

Questions on Personnel Screening

Q) Does the requirement for personnel screening permit "grandfathering?" If so, what are the grandfathering criteria?

A) Employees, contractors, and service providers who have had a background screening check within the previous five years from the implementation date of the standard will be "grandfathered," for a period not to exceed five years. Entities will be required to screen all others who have unrestricted access to critical cyber assets. The standard requires re-screening every five years.

Q) What are the criteria for background screening? Is drug testing included?

A) The standard requires social security number verification and seven year criminal check. Other criteria, such as drug testing, are left to the discretion of the individual entities. All background screening must be conducted in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

The FAQs for Section 1303 include references in the subject area. The team also recommends consulting in-house labor law experts for assistance.

Other 1300 Topics

Q) Why doesn't 1300 explain how to conduct a Risk Assessment? It would be useful to have examples.

A) A standard cannot include examples. The drafting team will update its FAQs to include more guidance. Also, NERC's Security Guidelines (available at www.esisac.com/library) contain more information about risk assessment approaches and resources.

Q) Are the requirements of AGA 12 applicable to this standard?

A) No, AGA 12 is an encryption standard. Encryption is not addressed in 1300.

Q) Under 1306, limited penetration tests are required. Did the drafting team consider vulnerability assessments instead?

A) The requirement limits controlled penetration testing to points of ingress and egress to the electronic security perimeter. The team recognizes the risk of poorly conducted testing, but does believe that testing at the perimeter provides meaningful information.

Q) In section 1307, incident reporting to the ES ISAC is required. How does the ES ISAC assure that sensitive information is not made public?

A) NERC is not a government entity, thus, it is not subject to the Freedom of Information Act. Furthermore, those submitting the incident reports determine with whom NERC may share information. If the data can be shared with the U.S. Department of Homeland Security, it is considered a voluntary submittal and is protected from disclosure by DHS.

Q) Comments submitted during the balloting of Urgent Action Cyber Security Standard 1200 indicated that 24 hours was impractical to update access control lists, yet the criteria in 1300 is more strict. Isn't this contradictory to industry expectations?

A) The drafting team did consider comments made in response to the Urgent Action Cyber Security Standard, but believed that stricter requirements were necessary to improve the level of cyber security across the industry.

Q) Telecommunications extend electronic perimeters, but telecommunications devices are excluded from 1300. Why?

A) The industry emphatically told NERC that telecommunications security should not be included in its Cyber Security Standard. (See comments that the drafting team received in response to its Standards Authorization Request on this standard.)

Q) Reliability Coordinators and Control Areas must self-certify compliance to Urgent Action Cyber Security Standard 1200. Should we expect the same for 1300?

A) No. NERC's functional model will be implemented with Version 0; therefore, all applicable entities as defined in Standard 1300 must comply with the standard.