Security Asset Management Strategy Appendix

A-1 Comparison of Risk Reduction

Executive Summary of Comparison of Risk Reduction

This document outlines the comparative risk reduction of the several security enhancement levels and tiers. It is important to understand the dynamics of the various threats noted in the tables. Reduction of risk is based on the effectiveness of a security system when compared to a given threat with given capability, intent, motive, and historical activity. Reduction of risk from a terrorist threat takes significantly greater investment in security than reduction in risk from other threats like general criminal activity and vandalism. In addition, certain types of security systems will be more effective for reducing risk from certain threats, while having practically no impact on others.

For example: The Alvey Substation 500kV Control House had received all required NERC CIP security systems yet, these systems had no impact in preventing intrusion into the energized yard wherein apparent metals theft was the motive. The resulting collateral damage of two ground mounted station service transformers, cable tread-ways and fire damage to the 500kV control house caused a prolonged outage of the 500kV California-Oregon AC intertie and nearly one million dollars in damage. The NERC CIP requirements had no risk reduction against general criminal activity.

Figure A-1.1 Collateral Damage from Attempted Metals Theft

This document supports the premises that regulatory compliance requirements will override the ability to apply a risk based decision process with respect to implementation of security strategies.

Conversely, this document supports the notion that a risk based approach to security will allow for a graded approach to implementing security strategies based on actual operational criticality of a site, business need and other factors deemed important by agency decision makers.

Beginning in 2001 BPA began to implement security improvements based on risk assessments. The improvements were developed in progressively increasing levels with greater risk reduction. This early process described security “Levels” for gradually increasing security protection.

In 2008 security protection required by NERC CIP 006 began to be implemented. Irrespective of actual risk assessment results, or risk reduction, the regulatory compliance requirements stemming from NERC CIP 006 were mandated and implemented. Due to limited financial and human resources, risk based decisions for implementing security at identified critical sites ceased, except for the risk associated with non compliance. Financial and human resources have been completely dedicated to regulatory compliance with little in the way of actual risk reduction accomplished.

In 2010 BPA began to develop a Graded Security Policy consistent with recent DOE published requirements. This policy, captured in the Critical Asset Security Plan (CASP), brings together in one comprehensive document all the various regulatory compliance requirements and the risk based approach of the Streamlined Security Risk Assessment Strategy (SSRA).

In order to facilitate a continuing risk based security assessment process to identify the effectiveness of security systems and risk reduction; in 2010 the Streamlined Security Risk Assessment Strategy was developed. Based on the RAM-T and data acquired from the preceding 10 years of risk assessment activity, the SSRA leverages the RAM-T data and the flexibility the RAM-T methodology offers.

The A-1.1 below indicates the various security system attributes of the early level one and two systems, and the more recently developed Tier 1, 2, 3, and 4 as well as the NERC CIP required systems.

Table A-1.1 Systems Insalled Under Each Protection Approach

Security Element	**No Upgrades**	**L-1** 2001	**L-2** 2004	**NERC** 2009	**T-4** 2010	**T-3** 2010	**T-2** 2010	**T-1-CC** 2010
Fences (standard Chain Link)	X				TBD			
Fully Fenced Control House (Chain Link)		X	X		TBD			
Fully Fenced with Beta Fence Including Control House					TBD	X	X	TBD
Automated Gates		X	X		TBD	X	X	X
Fence Intrusion Detection Systems			X		TBD	X	X	TBD
Control House Video Surveillance				X	TBD	X	X	X
Single Video Surveillance Camera at One Automated Gate		X	X		TBD	X	X	X
Yard Video Surveillance			X		TBD	X	X	NA
Standard Facility Lighting	X	X	X		TBD	X	X	X
Increased Security Lighting					TBD	X	X	TBD
Motion Detectors (Exterior with Video)			X		TBD	X	X	TBD
Motion Detectors (Interior)				X	TBD	X	X	
Enhanced Perimeter Detection					TBD		X	
Door Contacts				X	TBD	X	X	X
Access Control Systems				X	TBD	X	X	X
24/7 Security / Armed Security and Patrol					TBD			X
Security Screening					TBD			X
HSPD-12 Background Screening	X	X	X		TBD	X	X	X
Personnel Risk Assessments				X	TBD	X	X	X
Recurring Background Checks (7yr)				X	TBD	X	X	X
Recurring Security Training	X	X	X	X	TBD	X	X	X
Incident Reporting Policies Requirements	X	X	X	X	TBD	X	X	X

Part 1 of this document covers the estimated risk tables for substations having a maximum voltage of 525kV and in compliance with NERC CIP Versions 1-3 and Version 5, with explanations. Version 4 only

increased the number of sites requiring protection not the scope of the specific requirements. BPA identified 58 substations and 2 control centers under the requirements outlined in NERC CIP 002 Critical Cyber Asset Identification often referred to as the top 60 sites. *NOTE: The analysis below does not include the Control Center risk assessments.*

Part 2 covers sites that would be included in "NERC CIP 002 –Critical Cyber Asset Identification Version 4" (V-4).

Risk rating is calculated using the following equation:

Risk = Threat (Pa) x Consequence (c) x (1 - Security system effectiveness (Pe))

The rating scales for threat, consequence and security system effectiveness are shown in the figures below.

Figure A-1.2 Threat Assessment Scale Tool

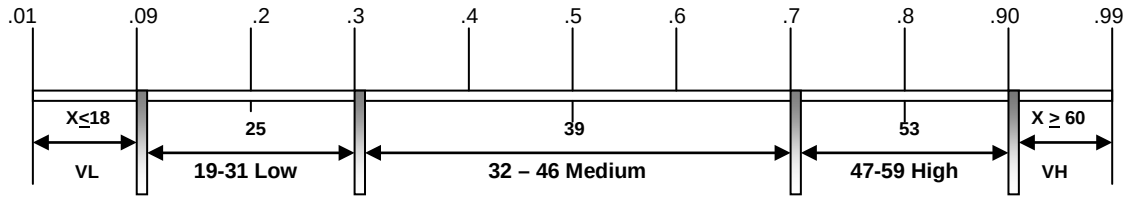
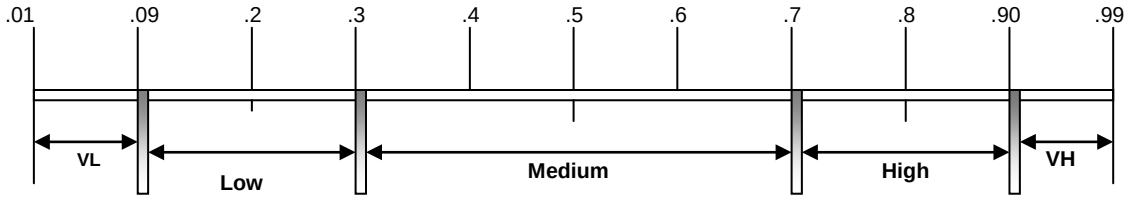


Figure A-1.3 Consequence and Security System Effectiveness Scale Tool



Part 1: Top 58 Critical Sites

As a baseline, Table A-1.2 shows an estimation of security risk according to previous conditions wherein no security enhancements had been installed. This data has been retrieved from risk assessments conducted from 2001-2008 and updated in the SSRA.

Table A-1.2 Estimated Risk for 500kV Critical Substations- No Security Enhancements

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Equation	Risk Numerical	Risk Range
International Terrorist	.5	.99	.01	.5 x .99 x(1-.01)	.49	Medium
Eco Terrorist/Special Interest	.5	.9	.01	.5 x .9 x (1-.01)	.45	Medium
Criminal Activity	.99	.5	.01	.99 x .5 x (1-.01)	.49	Medium
Vandal	.9	.5	.01	.9 x .5 x (1-.01)	.45	Medium
Insider	.5	.5	.1	.5 x .5 x (1-.1)	.23	Low

Table A-1.3 represents an estimation of risk based on minimum security enhancements referred to as Level One Enhancements. Level One Enhancements included extending the substation chain link fence line to include completely enclosing the Control House, one automated vehicle gate with card key reader and one video camera at the vehicle gate. These enhancements were intended to provide a simple baseline level of security for all BPA sites of significant importance including maintenance headquarters.

It was understood at the time that there would be relatively little in the way of risk reduction, particularly for higher level threats such as terrorist groups. This table is not expressed in the Streamlined Security Risk Assessment Strategy (SSRA) because at the time the SSRA was developed; all sites with Level One Enhancements had received or were scheduled to receive the required NERC CIP security systems up to CIP 006 Version 3.

Table A-1.3 Estimated Risk for 500kV Critical Substations- Level One Enhancements Only

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Equation	Risk Numerical	Risk Range
International Terrorist	.5	.99	.01	.5 x .99 x (1-.01)	.49	Medium
Eco Terrorist/Special Interest	.5	.9	.01	.5 x .9 x (1-.01)	.45	Medium
Criminal Activity	.99	.5	.1	.99 x .5 x (1-.1)	.45	Medium
Vandal	.9	.5	.1	.9 x .5 x (1-.1)	.4	Medium
Insider	.5	.5	.1	.5 x .5 x (1-.1)	.23	Low

Table A-1.4 is derived directly from the SSRA. This table reflects that the only adversary group impacted by the NERC CIP 006 security requirements was the insider threat. NERC CIP systems up to Version 3 would have no impact on highly capable, motivated adversaries. Despite the erroneous assumption by some, that the NERC CIP security requirements would impact terrorists, and motivated criminals, the systems are not capable of impeding the activities commonly associated with those threats. BPA as an agency generally enjoyed a relatively low level of insider threat. NERC CIP security requirements tend to leverage the HSPD 12 requirements as well as the internal substation operations policies for authorized unescorted access to energized facilities. Therefore, we see a significant reduction is the insider threat while other "outsider" threats remain relatively unaffected by the investment in these systems. However, the implementation of the NERC CIP systems provides detection and monitoring capability. These benefits are difficult to quantify without a response capability sufficient to interrupt the undesired event. We now have detection and response capability that includes notifying police and Transmission Dispatch but the ability to quantify that response cannot be accurately quantified. These types of benefits are often referred to as "Intangible Benefits." *These systems are not capable of stopping determined adversaries, but an analyst may choose to estimate an increase in Security System Effectiveness in very small increments not likely to result in a significant risk reduction.*

Table A-1.4 Estimated Risk for 500kV Substations having Level One and NERC CIP Security systems up to CIP 006 Version 3.

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Equation	Risk Numerical	Risk Range
International Terrorist	.5	.99	.01	.5 x .99 x (1-.01)	.49	Medium
Eco Terrorist/Special Interest	.5	.9	.01	.5 x .9 x (1-.01)	.45	Medium
Criminal Activity	.99	.5	.1	.99 x .5 x (1-.1)	.45	Medium
Vandal	.9	.5	.1	.9 x .5 x (1-.1)	.4	Medium
Insider	.5	.5	.5	.5 x .5 x (1-.5)	.13	Low

NERC CIP 006-5 (V-5) requires that any opening of 96 square inches or greater with one dimension of 6 inches or greater be protected from physical entry by using barriers, bars, steel screens or other means. Analysis of the actual physical protection properties of these materials used to cover openings of 96 square inches clearly indicates there are no actual physical protection benefits for these types of openings.

These types of openings are typically covered with windows, bug screens, louvers and other common devices.

Under the new version, windows, HVAC vents, and other common openings will require the addition of the described barriers.

Comprehensive Threat Analysis including the analysis of threat capability, intent and attack methods indicates the V-5 recommendation for securing openings of 96 square inches is either completely ineffective or completely inappropriate or both. BPA risk analysis over the last 12 years has yielded no information to suggest openings of 96 square inches have ever been, or will ever be exploited. To the contrary, in all instances of substation burglary, the burglar has used common entries such as doors. There are no records of burglary at BPA through the use of a small opening such as the size described in the standard.

Therefore, there is no reasonable basis to assign a risk reduction by virtue of a security system effectiveness increase resulting from the assumed implementation of NERC CIP 006 Version 5. Table A-1.5 remains unchanged from the Table A-1.4 reflecting Level One and NERC CIP 006 Versions 1-3. Sites identified as NERC CIP sites are equipped with intrusion detections systems for all areas that could be used as an access point at the control houses and relay houses including access tunnels and all windows.

Table A-1.5 Estimated Risk Reduction for 500kV sites assuming Level One, NERC CIP Version 1-3, and Version 5 as it applies to these sites

Note: *NERC CIP 002-4 (V-4) deals with broadening the criteria "Critical Assets" are defined by and will include many 230-115kV and below substations. The scope of the actual protective requirements was not affected by V-4. Therefore the table below does not reflect changes in risk from the implementation of V-4.*

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Equation	Risk Numerical	Risk Range
International Terrorist	.5	.99	.01	.5 x .99 x (1-.01)	.49	Medium
Eco Terrorist/Special Interest	.5	.9	.01	.5 x .9 x (1-.01)	.45	Medium
Criminal Activity	.99	.5	.1	.99 x .5 x (1-.1)	.45	Medium
Vandal	.9	.5	.1	.9 x .5 x (1-.1)	.4	Medium
Insider	.5	.5	.5	.5 x .5 x (1-.5)	.13	Low

Tier 2 security improvements include: penetration resistant "Beta" fence with integrated fence intrusion detection system, security lighting with outward pointing high intensity motion sensor activated lighting and Infra-red video surveillance systems. The entire perimeter including the control house is fenced with automated card key operated vehicle gates.

Table A-1.6 represents a modest increase in security system effectiveness against highly motivated and capable adversaries such as international terrorist groups and a significant increase in effectiveness against burglary, theft, and vandalism.

The Tier 2 security system provides a sophisticated level of surveillance and detection giving BPA the opportunity to leverage early warning information of unauthorized or criminal activity. Table A-1.6 does not represent the full potential of risk reduction at this time.

To fully realize the potential risk reduction of Tier 2 security systems, a robust response plan capable of interrupting, stopping or mitigating the attack is necessary.

Table A-1.6 Estimated Risk Reduction for 500kV site with Tier 2 and NERC CIP 006 Versions 1-3.

Note: *NERC CIP 002-4 (V-4) deals with broadening the criteria "Critical Assets" are defined by and will include many 230-115kV and below substations. The scope of the actual protective requirements was not affected by V-4. Therefore the table below does not reflect changes in risk from the implementation of V-4. CIP 006 Version 5 risk reduction is null as previously indicated in Table 4.*

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Equation	Risk Numerical	Risk Range
International Terrorist	.5	.99	.15	.5 x .99 x (1-.15)	.42	Medium
Eco Terrorist/Special Interest	.5	.9	.2	.5 x .9 x (1-.2)	.36	Medium
Criminal Activity	.9	.5	.55	.9 x .5 x (1-.55)	.2	Low
Vandal	.8	.5	.55	.9 x .5 x (1-.55)	.18	Low
Insider	.5	.5	.5	.5 x .5 x (1-.5)	.13	Low

Part 2 – CIP Version 4 Defined Critical Sites

Part 2 covers the estimated risk tables for Sites impacted by the requirements found in NERC CIP 002 Version 4 Identification of Critical Cyber Assets. For sites impacted by this version such as those sites having a maximum voltage of 230kV, the same rational for an absence of risk reduction if Version 5 were to be implemented applies.

The sites represented by this section are consistent with the sites on the Priority Pathway list, ranging from site number 68-167. The RAM-T ranking process resulted in significantly lower scores based on impacts to National Security, Economic Security, Public Health and Safety, Generation and overall Grid Reliability. These sites scored between 7 and 10 points out of a possible 15, with only 4 of the 29 sites scoring 10 points. Unlike the top 60 substations on the Priority Pathways list having maximum voltage of 525kv and being considered as the most operationally critical substations; the sites in this section are somewhat less critical based on the data provided in the Priority Pathway list, the RAM-T rankings, and by having up to 230kV.

Table A-1.7 represents an initial estimation of consequence values somewhat less than the consequence values found in the top 60 substations. Often, the target desirability changes with criticality and consequence. The screening criteria required by NERC CIP 002 Version 4, to identify Critical Cyber Assets may not have otherwise been applied to these sites, absent being a NERC requirement.

Without adequate consequence results from an attack or intrusion, an adversary may choose to conserve resources in order to execute an action at a more critical target. The security systems associated with this table are insufficient to deter a determined, capable and prepared adversary.

Table A-1.7 Estimated Risk for NERC CIP 002 Version 4 sites under current conditions (no security systems)

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Equation	Risk Numerical	Risk Range
International Terrorist	.5	.8	.01	.5 x .8 x (1-.01)	.4	Medium
Eco Terrorist/Special Interest	.5	.75	.01	.5 x .75 x (1-.01)	.37	Medium
Criminal Activity	.99	.4	.01	.99 x .4 x (1-.01)	.39	Medium
Vandal	.9	.4	.01	.9 x .4 x (1-.01)	.36	Medium

Insider	.5	.5	.1	.5 x .5 x (1-.1)	.23	Low

Level One Enhancements included extending the substation chain link fence line to include completely enclosing the Control House, one automated vehicle gate with card key reader and one video camera at the vehicle gate. These enhancements were intended to provide a simple baseline level of security for all BPA sites of significant importance including maintenance headquarters. It was understood at the time there would be relatively little in the way of risk reduction, particularly for higher level threats such as terrorist groups. It is unlikely that the sites identified as a result of version 4 would have otherwise received security enhancement absent a site specific need.

Table A-1.8 Estimated Risk for NERC CIP 006 Version 4 identified sites with Level One Security Systems only.

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Equation	Risk Numerical	Risk Range
International Terrorist	.5	.8	.01	.5 x .8 x (1-.01)	.4	Medium
Eco Terrorist/Special Interest	.5	.75	.01	.5 x .75 x (1-.01)	.37	Medium
Criminal Activity	.99	.4	.1	.99 x .4 x (1-.1)	.35	Medium
Vandal	.9	.4	.1	.9 x .4 x (1-.1)	.32	Medium
Insider	.5	.5	.1	.5 x .5 x (1-.1)	.23	Low

With the NERC CIP Versions 1-3 and Level One security systems installed, the decrease in Insider risk is reduced. This is consistent with the risk analysis and threat analysis of previous risk assessments and the Streamlined Security Risk Assessment Strategy (SSRA). The Version 1-3 requirements would not deter a determined adversary therefore there is no reduction for other adversary groups. It is unlikely that the sites identified as a result of version 4 would have otherwise been considered to receive security enhancement absent a site specific need.

Table A-1.9 Estimated Risk for NERC CIP 006 Version 4 identified sites with Level One and NERC CIP 006 Versions 1-3 Security Systems

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Equation	Risk Numerical	Risk Range
International Terrorist	.5	.8	.01	.5 x .8 x(1-.01)	.4	Medium
Eco Terrorist/Special Interest	.5	.75	.01	.5 x .75 x (1-.01)	.37	Medium
Criminal Activity	.99	.4	.1	.99 x .4 x (1-.1)	.35	Medium
Vandal	.9	.4	.1	.9 x .4 x (1-.1)	.32	Medium
Insider	.5	.5	.5	.5 x .5 x(1-.5)	.13	Low

A-2. Additional 25% Capital Reduction

An alternate implementation schedule has been developed to assess the impact of an additional 25 percent reduction from base funded amount[1]. Achieving the 25 percent requires:

- Extension of the implementation schedule for Tier 2 sites by four years.
- Delaying protection of critical Tier 3 and essential Tier 4 sites by as much as a decade.
- Foregoing capitalization of large-scale system updates as recommended in section 3.3.3 resulting in an increase in the expense budget by over $2 million dollars.

This type of a cut would expose BPA to risks that would be mitigated by the strategic initiatives 1 to 3 as documented in Table 1, as well as the Agency Level Risks identified in Table 6. The asset management objectives of compliance and protection would be severely compromised.

Table A-1. Capital Cost Projection with Additional 25% Reduction ($000s) (ALTERNATIVE)

FY	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
Base Capital Budget	4,190	4,948	4,947	4,942	5,700	5,699	6,232	5,443	5,445	5,436	52,982
Additional 25%	3,143	3,711	3,710	3,707	4,275	4,274	4,674	4,082	4,084	4,077	39,737
Tier 2 Critical Site Protection	2,900	-	-	-	-	1,412	4,674	4,082	4,084	4,077	**21,229**
Tier 3 Critical Site Protection	-	-	-	-	-	-	-	-	-	-	-
NERC CIP Version 2 & 3 at 17 sites	450	-	-	-	-	-	-	-	-	-	**450**
NERC CIP Version 2 & 3 at 36 sites	-	1,640	-	-	-	-	-	-	-	-	**1,640**
NERC CIP Version 4 at 33 sites	-	2,071	2,054		-	-	-	-	-	-	**4,125**
NERC CIP Version 5*	-	-	1,656	3,707	4,275	2,862	-	-	-	-	**12,500**
Non-Transmission & Tier 4 Sites Protection	-	-	-	-	-		-	-	-	-	-
Capital update of failing systems	-	-	-	-	-	-	-	-	-	-	-
TOTAL CAPITAL	**3,350**	**3,711**	**3,710**	**3,707**	**4,275**	**4,274**	**4,674**	**4,082**	**4,084**	**4,077**	**39,944**
Delta (75% budget vs. estimate)	-207	0	0	0	0	0	0	0	0	0	-207

[1] Base amount includes an already applied 10% reduction + 15% lapsed factor