Michael Assante
Vice President and Chief Security Officer

April 7, 2009

TO: Industry Stakeholders

RE: Critical Cyber Asset Identification

Ladies & Gentlemen,

In the interests of supporting NERC's mission to ensure the reliability of the bulk power system in North America, I'd like to take this opportunity to share my perspectives with you on the results of NERC's recently completed self-certification compliance survey for NERC Reliability Standard CIP-002-1 – Critical Cyber Asset Identification for the period July 1 — December 31, 2008 along with our plans for responding to the survey results. As you may already be aware, compliance audits on this standard will begin July 1, 2009.

The survey results, on their surface, raise concern about the identification of Critical Assets (CA) and the associated Critical Cyber Assets (CCA) which could be used to manipulate them. In this second survey, only 31 percent of separate (i.e. non-affiliated) entities responding to the survey reported they had at least one CA and 23 percent a CCA. These results are not altogether unexpected, because the majority of smaller entities registered with NERC do not own or operate assets that would be deemed to have the highest priority for cyber protection. In that sense, these figures are indicative of progress toward one of the goals of the existing CIP standards: to prioritize asset protection relative to each asset's importance to the reliability of the bulk electric system. Ongoing standards development work on the CIP standards seeks to broaden the net of assets that would be included under the mandatory standards framework in the future, but this prioritization is an important first step to ensuring reliability.

Closer analysis of the data, however, suggests that certain qualifying assets may not have been identified as "Critical." Of particular concern are qualifying assets owned and operated by Generation Owners and Generation Operators, only 29 percent of which reported identifying at least one CA, and Transmission Owners, fewer than 63 percent of which identified at least one CA.

Standard CIP-002 "requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System." The standard goes on to specify that these assets are to be "identified through the application of a risk-based assessment." Although significant focus has been placed on the development of risk-based assessments, the ultimate outcome of those assessments must be a comprehensive list of all assets critical to the reliability of the bulk electric system.

A quick reference to NERC's glossary of terms defines a CA as those "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

Most of us who have spent any amount of time in the industry understand that the bulk power system is designed and operated in such a way to withstand the most severe single contingency, and in some cases multiple contingencies, without incurring significant loss of customer load or risking system instability. This engineering construct works extremely well in the operation and planning of the system to deal with expected and random unexpected events. It also works, although to a lesser extent, in a physical security world. In this traditional paradigm, fewer assets may be considered "critical" to the reliability of the bulk electric system.

But as we consider cyber security, a host of new considerations arise. Rather than considering the unexpected failure of a digital protection and control device within a substation, for example, system planners and operators will need to consider the potential for the simultaneous manipulation of all devices in the substation or, worse yet, across multiple substations. I have intentionally used the word "manipulate" here, as it is very important to consider the misuse, not just loss or denial, of a cyber asset and the resulting consequences, to accurately identify CAs under this new "cyber security" paradigm. A number of system disturbances, including those referenced in NERC's March 30 advisory on protection system single points of failure, have resulted from similar, non-cyber-related events in the past five years, clearly showing that this type of failure can significantly "affect the reliability (and) operability of the bulk electric system," sometimes over wide geographic areas.

Taking this one step further, we, as an industry, must also consider the effect that the loss of that substation, or an attack resulting in the concurrent loss of multiple facilities, or its malicious operation, could have on the generation connected to it.

One of the more significant elements of a cyber threat, contributing to the uniqueness of cyber risk, is the cross-cutting and horizontal nature of networked technology that provides the means for an intelligent cyber attacker to impact multiple assets at once, and from a distance. The majority of reliability risks that challenge the bulk power system today result in probabilistic failures that can be studied and accounted for in planning and operating assumptions. For cyber security, we must recognize the potential for simultaneous loss of assets and common modal failure in scale in identifying what needs to be protected. This is why protection planning requires additional, new thinking on top of sound operating and planning analysis.

"Identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System" necessitates a comprehensive review of these considerations. The data submitted to us through the survey suggests entities may not have taken such a comprehensive approach in all cases, and instead relied on an "add in" approach, starting with an assumption that no assets are critical. A "rule out" approach (assuming every asset is a CA until demonstrated otherwise) may be better suited to this identification process.

Accordingly, NERC is requesting that entities take a fresh, comprehensive look at their risk-based methodology and their resulting list of CAs with a broader perspective on the potential consequences to the entire interconnected system of not only the loss of assets that they own or control, but also the potential misuse of those assets by intelligent threat actors.

Although it is the responsibility of the Registered Entities to identify and safeguard applicable CAs, NERC and the Regional Entities will jointly review the significant number of Table 3 and 4 entities[1] that reported having no CAs to determine the root cause(s) and suggest appropriate corrective actions, if necessary. We will also carry out more detailed analyses to determine whether it is possible that 73% of Table 3 and 4 Registered Entities do not possess any assets that, "if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

Additionally, NERC plans to host a series of educational webinars in the coming weeks to help Registered Entities understand CIP standards requirements and what will be required of them to demonstrate compliance with the standards once audits begin in July. NERC also plans to incorporate a set of informational sessions into this series, designed to allow the industry to share practices and ask questions of each other in an open, but facilitated, dialogue.

We expect to see a shift in the current self-certification survey results as entities respond to the next iteration of the survey covering the period of January 1 – June 30, 2009 and when the Regional Entities begin to conduct audits in July.

I look forward to an ongoing dialogue with you on these important issues. As always, please do not hesitate to contact me, or any of my staff, with any questions or concerns.

Sincerely,

Michael Assante
Chief Security Officer

---

[1] Table 3 and 4 entities refers to those entities identified in the Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1.