



SPP RE Assessment

Monitoring and Implementation of

Reliability Standard CIP-002-1

Cyber Security – Critical Cyber Asset Identification

Requirement R1

Critical Asset Identification Method

January 18, 2010



1. Introduction

The cornerstone to compliance with the NERC Reliability Standards CIP-002-1 through CIP-009-1, collectively referred to as the Cyber Security Standards, is a meaningful risk based assessment methodology. The methodology sets the stage for the rest of the Cyber Security Standards in that it defines the procedures and criteria for identifying those facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.¹ Only after a registered entity has identified one or more Critical Assets and then has identified one or more Cyber Assets essential to the reliable operation of the Critical Asset(s)² do the remaining Cyber Security Standards come into scope.

All entities in the SPP RE footprint registered as a Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, or Load Serving Entity are subject to the Cyber Security Standards.³ Initial compliance milestone dates for an entity's registered function are defined in Tables 1 through 4 of the *(Revised) Implementation Plan for Cyber Security Standards - CIP-002-1 through CIP-009-1*, dated 2/3/2006⁴. Each entity is required to self-certify its compliance status semi-annually and additionally answer a number of questions regarding the types and numbers of identified Critical Assets.

Michael Assante, NERC's Chief Security Officer, raised concerns about the industry's identification of Critical Assets (CA) in an April 7, 2009 letter to the industry⁵. In that letter, Mr. Assante pointed out that only 31 percent of separate (i.e. non-affiliated) entities responding to a recent survey reported they had at least one Critical Asset. The letter goes on to state that while not entirely unexpected due to the number of small entities that do not own or operate high impacting assets, closer examination of the survey results,

“...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.”

NERC requested 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 (*emphasis added*) of those assets by intelligent threat actors.”

Similarly, in Order 706 approving Version 1 of the Cyber Security Standards, the Federal Energy Regulatory Commission (FERC) stated at Paragraph 280:

...Requirement R1.2.1 requires responsible entities to consider control centers and backup control centers as potential critical assets. In determining whether those control centers should be critical assets, we believe that responsible entities should examine the impact on reliability if the control centers are unavailable, due for example to power or communications failures, or denial of service attacks. Responsible entities should also examine the impact that misuse of those control centers could have on the electric facilities they control and what the combined impact of those electric facilities could be on

¹ See the NERC Glossary of Terms Used in Reliability Standards: Critical Asset.

² See the NERC Glossary of Terms Used in Reliability Standards: Critical Cyber Assets.

³ See Section 4 (Applicability) of each of the NERC Reliability Standards CIP-002-1 through CIP-009-1.

⁴ Download the implementation plan at:

http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf

⁵ Download the letter to the industry at: <http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf>

the reliability of the Bulk-Power System. The Commission recognizes that, when these matters are taken into account, it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset.

Given the importance of the risk based assessment methodology in identifying Critical Assets, the SPP RE undertook a project in the second half of 2009 to evaluate the methodologies of all registered entities in the SPP RE region subject to Tables 1, 2, or 3 of the version 1 implementation plan. As the Compliant milestone date had already been reached for Table 1 and 2 entities, the evaluation was conducted in the form of a compliance spot check of CIP-002-1, Requirement R1. Table 3 entities were also requested to submit their methodologies for review in the form of a data request, with no compliance implications due to the fact that the Compliant milestone date was still in the future. Table 4 entities were not included in this project. The breakdown of the registered entities by applicable implementation plan table is depicted in Figure 1. When multiple implementation plan tables are applicable, the entity was categorized using the earliest applicable Compliant milestone date.

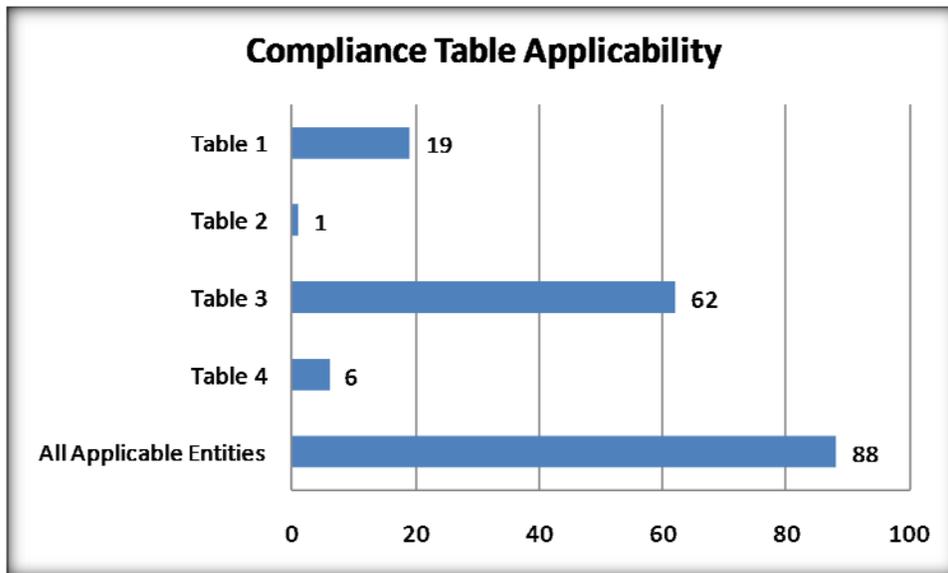


Figure 1 – Entity Categorization

Registered entities typically perform multiple functions. Figures 2, 3, and 4 break down the entities by registered function.

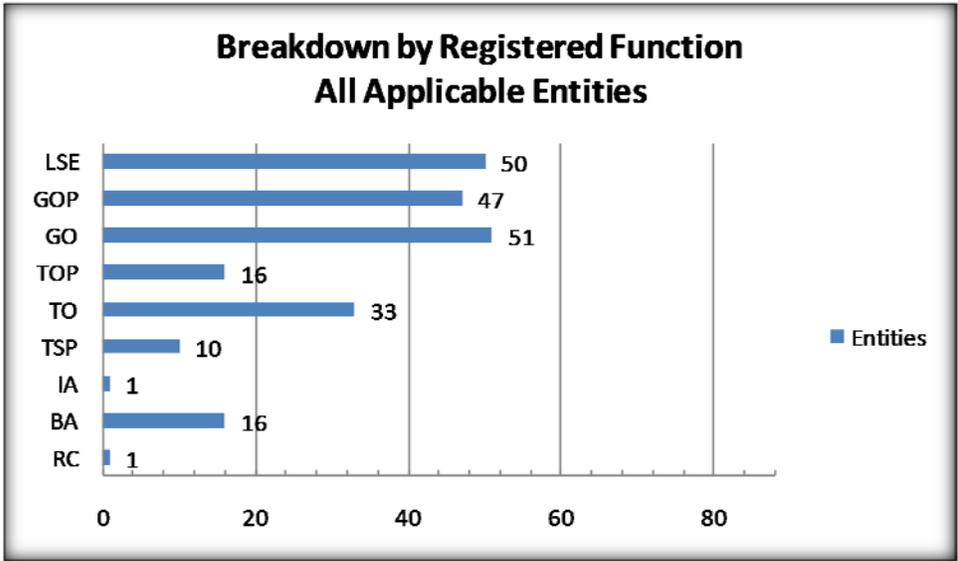


Figure 2 – Registered Functions (All Applicable Entities)

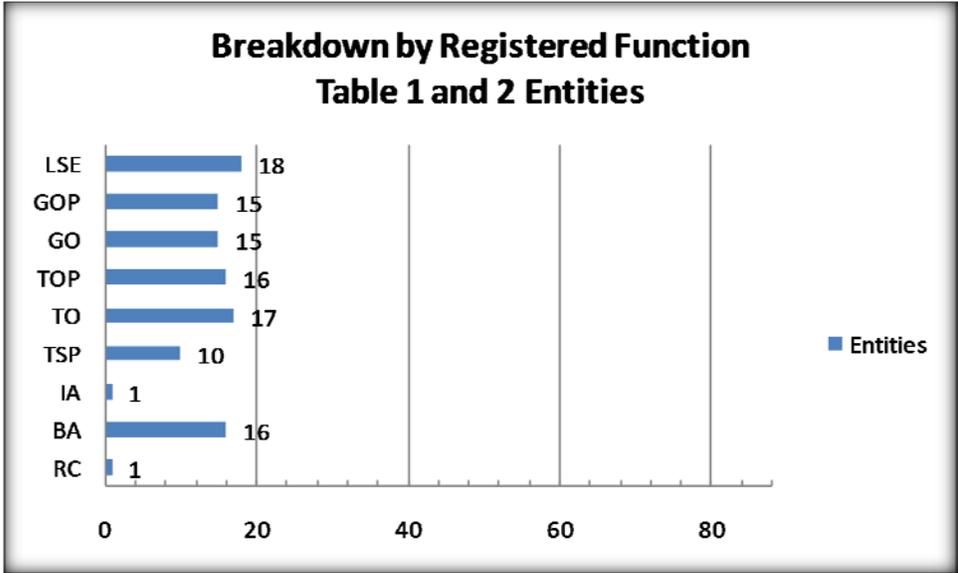


Figure 3 – Registered Functions (Table 1 and 2 Entities)

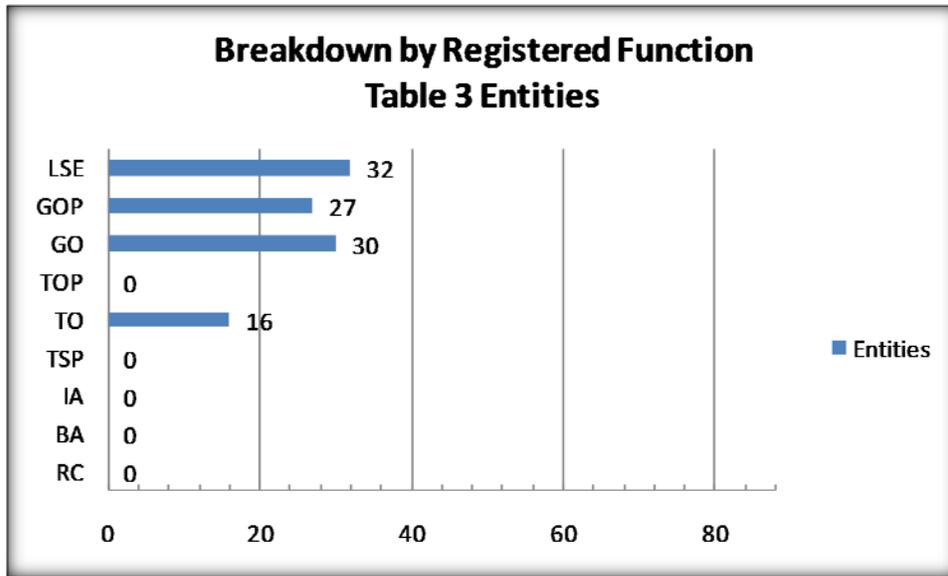


Figure 4 – Registered Functions (Table 3 Entities)

The compliance (or apparent compliance with respect to Table 3 entities) was determined and reported to the registered entity. In addition to identifying non-compliance issues, each entity’s report included a number of suggestions for improvement for the entity’s consideration.

This document presents the results of an analysis of the risk based assessment methodology evaluation project.

2. Analysis

Evaluation of Compliance

Overall, as depicted in Figure 5, 16 of 20 Table 1 and 2 entities were found to be compliant with CIP-002-1, Requirement R1, and 40 of 62 Table 3 entities appeared to be compliant.

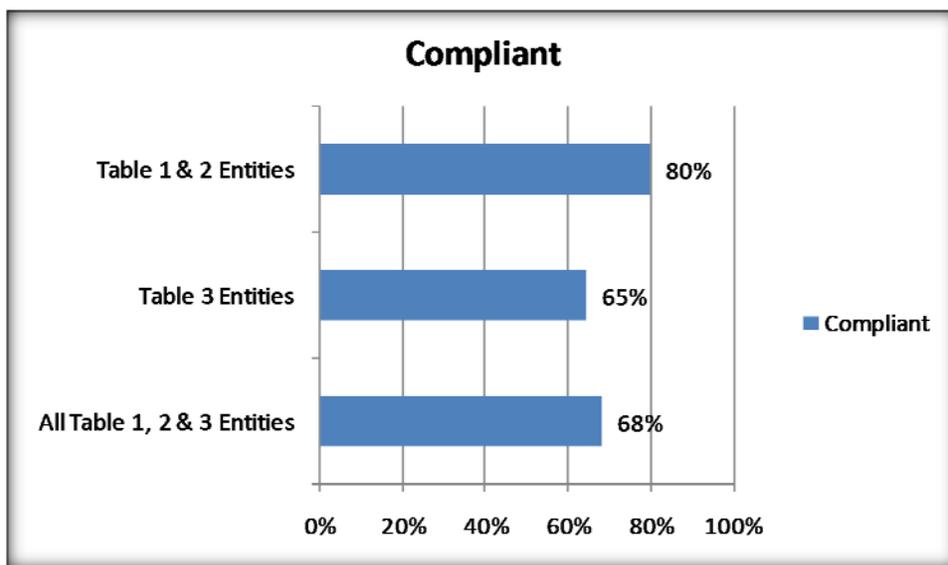


Figure 5 – Compliance with CIP-002-1/R1

For the remaining entities with deficient methodologies, concerns were found with one or both major sub requirements. Requirement R1.1 requires the registered entity to maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria. Considerable latitude is given to the registered entity in determining how the assessment is to be conducted and what criteria are to be applied. Typically, the entity will choose to rely upon an experience-based approach (also referred to as a red-team approach), an engineering analysis approach, or a hybrid of the two.

If an experience-based evaluation is performed, the methodology will ideally identify the scenarios evaluated in reaching the Critical Asset determination. If an engineering analysis approach is used, the methodology will ideally identify the engineering criteria thresholds used in reaching the Critical Asset determination. Criteria, especially engineering thresholds, can be supported by other NERC standards, SPP criteria, or other published references.

There are a variety of resources available to the registered entity in defining the Critical Asset identification criteria. Perhaps the most comprehensive guidance can be found in the “Security Guideline for the Electricity Sector: *Identifying Critical Assets*” document posted on the NERC web site as a Guideline in Support of a Standard.⁶ Other resources include:

1. NERC Reliability Standards TPL-001 through TPL-004
2. Attachment 1-EOP-004 to NERC Reliability Standard EOP-004-1
3. Published IROL flow gates
4. Published regional criteria or standards
5. DOE OE-417 reporting criteria
6. The entity or regional black start plan

As depicted in Figure 6, approximately one in ten risk based assessment methodologies did not include the procedures for performing the annually required Critical Asset identification. Approximately two in ten assessment methodologies either failed to include criteria for identifying Critical Assets, or the documented criteria was insufficient to determine how an asset was identified to be critical. One Table 3 entity failed to submit a risk based assessment methodology for review and a second Table 3 entity asserted the use of Reasonable Business Judgment in lieu of a documented risk based assessment methodology for identifying Critical Assets.

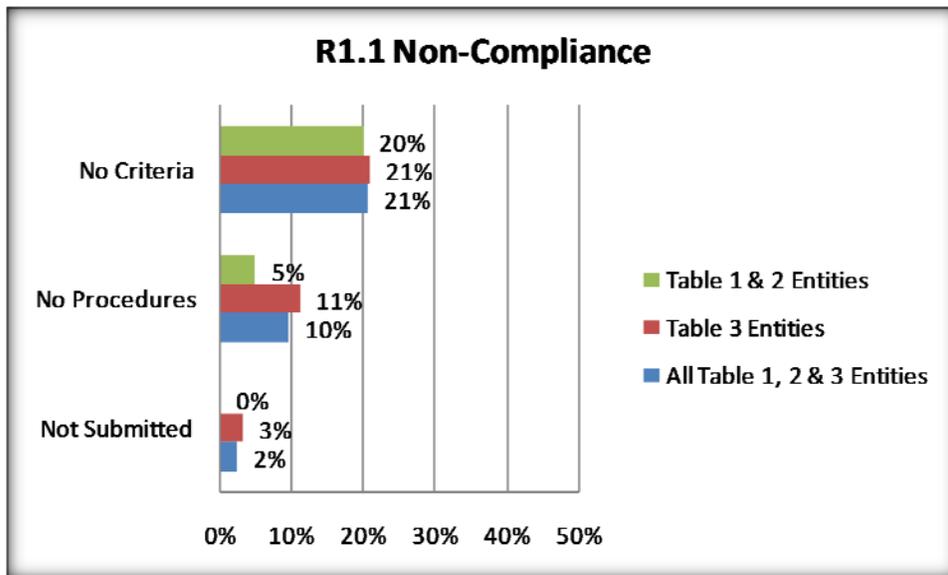


Figure 6 – Requirement R1.1 Deficiencies

⁶ Download the Guideline at: http://www.nerc.com/fileUploads/File/Standards/Reference%20Documents/Critical_Asset_Identification_2009Nov19.pdf

With respect to invoking Reasonable Business Judgment in lieu of documenting a risk based assessment methodology, CIP-002-1, Requirement R1 prescribes that “[t]he Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.” This is a specific action that must be taken, is not subject to discretion, and therefore is not subject to Reasonable Business Judgment.

Requirement R1.2 requires the risk based assessment methodology to consider seven specific types of assets:

1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of the standard.
2. Transmission substations that support the reliable operation of the Bulk Electric System.
3. Generation resources that support the reliable operation of the Bulk Electric System.
4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.
5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.
6. Special Protection Systems that support the reliable operation of the Bulk Electric System.
7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

In some instances the risk based assessment methodology did not explicitly reference or consider any of the seven required elements. In other instances, the methodology considered some but not all of the required elements. Figure 7 depicts the occurrences of concern for each requirement. While Requirement R1.2.7 (additional assets deemed appropriate for inclusion) is shown, this element was only counted if the risk based assessment methodology also failed to consider one or more of the other six elements. For methodologies that only failed to explicitly reference and consider additional assets (R1.2.7), that aspect of the methodology was deemed to be compliant with a suggestion for improvement.

In a significant number of risk based assessment methodologies where Requirement R1.2 was an issue, the registered entity only considered the types of assets it owned or operated. For example, a generation owner might have only considered its generation resources (Requirement R1.2.3) and possibly its system restoration facilities (Requirement R1.2.4). While this approach is understandable, it is not compliant. Each of the seven elements prescribed in the NERC standard should be explicitly referenced, with an acknowledgement that the entity does not own or operate a specific element where appropriate. It should not be “understood” that a required element is not applicable to the entity. Additionally, referencing an inapplicable element as such in the methodology serves as a reminder and place holder for the future in the instance assets of that type are added to the list of owned and operated assets.

Several registered entities simply restated the language of the CIP-002-1 requirements. In the absence of any additional information, this approach is insufficient to demonstrate each of the required elements has actually been considered. Several other registered entities failed to reference or consider the required elements in the documented methodology itself (the requirement) but accounted for one or more of the elements in worksheets used in conjunction with the actual annual assessment. Depending on how the various documents and worksheets are linked and cross-referenced, this approach may or may not be accepted as being compliant. For example, a conforming worksheet would typically be accepted if the risk based assessment methodology explicitly referenced the use of the worksheet in the assessment procedures part of the document.

The Critical Asset Identification criteria required by Requirement R1.1 is best placed into the methodology in the context of the specific asset type (element) prescribed by Requirement R1.2. In this manner, not only is it clear the required element has been considered, the application of the criteria is also well understood.

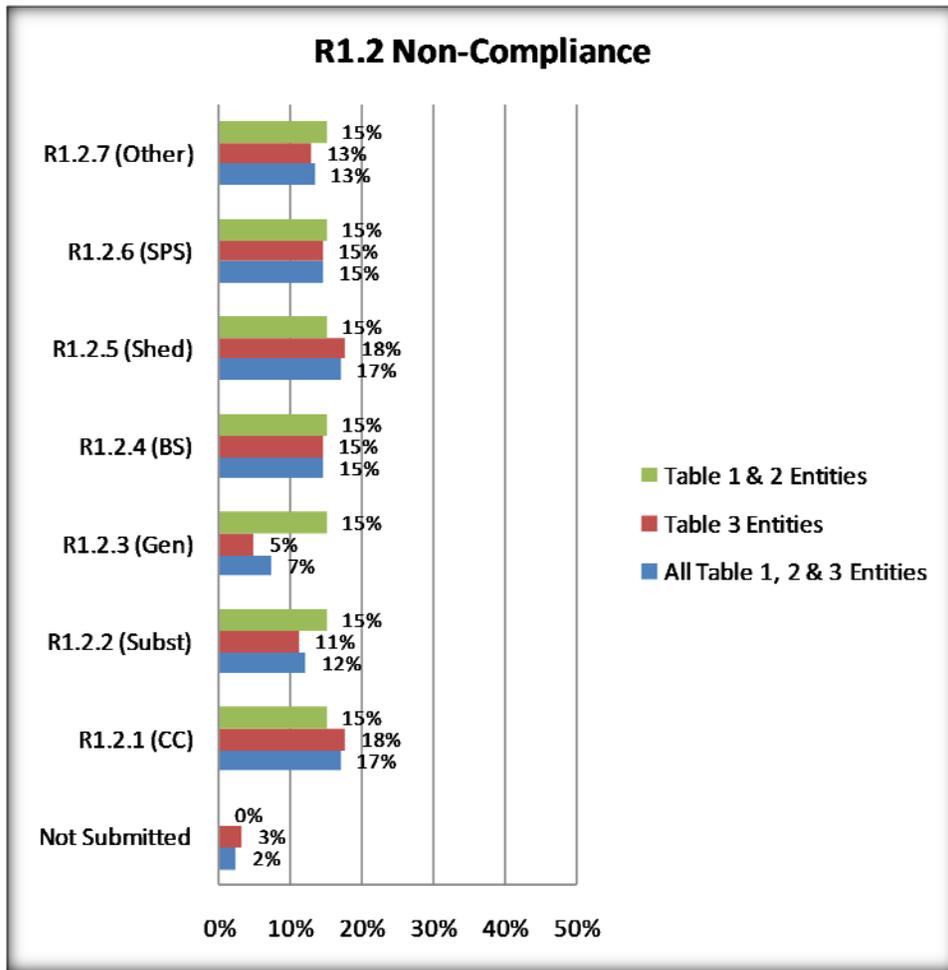


Figure 7 – R1.2 Deficiencies

In addition to two Table 3 entities that failed to submit a risk based assessment methodology for review, nine registered entities submitted a traditional risk assessment process in lieu of a risk based assessment methodology. While appropriate for corporate risk management, the traditional risk assessment is ill suited for the purposes of the CIP standards. As noted in the NERC “Security Guideline for the Electricity Sector: *Identifying Critical Assets*”, “risk” is a function of impact (or consequences) and the probability of occurrence of a security event. Threat is commonly defined as “the potential for a particular threat-source to successfully exploit a particular vulnerability” according to NIST Special Publication 800-30. Quantitatively determining threat is a difficult and subjective task, especially when it comes to the threat of a cyber attack. The Guideline notes that a conservative approach is to assume the potential for threats always exists. Likewise according to NIST, vulnerability is “a weakness that can be accidentally triggered or intentionally exploited”. The Guideline points out that quantifying vulnerabilities is also difficult and dynamic. Cyber hackers discover new vulnerabilities every day. Therefore, it is conservative to assume that vulnerabilities will always be present in any network or physical protection scheme. While a traditional risk assessment normally considers both the probability of loss and the impact or consequences of the loss, the CIP-002-1 standard relies upon the definition of Critical Assets as found in the NERC Glossary. The Glossary defines Critical Assets as “Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.” Using that definition, the CIP-002-1 standard expects the methodology to assume the asset has been lost and to evaluate the resulting consequences. The risk based assessment methodology essentially becomes an impact analysis that asks the simple question: Does an asset, if destroyed, degraded, compromised or otherwise rendered unavailable, adversely impact the reliability or operability of the BES?⁷

⁷ Security Guideline for the Electricity Sector: Identifying Critical Assets, Page 2.

A major difficulty in attempting to use a traditional risk assessment rather than assuming the probability (or likelihood) of occurrence is 1.0 (100%) is justifying the assigned probability for any given asset. Entities typically do not have sufficient, credible threat information to make such an estimate, thus the assigned probability is often an arbitrary number. Similarly, the relative cost of a successful attack or the compensating and mitigating measures in place to protect the asset, while a valid aspect of risk management, have no bearing on whether the asset, if lost or compromised, is a Critical Asset as defined in the NERC Glossary.

Suggested Improvements

In addition to opining on whether the presented risk based assessment methodology was compliant with CIP-002-1, Requirement R1, each evaluation included one or more suggestions for improvement. These suggestions are not to be construed as Remedial Action Directives (as defined in Section 7.0 of the NERC Compliance Monitoring and Enforcement Program). They do, however, represent in many cases issues or concerns cited in FERC Order 706.

Several suggestions received prominent attention. Only a handful of registered entities considered the impact of **misuse** of the asset in addition to the complete loss of the asset. In reality, the misuse of an asset often poses the greater risk to the reliability of the Bulk Electric System. For example, the loss of a SCADA/EMS system at the primary control center typically results in a fail over, either to the standby system or to the backup control center. Should both the primary and backup control center systems be taken down, manual control procedures can be initiated until the automated control systems are restored. In the short term, the risk to the Bulk Electric System could be relatively minor and the lights will stay on. However, a compromise of the same SCADA/EMS system resulting in its misuse could have serious ramifications. Remembering that a SCADA/EMS system effectively controls most or all of the registered entity's generation and/or transmission assets, a malicious attack that, for example, disconnects generation resources while leaving load connected could result in a local blackout or worse due to voltage or frequency excursions.

In addition to considering misuse, the registered entity is well advised to consider abnormal operating conditions. There are several issues here. First, the Bulk Electric System is designed to survive an N-1 contingency, such as the loss of a generating unit or transmission line. However, multiple contingency events, such as the loss of a multi-unit generating plant or a large transmission substation could have markedly different results. Second, some registered entities rely upon redundancy as an argument for not declaring assets as critical. While not prevalent in the SPP RE, some registered entities have determined their control centers are not "critical" because there is a backup control center available. Others have asserted a control center asset is not critical because while, for example, it can be used to control the transmission system if needed, that is not its normal function. However these determinations do not consider the impact of possible misuse. Within the SPP RE, some registered entities have asserted that restoration assets need not be designated as critical because there are alternate paths. Certain assets appear, however, in the regional black start plan. While there may be alternatives in the instance a specific restoration asset is not available, the assets in the black start plan that are not qualified as "if needed" should be identified as Critical Assets. The region conducts periodic training and recovery drills using the black start plan and the assets in the plan are the resources being relied upon for fast restoration from a blackout. Having to devise a "Plan B" because primary path resources are not available will likely unnecessarily prolong the recovery process.

A number of generation owner/operator-only entities assert that they cannot perform a proper risk based assessment because they do not have sufficient information about their potential impact to the Bulk Electric System. While this may be true, the entity is not relieved of its responsibility for devising a compliant methodology and identifying its Critical Assets. Such encumbered entities should consider seeking engineering analysis support from their Balancing Authority and/or Southwest Power Pool. And, when the supporting entity states the registered entity does not have any Critical Assets, the entity needs to ask what the specific criteria was in making that determination. That criteria should be documented in the entity's risk based assessment methodology. Simply stating in the methodology that another entity has or will make the determination of Critical Assets is not sufficient to demonstrate compliance. It would be best if a copy of the actual analysis results is obtained for inclusion with any compliance documentation.

Finally, once a registered entity has identified its Critical Assets, best practice would be for it to seek a concurring opinion. The FERC, at Paragraph 322 of Order 706, found that an external review of critical assets by an appropriate organization is needed to assure that such lists are considered from a wide-area view (i.e., from a regional perspective) and that an external review will provide an appropriate level of consistency. The registered entity can seek an opinion from its Balancing Authority (if it is not a BA itself). The entity can also seek a concurring opinion from neighboring utilities and the Southwest Power Pool Reliability Coordinator.

3. Summary

A total of 88 entities registered in the SPP RE region are subject to the Cyber Security Standards (CIP-002-1 through CIP-009-1) by virtue of their registered functions. Six entities are recent registrants subject to Table 4 of the Version Cyber Security Standards implementation plan and were not included in the evaluation project. Of the 82 entities in the SPP RE region whose risk based assessment methodologies were evaluated, approximately 68% were found to be compliant. The evaluation only looked at the entity's current methodology and did not confirm full compliance dating back to July 1, 2008 for Table 1 and 2 entities. Similarly, the evaluation did not consider whether the methodology had been properly applied to identify Critical Assets or, following that, if Critical Cyber Assets had been properly identified.

Where an entity was not compliant, deficiencies of Critical Asset identification criteria were twice as prevalent as deficiencies in the documented process itself. Entities either failed to explicitly reference or consider any of the required elements in Requirement R1.2, or more typically only referenced and considered the types of assets they owned or operated.

Two entities failed to submit a documented risk based assessment methodology at all, with one of the two asserting the application of Reasonable Business Judgment in lieu of a documented methodology.

Every registered entity received suggestions for improvement. Suggestions were tailored to their risk based assessment methodology. The most common suggestions included consideration of misuse of the asset, consideration of abnormal conditions beyond N-1, elimination of redundancy as a determining criterion, and seeking third-party review and concurrence of the Critical Asset list.