SECURITY ASSET MANAGEMENT STRATEGY

FY2014 - 2023

DRAFT

This asset strategy was prepared before BPA's proposal to reduce costs. Spending levels in this document may not tie to proposed reductions. The strategy will be revised upon conclusion of the CIR and the IPR.

Z. SHAHUMYAN

FEBRUARY 2014

TABLE OF CONTENTS

Executive Summary 3
Overarching Strategy 10
1. Asset Management Goals, Objectives, Initiatives and Risks 11
1.1 Goals 11
1.2 Objectives 11
1.3 Strategic Initiatives 12
1.4 Work Prioritization 13
1.5 Strategic Challenges 14
2. Asset Category Overview 15
2.1 Definition 15
2.2 Primary Asset Types and Groupings 15
2.3 Service Provided 17
2.4 Criticality Rating 17
2.5 Roles and Responsibilities 18
2.6 Metrics 20
3. Capital Investment Recommendations 21
3.1 NERC CIP Version 1 through 5 Compliance Enhancements 21
3.2 Protection of Tier 1 Sites 22
3.3 Protection of Tier 2 Sites 23
3.4 Protection of Tier 3 Sites 23
3.5 Other Essential Infrastructure Protection 24
3.6 Other Considerations 24
4. Investment Recommendations - Expense 25
4.1 Performance Testing & Preventative Maintenance – Initiative 4 25
4.2 Replacement and Renewal Program – Initiative 5 27
4.2.1 Deployment of New Standard 27
4.2.2 Replacement Upon Failure 28
4.2.3 Maintaining Tier 2 Site Enhancements 28
5. Summary of Recommended Investments 29
5.1 Proposed Capital Plan for FY2014 – FY2023 29
5.2 Proposed Expense Plan for FY 2014 - FY 2023 29
Appendix A - Risk Reduction 31

EXECUTIVE SUMMARY

The Office of Security and Continuity of Operation (OSCO) is accountable for supporting Bonneville Power Administration's (BPA) mission and stakeholder interests by protecting BPA's people, facilities critical systems and information. The program scope covers more than 300 facilities, over 5,000 employees and contractors, as well as thousands of visitors each year. Security system designs and standards ensure BPA is compliant with regulatory requirements, guidelines, provisions and principles prescribed by the North American Electric Reliability Corporation (NERC), Federal Energy Regulatory Commission (FERC), U.S. Department of Energy (DOE), and U.S. Department of Homeland Security (DHS) as outlined in Presidential Decision Directives.

There are two fundamental changes from the previous strategy pertaining to:

1. the order of implementing security upgrades at critical sites, and
2. the strategy for managing failing and obsolete security infrastructure.

Due to the unpredictable nature of threat activity and resulting security conditions, the prioritization scheme must allow for flexibility to maneuver in an environment where security conditions can change with little advanced warning, while also ensuring an adequate baseline level of security commensurate with criticality.

Our previous method for prioritizing work simply based on relative criticality of the site may not be the best approach under all circumstances because security risk is influenced by several other factors including threat information and security system or mitigating strategies. For example, while a given site may have a greater consequence resulting from malevolent acts, another potentially less critical site that is experiencing a high level of criminal activity may be at a greater "risk" of loss, thereby warranting an earlier or greater investment in security infrastructure.

The former strategy of actively replacing obsolete system components on a scheduled basis is not practical or feasible in the long term because the supporting infrastructure will need to be upgraded to support new technology. BPA is proposing a new way forward to address this challenge by developing a protection design standard which leverages new technology and can be sustained over the long term.

Profile of Assets

The purpose of security assets is to implement BPA requirements for protection and compliance. BPA defines a *security asset* as material, equipment, software or hardware that is used for the primary purpose of providing protection. Individual assets or components make up security systems that collectively provide various levels of physical security protection depending on the asset being protected. Table "A", on the following page, outlines the systems, their purpose, and provides examples of the types of components included in each system.

Table A - Systems and Component Overview

Systems	Purpose	Asset Types Include	
Protective Barrier	Provide a physical barrier between adversary and target. Protective barriers delay an adversary's attempts to gain entry or cause damage to critical components.	• Fence • Gate • Padlock • Bollards	• Chains • Barbed wire • Door • Reinforced glass
Intrusion Detection	Provide warning of pending intrusion and notification of an intrusion by unauthorized people.	• Motion detectors • Fence detection systems • Glass break sensors	• Motion sensing cameras
Surveillance	Video surveillance systems allow for the real- time viewing of activity as well as the ability to review activity in the past. Used in support of detection systems in order to asses alarm annunciations.	• Fixed cameras • PTZ cameras • DVR/NVR • Thermal imaging devices	• Mounting structures, hardware, wiring, and circuitry
Lighting	Lighting used specifically to address a security need, whether to support low light camera operation or to illuminate an area of security concern, would be considered security lighting.	• Entrance or gates • Camera lights • Perimeter lights	• Special area lights
Early Intrusion Detection	Provide the capability to detect activity outside the perimeter of the facility and provide early warning of potentially malevolent activity.	• Motion/Thermal detection surveillance devices	
Screening	Ensure that contraband, such as weapons, firearms, and controlled substances, are not brought into BPA facilities.	• X-ray machines	• Metal detectors

Objectives of this Strategy

OSCO's strategic goals of *compliance* and *protection* will be achieved by meeting the following strategic objectives:

1. Prioritize and fund security gaps in protection standards set by BPA's ***Critical Asset Security Plan (CASP)***. The CASP integrates risk-based protection strategies in accordance with DOE's Graded Security Policy (GSP) and compliance driven security standards for NERC CIP and HSPD compliance, into a comprehensive protection approach. Protection standards are defined and grouped by facility's criticality level or tier, where Tier 1 is most critical.

2. Forecast, prioritize and fund system maintenance activities which are economical, sustainable, risk informed and ensure reliable system performance. In accordance with DOE O 473.3, the maintenance standards are informed by **System Performance Assurance, Component Testing and Preventative Maintenance Program *(SPAP)***. The SPAP requires that BPAs security systems are tested and maintained on a regular basis, with corrective maintenance addressed commensurate with the level of criticality and location of the system.

Outside the scope of this strategy are:

- Cyber security systems
- IT infrastructure (networks, servers, etc.) used to operate the digital security components
- Administration, maintenance, and cyber security of the software solution used to carry the video and alarm data feed
- Ongoing security fence maintenance is supported by Facilities Asset Management

OSCO coordinates with Information Technology and Facilities to ensure that these, and related requirements, are addressed in the appropriate asset management plans.

Strategic Challenges

There are two strategic challenges which are actively being addressed starting in FY14.

Rapidly evolving regulatory requirements

Critical Infrastructure Protection (CIP) requirements issued by NERC CIP have had a major impact on BPA's security program, both in terms of resourcing as well as developing processes for successful implementation. NERC requirements emerge every one to two years requiring implementation within 12 to 18 months. It is difficult to anticipate the scope and budget for NERC projects in advance. Standard BPA processes for capital projects require a least a two to three year planning window which does not accommodate NERC timelines. Furthermore, NERC CIP impacts several BPA organizations with complex interdependencies and upstream/downstream impacts.

To address these challenges, BPA is developing an all stakeholder inclusive process for managing NERC CIP related and other security project work. BPA is looking to transition security capital program management to the appropriate organizational structure within BPA. This allows physical security resources to focus on NERC and other physical security activities related to assessment, standards development, implementation, training, performance testing and security threat management.

Aging and technologically obsolete systems

Large number of systems (primarily cameras) are projected to fail in the next few years due to exceeding manufacturer recommended Mean Time to Failure (MTTF). If not managed, this may impact security system effectiveness, cause a spike in maintenance fees and drain on limited resources.

The former strategy of actively replacing obsolete system components on a scheduled basis is not practical or feasible in the long term because the supporting infrastructure will need to be upgraded to support new technologies. Additionally, BPA security subject matter experts believe that the large number of cameras currently deployed is not providing a security risk reduction benefit commensurate to the level of investment and long term costs associated with reliable sustainability. BPA's OSCO is proposing a protection design standards which leverages new technology that can be sustained over the long term. The benefits to this approach are:

- Immediate reduction in costs associated with video surveillance maintenance
- Reduction in information technology band width and licensing costs
- Ability to redirect resources to more sustainable security system's development and implementation
- Maintaining "security in depth" and multi-layered alarm assessment capability

BPA implements a layered security approach that includes all aspects of the physical security, personnel security, information security and operations security disciplines. Video surveillance is almost exclusively used to assess alarm activity after the fact. This has traditionally been one of two primary assessment tools to determine the nature of an alarm. The proposed strategy uses other less costly more sustainable technology to provide assessment capability in depth. Therefore the decommissioning of significant video

surveillance assets at substations is expected to have very minimal to no impact of security system effectiveness or assessment capability.

Major Elements of the Strategy

Prioritization

When prioritizing, several factors are considered:

- Real-time security threat information, including increased rates of incidents
- Regulatory mandates
- The criticality of the facility as measured by the impact of its loss on BPA's ability to achieve its mission
- Criticality of a system or components based on its failure on maintaining security compliance and security system effectiveness
- Efficiencies to be gained by coupling the project with other work at the site

Table "B" shows the priority matrix used to resource and schedule investments during initial enhancements as well as future maintenance.

Table B - Priority Matrix

Priority Level	*Description*
Priority 1	Immediate threat mitigation in response to an event or change in threat conditions which may or may not be based on tier designation
Priority 2	Tier 1, 2, and 3 protection according to regulatory compliance requirements and by a graded security approach
Priority 3	Protection of both energy and non-energy facilities based on improving or enhancing security conditions using federal facility protection guidelines and standards provided by DOE, General Services Administration (GSA) etc. and risk informed protection strategies to address security threats and gain efficiencies.

Strategic initiatives

Five initiatives have been identified for meeting the strategic objectives and reducing variety of security and operational risks. Table "C", on the next page, summarizes each initiative and provides the risk exposure from forgoing or delaying implementation.

Table C - Strategic Initiatives, Risks and Costs

Drivers	Initiatives	Risks of Foregoing Implementation	10 Year Cost Capital / Expense	
BPA Critical Asset Security Plan (CASP)	**1. Compliance** Ensure compliance with security regulation by applying mandatory security enhancements as required by NERC, DHS, DOE, etc.	**Financial and Reputational Risk Due to Regulatory Non-Compliance:** Findings by regulatory entities within one year leading to; a) possible financial sanctions, b) mandated policy changes and, c) public criticism.	$8.7 M	
	2. Critical Infrastructure Protection in Support of GSP Installation of security systems designed to provide the appropriate level of protection for critical infrastructure with a Tier 1[1], Tier 2 or Tier 3 criticality level designation.	**Financial and Operational Risk Due to Terrorist/Criminal Activity:** Continual exposure to "medium risk[2]" of terrorist attack or collateral damage from criminal activity which could result in the loss of critical transmission facilities with; a) an extreme consequence to the bulk electric system, b) major economic impact to regional customers and economy and, c) severe observable impact and orders for substantial corrective action, including some mandatory changes in BPA operation or administration.	$37.1 M	
	3. Essential Infrastructure Protection Improving or enhancing security systems at essential sites using federal facility protection guidelines and standards provided by DOE, GSA etc. and risk informed protection strategies to address security threats and gain efficiencies.	**Financial and Operational Risk Due to Criminal Activity:** a) Increased exposure to criminal activity and potential collateral damage impacting Bulk Electrical System (BES), b) inability to replace or update obsolete security systems compromising protection of essential facilities such as the headquarter building, c) using more costly guard force contract labor to protect facilities as opposed to automated systems which cost less over time and provide equal or greater level of protection.	$1.5 M	
BPA System Performance Assurance, Testing and Preventative Maintenance Program (SPAP)	**4. Performance Testing & Preventative Maintenance** Bi-annual assessment of security systems through performance tests leading to repair or replacement of components that may impact security system reliability or compliance.	**Financial and Reputational Risk Due to Inadequate Maintenance:** Lack of awareness of failing or faulty security systems and equipment leading to; a) compromised protection of critical infrastructure, b) strain on limited resources to support urgent vendor callouts, c) non-compliance with DOE order 473.3 and, d) criticism by regulatory entities due to unplanned outages of critical security systems.		$0.5 M
	5. Replacement & Renewal Program Timely replacement of failed components commensurate with criticality of system to maintain compliance and provide protection. Strategic phase-out of components no longer technological viable.	**Operational and Reputational Risk Due to Inadequate Maintenance:** Failing or faulty security systems and equipment leading to; a) compromised protection of critical infrastructure, b) strain on limited resources to support O&M activity and, c) criticism by regulatory entities due to unplanned outages of critical security systems.		$6.0 M
		TOTAL	**$47.3M**	**$6.9M**

[1] Tier designation of level of criticality of the site is based on DOE's graded security policy where Tier 1 is most critical and Tier 4 is essential and may or may not be an electrical facility.

[2] DHS and other federal national security resources have assessed critical national infrastructure assets, including high voltage transmission facilities such as BPAs, at "Medium Risk" of terrorist attack; meaning there is credible information suggesting sites such as these are of interest to both international and domestic terrorist groups.

Results to be Achieved

BPA and its stakeholders can expect ongoing compliance with requirements, improved critical site protection, and reliable security system performance.

Compliance

Success in maintaining security compliance will be measured by BPA having zero violations of a NERC requirement as a result of lacking security systems or underperformance of existing systems. Violations count only when not previously self-reported and assigned a low to moderate Violation Risk Factor (VRF) and Violation Security Level (VSL) as identified by a regulatory audit or investigation.

Protection

By the end of 2017 five additional Tier 2 critical substations will have security enhancements installed, which will result in a notable reduction in risk. Table "D" shows the estimated risk reduction to be gained as a result of the proposed implementation.

Table D - Estimated Security Risk Impact - Tier 2 Protection

	Before[3] Tier 2 Treatment		After Tier 2 Treatment		
Threat	**Risk Numerical**	**Risk Range**	**Risk Numerical**	**Risk Range**	**% Risk Reduction**
International Terrorist	0.49	Medium	0.42	Medium	**7%**
Eco Terrorist / Special Interest	0.45	Medium	0.36	Medium	**9%**
Criminal Activity	0.45	Medium	0.2	Low	**25%**
Vandal	0.4	Medium	0.18	Low	**22%**
Insider	0.13	Low	0.13	Low	**0%**

Additionally, three Tier 3 critical substations will be protected with required security measures with notable reduction in security incidents.

Security system reliability

New design standards will be defined and incorporated into a long-rage implementation plan. It is believed that a large number of outdated cameras can be decommissioned with minimal to no impact to security system effectiveness and reduce maintenance overhead in the long run. Furthermore, efficiencies may be gained by coupling security work with Facilities Asset Management (FAM) projects.

Spending Levels

Proposed capital plan for FY 2014 - FY 2023

BPA's OSCO is proposing a capital model which funds:

- NERC CIP required protection with place holder funding beyond the current NERC CIP version at $500,000 per year starting in FY16
- Graded security and critical infrastructure protection at Tier 1, 2 and 3 sites
- Anticipated work in the future for essential infrastructure protection such as headquarter building

[3] *The "Before" state assumes Level 1 and NERC CIP systems up to CIP 006 Version 3.*

Table E - Proposed Capital Plan ($000s)

FY	2012 Actual	2013 Actual	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total FY14-23
Immediate Threat Mitigation	-	-	-	-	-	-	-	-	-	-	-	-	-
Regulatory Compliance	482	2,290	3,197	1,500	500	500	500	500	500	500	500	500	8,697
Tier 1 Critical Site Protection	-	351	304	-	-	-	-	-	-	-	-	-	304
Tier 2 Critical Site Protection	2,923	133	-	6,661	3,033	7,070	5,517	7,307	4,131	-	-	-	33,719
Tier 3 Critical Site Protection	-	-	-	250	2,850	-	-	-	-	-	-	-	3,100
Essential Facilities	-	534	-	-	-		-	-	-	500	500	500	1,500
TOTAL CAPITAL	**3,405**	**3,309**	**3,501**	**8,411**	**6,383**	**7,570**	**6,017**	**7,807**	**4,631**	**1,000**	**1,000**	**1,000**	**47,320**

Proposed expense plan for FY 2014 - FY 2023

BPA's security maintenance strategy has shifted from individual component maintenance and upgrade to a more holistic approach of upgrading the entire security infrastructure at a site based on a new standard. The maintenance and update activities are funded from two sources. Security systems at transmission sites are funded by Transmission Field (TF) budget, while systems installed at headquarter building are paid for out of the corporate cost center. The proposed spending level for each category is outlined in Table "F".

Table F - Expense Plan for Security System Maintenance from FY 2014–FY 2023 ($000s)

FY	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Transmission Funds										
Performance Testing & Maintenance	41	42	44	45	46	48	49	51	52	459
Replacement Upon Failure	218	220	223	225	227	229	232	234	236	2,260
New Standard Deployment	476	407	323	337	321	248	238	145	112	2,892
Tier 2 Maintenance	5	10	40	80	95	195	205	220	250	1,100
Trans. Sub-Total	**740**	**680**	**630**	**687**	**689**	**720**	**723**	**650**	**650**	**6,710**
Corporate Funds										
Performance Testing & Maintenance	7	7	8	8	8	8	9	9	9	80
Replacement Upon Failure	11	12	12	13	13	14	15	15	15	131
Corp. Sub-Total	**18**	**19**	**20**	**21**	**21**	**22**	**24**	**24**	**24**	**211**
TOTAL	**758**	**699**	**649**	**708**	**711**	**743**	**747**	**674**	**674**	**6,922**

Summary

The security asset management strategy seeks to balance compliance and graded protection initiatives to provide BPA with the most risk appropriate security, applying sound asset management principles and efficiencies to minimize costs and maximize the use of rate payer dollars. Process improvements and new design standards are the highlights of the current approach and will set the direction for the next decade.

SECURITY ASSET MANAGEMENT OVERARCHING STRATEGY

1. Asset Management Goals, Objectives, Initiatives and Risks

1.1 Goals

The goal of the Security Infrastructure Asset Management Strategy is to establish a prioritization strategy for both initial security system deployment and subsequent life-cycle maintenance to address the ever changing security threats and compliance requirements, while balancing sound business and asset management principles, ensuring the following long-term outcomes:

- ***Compliance*** – BPA is in compliance with all security requirements (e.g., NERC CIP, HSPD-12, DOE's Graded Security Policy (GSP)).
- ***Risk Informed Protection*** – Protection strategies consider risks as measured by existing threat and potential consequence of impact to BPA's people, mission, and fiscal health while also considering mitigating strategies such as security systems, policy and employee awareness training.

1.2 Objectives

OSCO's strategic goals of *compliance* and *protection* will be achieved by meeting the following strategic objectives:

1. Prioritize and fund security gaps in protection standards set by BPA's ***Critical Asset Security Plan (CASP)*****.** The CASP integrates risk-based protection strategies in accordance with DOE's Graded Security Policy (GSP) and compliance driven security standards for NERC CIP and HSPD compliance, into a comprehensive protection approach. Protection standards are defined and grouped by facility's criticality level, or tier, where Tier 1 is most critical.

2. Forecast, prioritize and fund system maintenance activities which are economical, sustainable, risk informed and ensure reliable system performance. In accordance with DOE O 473.3 the maintenance standards are informed by **System Performance Assurance, Component Testing and Preventative Maintenance Program *(SPAP)***. The SPAP requires that BPA's security systems are tested and maintained on a regular basis, with corrective maintenance addressed commensurate with the level of criticality and location of the system.

Methodologies used to deploy initial installation and subsequent maintenance activities seek to:

- Leverage new technologies to sustain or enhance current system effectiveness
- Improve security system reliability
- Reduce maintenance overhead
- Promote sustainability
- Minimize impact on the environment

These objectives align with BPA's strategic direction in the following ways:

- *Strategic Objective S1 – Policy & Regional Actions*: Protecting BPA's critical transmission assets supports system reliability
- *Strategic Objective S9 – Stakeholder Satisfaction*: Customers expect BPA to protect its critical transmission infrastructure
- *Strategic Objective I4 – Asset Management*: BPA's valued assets and property are protected from loss or damage
- *Strategic Initiative I7 – Risk-Informed Decision Making & Transparency*: This protection strategy utilizes a risk informed process to prioritize the protection of critical assets
- *Strategic Initiative P4 – Positive Work Environment*: Protection of employees supports safety in the workplace

Outside the scope of this strategy are cyber security systems and the underlying IT infrastructure (networks, servers, etc.) used to operate the digital and remaining analog security components. Administration, maintenance, and security of the software solutions used to support the video and alarm data are covered by IT as well. Security fence maintenance is covered by Facilities Asset Management. OSCO coordinates with IT and Facilities to ensure that out of scope requirements are covered in the appropriate asset management plans.

1.3 Strategic Initiatives

Strategic initiatives to meet the asset management objectives are identified in Table 1, located on this and the following pages. It describes each initiative and identifies risks being mitigated by implementation.

Table 1. Strategic Initiatives, Risks Addressed and Costs

Drivers	Initiatives	Risks Mitigated by Initiative	10 Year Cost Capital / Expense	
BPA Critical Asset Security Plan (CASP)	**1. Compliance** Ensure compliance with security regulation by applying mandatory security enhancements as required by NERC, DHS, DOE, etc.	**Financial and Reputational Risk Due to Regulatory Non-Compliance:** Findings by regulatory entities within one year leading to; a) possible financial sanctions, b) mandated policy changes and, c) public criticism.	$8.7 M	
	2. Critical Infrastructure Protection in Support of GSP Installation of security systems designed to provide the appropriate level of protection for critical infrastructure with a Tier 1[4], Tier 2 or Tier 3 criticality level designation.	**Financial and Operational Risk Due to Terrorist/Criminal Activity:** Continual exposure to "medium risk[5]" of terrorist attack or collateral damage from criminal activity which could result in the loss of critical transmission facilities with; a) an extreme consequence to the bulk electric system, b) major economic impact to regional customers and economy and, c) severe observable impact and orders for substantial corrective action, including some mandatory changes in BPA operation or administration.	$37.1 M	
	3. Essential Infrastructure Protection Improving or enhancing security systems at essential sites using federal facility protection guidelines and standards provided by DOE, GSA etc. and risk informed protection strategies to address security threats and gain efficiencies.	**Financial and Operational Risk Due to Criminal Activity:** a) Increased exposure to criminal activity and potential collateral damage impacting Bulk Electrical System (BES), b) inability to replace or update obsolete security systems compromising protection of essential facilities such as the headquarter building, c) using more costly guard force contract labor to protect facilities as opposed to automated systems which cost less over time and provide equal or greater level of protection.	$1.5 M	

[4] Tier designation of level of criticality of the site is based on DOE's graded security policy where Tier 1 is most critical and Tier 4 is essential and may or may not be an electrical facility.

[5] DHS and other federal national security resources have assessed critical national infrastructure assets, including high voltage transmission facilities such as BPAs, at "Medium Risk" of terrorist attack; meaning there is credible information suggesting sites such as these are of interest to both international and domestic terrorist groups.

BPA System Performance Assurance, Testing and Preventative Maintenance Program (SPAP)	**4. Performance Testing & Preventative Maintenance** Bi-annual assessment of security systems through performance tests leading to repair or replacement of components that may impact security system reliability or compliance.	**Financial and Reputational Risk Due to Inadequate Maintenance:** Lack of awareness of failing or faulty security systems and equipment leading to; a) compromised protection of critical infrastructure, b) strain on limited resources to support urgent vendor callouts, c) non-compliance with DOE order 473.3 and, d) criticism by regulatory entities due to unplanned outages of critical security systems.		$0.5 M
	5. Replacement & Renewal Program Timely replacement of failed components commensurate with criticality of system to maintain compliance and provide protection. Strategic phase-out of components no longer technological viable.	**Operational and Reputational Risk Due to Inadequate Maintenance:** Failing or faulty security systems and equipment leading to; a) compromised protection of critical infrastructure, b) strain on limited resources to support O&M activity and, c) criticism by regulatory entities due to unplanned outages of critical security systems.		$6.0 M
		TOTAL	**$47.3M**	**$6.9M**

1.4 Work Prioritization

Due to the unpredictable nature of threat activity and resulting security conditions; the prioritization scheme must allow for flexibility to maneuver in an environment where: a) security conditions can change with little advanced warning and b) ensures an adequate baseline level of security commensurate with criticality.

Prioritizing simply based on relative criticality of the site (tier level) may not be the best approach under all circumstances because security risk is influenced by several other factors including threat information and security system or mitigating strategies. For example, while a Tier 1 or 2 site may have a greater consequence resulting from malevolent acts, a Tier 3 or 4 site that is experiencing a high level of criminal activity may be at a greater “Risk” of loss thereby warranting an earlier or greater investment in security infrastructure.

When prioritizing, several factors are considered:

- Real-time security threat information, including increased rates of incidents
- Regulatory mandates
- The criticality of the facility as measured by the impact of its loss on BPA’s ability to achieve its mission
- Criticality of a system or component based on its failure on maintaining security compliance and security system effectiveness
- Efficiencies to be gained by coupling the project with other work at the site

Table 2, on the following page, shows the typical prioritization scheme used to resource and schedule investments during initial enhancements as well as future maintenance.

Table 2. Priority Matrix

Priority Level	*Description*
Priority 1	Immediate threat mitigation in response to an event or change in threat conditions, which may or may not be based on tier designation.
Priority 2	Tier 1, 2, and 3 protection according to regulatory compliance requirements and by a graded security approach.
Priority 3	Protection of both energy and non energy facilities based on improving or enhancing security conditions using federal facility protection guidelines and standards provided by DOE, GSA etc. and; risk informed protection strategies to address security threats and gain efficiencies. These facilities may be assessed as Tier 4 sites.

1.5 Strategic Challenges

There are two main challenges which must be overcome for successful implementation of this strategy. These challenges and OSCO's current approach for managing them are outlined below.

Rapidly evolving regulatory requirements

Critical Infrastructure Protection (CIP) requirements issued by NERC CIP have had a major impact on BPA's security program, both in terms of resourcing as well as developing processes for successful implementation. NERC requirements emerge every one to two years requiring implementation within 12 to 18 months. It is difficult to anticipate the scope and budget for NERC projects in advance. Standard BPA processes for capital projects require a least a two to three year planning window which does not accommodate NERC timelines. Furthermore, NERC CIP impacts several BPA organizations with complex interdependencies and upstream/downstream impacts.

To address these challenges, BPA is developing an all stakeholder inclusive process for managing NERC CIP related and other security project work. BPA is looking to transition security capital program management to the appropriate organizational structure within BPA. This allows physical security resources to focus on NERC and other physical security activities related to assessment, standards development, implementation, training, performance testing and security threat management.

Aging and technologically obsolete systems

Large number of systems (primarily cameras) are projected to fail in the next few years due to exceeding manufacturer recommended Mean Time to Failure (MTTF). If not managed, this may impact security system effectiveness, cause a spike in maintenance fees and drain on limited resources.

The former strategy of actively replacing obsolete system components on a scheduled basis is not practical or feasible in the long term because the supporting infrastructure will need to be upgraded to support new technologies. Additionally, BPA security subject matter experts believe that the large number of cameras currently deployed is not providing a security risk reduction benefit commensurate to the level of investment and long term costs associated with reliable sustainability. BPA's OSCO is proposing a protection design standards which leverages new technology that can be sustained over the long term. The benefits to this approach are:

- Immediate reduction in costs associated with video surveillance maintenance
- Reduction in information technology band width and licensing costs
- Ability to redirect resources to more sustainable security system's development and implementation
- Maintaining "security in depth" and multi-layered alarm assessment capability

BPA implements a layered security approach that includes all aspects of the physical security, personnel security, information security and operations security disciplines. Video surveillance is almost exclusively

used to assess alarm activity after the fact. This has traditionally been one of two primary assessment tools to determine the nature of an alarm. The proposed strategy uses other less costly more sustainable technology to provide assessment capability in depth. Therefore, the decommissioning of significant video surveillance assets at substations is expected to have very minimal to no impact of security system effectiveness or assessment capability.

2. Asset Category Overview

2.1 Definition

A ***security asset*** is defined as material, equipment, software or hardware that is used for the primary purpose of providing security. The assets collectively make up security systems and overarching security infrastructure. OSCO defines the standards and requirements for the use of these systems based on subject matter expertise in interpreting and applying regulatory requirements and risk mitigation techniques. OSCO is ultimately accountable for the security infrastructure performance and its strategic deployment to provide the most effective protection for BPA assets.

2.2 Primary Asset Types and Groupings

Security assets are grouped by system or function. Protection strategies leverage several systems in unison for maximum benefit. In some instances individual components may support several systems simultaneously. The criticality of one component or system may change based on the number and type of strategies being deployed. Table 3 describes typical systems and components within those systems:

Table 3. Summary of Asset Groupings and Systems

- Maintenance rating is based on required service visits and/or associated costs. Service Cycle Scale: low = less than once a year, medium = at least once a year, high = more than once a year
- Cost Scale: low = < $5,000, medium = $5,000 - $10,000, high = > $10,000
- Life Cycle Scale: short = <5 years, medium = 5 to 10 years, long = > 10 years

System or Function	Purpose	Asset Types Include	O&M Characteristics	Assets Owner
Protective Barrier	Provide a physical, protective barrier between adversary and target. Protective barriers delay an adversary's attempts to gain entry or cause damage to critical components.	• Fence • Gate • Padlock • Chains • Barbed wire • Door • Bullet resistant glass • Window protection • Vehicle Barriers	• Low maintenance • Long life-cycle • Generally not replaced in its entirety. Usually repairs and upkeep involve small sections of fence, gate repair, etc. • O&M is low, but replacement of an entire fence or gate can be very high.	FAM
Surveillance	Video surveillance systems support assessment of alarms and allow for review of incidents within the field of view of the various cameras.	• Fixed cameras • PTZ cameras • DVR/NVR • Mounting structures, hardware, wiring, and circuitry • Thermal imaging devices	• High maintenance • Short/Medium life-cycle • High replacement costs (as a system, i.e., multiple cameras + NVR, and peripherals)	IT-JS

Intrusion Detection	Provides warning of pending intrusion and notification of an intrusion by unauthorized people attempting to carry out a crime or attack or improper access by employees. Intrusion detection provides depth to regulatory driven security systems that support NERC CIP compliance. Intrusion detection systems monitor and detect unauthorized access. Intrusion detection supports faster and more effective law enforcement response and assessment of security related activity.	• Motion detectors • All "access control" components • Fence detection systems • Motion sensing cameras • Motion activated lights • Tamper alarms • Glass break sensors	• Maintenance varies by component, but most will fall between Low/Medium • Medium lifecycle • Low costs with the exception of a few select cameras and fence detection systems • Camera O&M will be noted in Surveillance section.	IT-JS
Access Control	Access control systems provide multiple functions: - Provide records of whom and when people access a facility -Increase security by decreasing the number of hard keys in circulation -Decrease the vulnerability of door lock mechanisms because card key electronic locks are less prone to forced entry -Reduces vulnerability by immediately deactivating card keys that are lost or stolen and reduces the requirement to change locks after hard keys are lost. Access controls support NERC CIP compliance for monitoring and logging access.	• Door contact • Electronic locks • Magnetic lock • Request to exit sensors • Associated wiring, circuitry, and power supplies	• Medium maintenance • Long life cycle • Low replacement costs • Electro mechanical locking mechanisms require most frequent service visits dependent of frequency of use	IT-JS
Lighting	Lighting used specifically to address a security need, whether to support low light camera operation or to illuminate an area of security concern would be considered security lighting.	• Entrance or gates • Camera lights • Perimeter lights • Special area lights	• Medium maintenance • Short life cycle for conventional lights. • Long life cycle for modern technology such as LED. • Medium replacement cost	FAM
Early Intrusion Detection	Early Intrusion Detection provides the capability to detect activity outside the perimeter of the facility and provide early warning of potentially malevolent activity.	• Motion/Thermal detection surveillance devices: •	• Low Maintenance • Long life cycle • Medium replacement cost	IT-JS
IT Support System	IT infrastructure supports the access control and monitoring systems.	• Servers (Primary and Failover) • Network (LAN/WAN) • Applications (ProWatch, OnSSI, and Rapid Eye) • Database & Backup • ProWatch Reporting • Information Security & Compliance Monitoring	• Maintenance for these systems is covered under the IT Asset Management Plan	IT-JS/ JSO/ JN/JNN
Screening	Ensure that contraband such as weapons, firearms, controlled substances are not brought into BPA facilities.	• X ray machines • Metal detectors •	• Low maintenance • Long life-cycle • High replacement cost	OSCO

2.3 Service Provided

Transmission Services is a primary client of OSCO. More than 90 percent of maintenance activities and budget are dedicated to supporting critical transmission infrastructure protection.

Security assets provide the following benefit to their clients:

- Protection of employees
- Protection of critical, national infrastructure
- Protection of critical cyber assets and information
- Reduction in security incidents and criminal activity
- Support transmission grid reliability and regulatory compliance requirements
- Access control to federal facilities

2.4 Criticality Rating

Critical Infrastructure

Identification and ranking of site criticality is covered in BPA's CASP. For the purpose of this document any site that is not specifically identified as "Critical" may be covered under "Essential" or a Tier 4 ranking, depending on security risk assessments and conditions. Table 4 provides a high level overview of protection requirements.

Table 4. Infrastructure Criticality Ranking

Criticality Ranking	Facility	Protection Requirements
Tier 1	Control Centers	Armed guards, perimeter protection and patrol, access control, visitor control by logging, screening and escort. Meets regulatory compliance requirements.
Tier 2	Most Critical Substations	Security rated fence, early detection, intrusion detection, surveillance, security lighting, and access controls & visitor control by logging and escort. Meets regulatory compliance requirements.
Tier 3[6]	Critical Substation	Security rated fence, access and visitor control by logging and escort. Meets regulatory compliance requirements
Tier 4	Essential Facilities	Protection based on site specific assessments, federal facility protection guidelines and regulatory compliance requirements.

Critical Systems and Components

Criticality of a security system or component is influenced by the interdependencies with other components and systems. Table 5 shows all items in the current inventory[7] with indication of relationship to NERC CIP compliance and the current Graded Security Policy approach. "Protection Program Essential Elements" are documented in Appendix A of the SPAP.

[6] Protection requirements for Tier 3 sites are based on the FY11 CASP but may changed depending on assessments done in the out years. In the short term, control houses at Tier 3 sites will be protected to NERC CIP required standard and substation yard protected using an interim solution.

[7] Last updated 8/30/2011.

Table 5. Critical Security Components

Item Category	Count	NERC CIP Required	GSP
Camera	707		x
Card Reader	892	x	x
Door Contact	465	x	x
DVR	111		x
Electronic Lock	718	x	x
Firewall	87	x	
Motion Sensors/Detectors	27		x
Network switch	6	x	
PW-6000 Intelligent Controller (IC)	113	x	x
REX (Request to Exit) Device	287	x	x
RSA Primary / Failover	3/2	x	x
Serial to IP Converter	57	x	x
Terminal Server Primary / Failover	3/2	x	x
UPS (Uninterruptible Power Supply)	16	x	
Glass Break Sensors	16		x

2.5 Roles and Responsibilities

Installing and maintaining the security infrastructure is a collaborative effort across several BPA organizations due to the complex nature of the components which tie into the IT infrastructure (e.g. digital video), facility design and maintenance (e.g. perimeter fence). Implementation requires an array of engineering disciplines to work together to develop a design, and relies on transmission project management to orchestrate the construction as most systems are installed at transmission substations. OSCO is ultimately responsible for the design and efficacy of the security infrastructure which must be risk informed and compliant with ever-evolving regulatory requirements.

Managing these services requires a coordinated effort between OSCO, IT, Transmission Services and Facilities. OSCO is currently reassessing its processes, and redefining some technical support roles and responsibilities, to address complex nature of security design, as well as meet shorter timeframes for compliance driven projects. High-level roles and responsibilities for each organization are listed below.

Office of Security and Continuity of Operations (OSCO) - NN

- Accountability for security system effectiveness
- Development of requirements and standards based on BPA's protection needs and compliance obligations
- System performance testing
- Prioritization of system maintenance and repair activities
- Review and approve design
- Information owner responsible for identifying criticality of information contained on information systems in support of FISMA requirements (Federal Information Security Management Act)
- Identification, prioritization and tracking of corrective actions

- Liaise/consult with TS, FAM and IT to ensure security systems and designs meet all compliance requirements
- Administrative operation of access control system
- Administrative operation of video management system
- Identity verification and personnel risk assessments
- Issuance and accountability of access credentials
- Budget management
- Business case development and approval

Physical Access Control & Monitoring Team (PAC&M) -JS

- Information System Owner (ISO) and Information System Security Officer (ISSO)
- Implement quality assurance standards and procedures in accordance with IT standards (projects & enhancements)
- Ensure security system quality assurance, interoperability, reliability and performance
- Software application maintenance, development and support
- Cyber security management, audit and compliance (e.g., BPA IT, FISMA, NERC CIP, OIG)
- Maintenance vendor management and contracts (COTR duties)
- Ensure vendor:
    - Conducts periodic preventative maintenance based on system or component maintenance requirements and priorities
    - Break/fix based on PAC&M COTR call-out supported by approved priorities
    - System upgrades or enhancements as appropriate to meet compliance requirements
- Security system hardware operations and maintenance
- Research and development of new security system technologies.
- Address system hardware and/or software corrective actions identified by OSCO and other BPA organizations
- Approving authority for new IT based system components
- Review and approve design from an IT compliance and maintenance perspective

Facilities Asset Management (FAM)- NW

- Transition Management of Security's non-NERC capital portfolio starting in FY15
- Operations and maintenance of systems and components in Table 3, where FAM is identified as the asset owner (e.g. fences, lights, doors, windows, etc.)
- Operations and maintenance of FAM systems and components that support security assets
- Address corrective actions identified by OSCO
- Review and approve design where FAM assets are involved
- Coordinate other Transmission projects to ensure security systems remain intact or mitigating security processes or infrastructure is used
- Include security systems in new construction and facility updates

Transmission Organizations

There are many interdependencies with various Transmission organizations. Some of the key support organizations are listed below:

- Transmission Operations (TO) - Responsible for identify and prioritize critical infrastructure
- Transmission Field Operations (TF) – Responsible for funding security system maintenance activities at Transmission owned assets
- Substation Design (TESD) – Coordinates security system design for substations based on BPA construction standards, requirements provided by OSCO, IT, Facilities, and various design groups including (Architectural Design (TESF), System Control Engineering (TEC), Telecom

Engineering(TECT), System Protection Technical Services (TECS), Communications Control Planning (TPMC)

- Project Management Team (TEP)
  - Manage (capital) security enhancement projects at substations
  - New security enhancement installation vendor management and contracts (COTR duties)
  - Ensure install vendor
    - Meet project schedule, scope, and budget
    - Provide updated blue prints (post installation)
  - Provide a monthly status update on project execution scope, schedule and budget
  - Coordinate other transmission projects to ensure security systems remain intact or mitigating security processes or infrastructure is used

2.6 Metrics

BPA's OSCO has established performance targets for all identified initiatives. On the following page, Table 6 shows current and future targets for measuring success of the asset management initiatives. Future targets will be phased in as appropriate by either addition to current measures or in place of those measures, with a progressive drive for improved performance.

Table 6. Performance Metrics

Initiative	FY14 Targets	FY15 & Future Target
1. Compliance	1) Security system enhancement in support of NERC CIP Versions 2-4 and subsequent versions. 2) No NERC-CIP violations as a result of inadequate or malfunctioning Physical Security assets (e.g. card readers, door contacts, etc.) resulting in a violation from an audit and that was not previously self-reported.	1) Complete security system enhancement in support of NERC CIP Version 3 and 4 by April 2014, within scope and budget. 2) No NERC-CIP violations as a result of inadequate or malfunctioning Physical Security assets (e.g. card readers, door contacts, etc.) resulting in a violation from an audit and that was not previously self-reported.
2. Critical Infrastructure Protection	1) Transition non-NERC capital initiative management to FAM 2) Complete business case for next set of Tier 2 security enhancements 3) Complete business case for Tier 3 security enhancements	1) FAM is successful in managing non-compliance capital initiatives as demonstrated by completion of slated projects. 2) Complete 2 Tier 2 security enhancements 3) Complete Tier 3 enhancements
3. Essential Infrastructure Protection	1) Audits/assessment indicate that federal facility protection guidelines and standards provided by DOE, GSA and other regulating bodies are found to be met within acceptable risk level.	1) Audits/assessment indicate that federal facility protection guidelines and standards provided by DOE, GSA and other regulating bodies are found to be met within acceptable protection levels and threat management practices.
4. Performance Testing & Preventative Maintenance	1) SPAP visits by OSCO are conducted as scheduled 2) JS conducts sites visits and preventative maintenance (PM) checks as scheduled	1) SPAP visits by OSCO are conducted as scheduled 2) JS conducts sites visits and PM checks as scheduled

5. Replacement and Renewal Program	1) JS - break/fix call outs are prioritized and addressed based on component criticality as documented in the maintenance vendor's Statement of Work. 2) Develop and start implementation of a new, risk informed protection design standard for upgrading security systems currently deployed.	1) JS - break/fix call outs are prioritized and addressed based on component criticality as documented in the maintenance vendor's Statement of Work. 2) Ongoing implementation of a new, risk informed, protection design standard for upgrading security systems currently deployed at Tier 3 sites. 3) Positive ROI on new standard as a result of Reduction in # of break/fix callouts by FY 2017.

3. Capital Investment Recommendations

The CASP was developed to document BPA's protection strategies of its critical systems and assets that are risk-informed and compliant with all regulatory obligations, including those mandated by U.S. Department of Energy (DOE), North American Electric Reliability Corporation (NERC) and Department of Homeland Security (DHS). This integrated protection approach is the primary driver behind security's capital program, and was supported by BPA's Business Operations Board (BOB) in September 2010 for implementation.

The implementation of the CASP translates into three strategic initiatives, which for the FY14-23 planning horizon result in the following activities:

- ***Initiative 1. Compliance*** - Implementation of security systems in response to regulatory mandates issued by NERC
- ***Initiative 2. Critical Infrastructure Protection*** - comprehensive protection of the most critical Tier 1, 2 and 3 sites
- ***Initiative 3. Essential Infrastructure*** - protection of facilities essential to operation.

The following sections describe the planning framework and provide investment recommendations. Some security enhancement initiatives are qualified by security risk reduction analysis based on a Streamline Security Risk Assessment strategy (SSRA) derived from the Risk Assessment Methodology for Transmission (RAM-T). More detail on the risk comparison is covered in Appendix A-1.

3.1 NERC CIP Version 1 through 5 Compliance Enhancements

NERC CIP implementation from the date of release to "go live" is typically eight quarters or two years. As such, projecting the cost impact of NERC requirements is typically limited to a three year window. Starting in 2012, OSCO has been focused on deploying security systems to meet requirements issued in NERC CIP 006 versions 2 through 4. Version 4 did not impact physical security system requirements. Version 4 defined how sites and critical cyber assets are identified and categorized. This has resulted in an increasing number of sites required to be protected. Version 5, again, changes and clarifies how sites and cyber assets are identified and categorized. The new "Draft" Version 5 establishes a bright-line criteria and three levels of site criticality; High, Medium and Low. It is currently under development and targeted for implementation 8 quarters after approval, which could start as early as February 2014. If implemented, it could have an impact on future budget requirements.

NERC CIP 006 Versions 2 and 3

The physical security requirements from NERC released in CIP 006 Versions 2 and 3 focus on protection of Critical Assets (CAs) containing Critical Cyber Assets (CCAs) by enhancing access control through electronic access controls, logging and monitoring. Video surveillance, motion sensors and glass breaks have been used to provide security in-depth in addition to meeting basic compliance requirements. As indicated by risk comparison in Table 7, this investment reduces the security risk posed by the insider threat, however has limited risk reduction on other threat categories.

Table 7. Security Risk Rating Impact of Tier II Protection

	Before NERC CIP Version 3[8]		After NERC CIP Version 3		
Threat	**Risk Numerical**	**Risk Range**	**Risk Numerical**	**Risk Range**	**% Risk Reduction[9]**
International Terrorist	0.49	Medium	0.49	Medium	**0%**
Eco Terrorist/Special Interest	0.45	Medium	0.45	Medium	**0%**
Criminal Activity	0.45	Medium	0.45	Medium	**0%**
Vandal	0.4	Medium	0.4	Medium	**0%**
Insider	0.23	Low	0.13	Low	**10%**

During 2010, Western Electricity Coordinating Council (WECC) conducted an audit of BPA's compliance with NERC CIP provisions and issued a Notice of Alleged Violation (NOAV) to BPA. The NOAV indicated that BPA has a gap in required access control, logging and monitoring systems when particular transmission equipment, which they considered to be a CCA, is brought online (e.g. D400s and Ethernet-based relays). In FY13 BPA enhanced access control at the 16 transmission sites with active critical cyber assets. Other sites were started and some completed in FY13 and will continue in FY14 in order to facilitate activation of CCA equipment for Transmission's operational compliance.

Table 8 shows the current funding assumption for NERC CIP related work. Starting in FY16, $500 thousand is set aside in anticipation of ongoing NERC activities. If NERC activities slow down, or stop, funding will be reprioritized to critical site protection program.

Table 8 . Capital Cost for NERC CIP ($000s)

FY	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
NERC CIP Version 2 - 5	3,197	1,500	-	-	-	-	-	-	-	-	4,697
NERC CIP Version X	-	-	500	500	500	500	500	500	500	500	4,000
TOTAL	**3,197**	**1,500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**8,697**

3.2 Protection of Tier 1 Sites

BPA's most critical facilities are its control centers. They are classified as Tier 1 facilities. Munro Control Center is being expanded in FY13 to FY15 to include a scheduling center. Assessment of the security systems, as covered by the construction plan, has revealed an opportunity for gaining efficiency in implementing physical security systems providing long term savings to BPA of approximately 250K annually. The assessment and resulting proposal is being implemented during the current construction of the Munro Control Center/Scheduling Center upgrade project. In addition, this security proposal will provide substantial assurance that the facility will be adequately protected during all operational conditions including normal, emergency and during major continuity of operations disaster recovery operations. Table 9 shows the cost to fund an enhanced security protective system for the Munro Complex that will deliver an integrated security solution that is expected to save BPA approximately $250,000 annually resulting in a return on investment after three years.

Table 9. Capital Cost Projection for Munro Complex - Tier 1 Protection ($000s)

FY	2013 Act.	2014	2015	2016	2017	2018	2019	2020	2021	Total
Tier 1 Critical Site Protection	351	304	-	-	-	-	-	-	-	**654**
TOTAL	**351**	**304**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**654**

[8] The "Before" state assumes Level 1 which includes fenced Control House, one automated vehicle gate, camera at the vehicle gate.

[9] Percentage of risk reduction is based on maximum Risk Numerical value of 1.

3.3 Protection of Tier 2 Sites

The objective of this program is the installation of security systems that provide the recommended solution for protecting BPA's most critical substations categorized as Tier 2 sites.

This program mitigates the possibility of BPA being noncompliant with regulatory requirements related to protection of national critical infrastructure and prevents the major consequences of attracting national and regional attention and criticism for failure to adequately protect national critical infrastructure. More importantly, this project helps to mitigate the rare, but extreme, risk of a malevolent attack against the transmission system. Such an attack could impact system reliability causing loss of revenue and long term reductions in transmission capability.

The design calls for installation of a security fence that is anti-cut, anti-climb and has reduced target visibility by up to 38.5% when compared to the current chain-linked fence. In addition to the robust fence, the design includes security lighting, surveillance, and video analytic capability for the perimeter which provides a moderate level of early detection.

Table 10. Estimated Security Risk Impact - Tier II Protection

	Before Tier II Treatment[10]		After Tier II Treatment		
Threat	**Risk Numerical**	**Risk Range**	**Risk Numerical**	**Risk Range**	**% Risk Reduction**
International Terrorist	0.49	Medium	0.42	Medium	7%
Eco Terrorist / Special Interest	0.45	Medium	0.36	Medium	9%
Criminal Activity	0.45	Medium	0.2	Low	25%
Vandal	0.4	Medium	0.18	Low	22%
Insider	0.13	Low	0.13	Low	0%

Ten substations were identified as needing this additional level of protection. The first Tier 2 site was treated as a proof of concept in FY12. BPA has assessed this initial design to identify improvements for the next implementation, thus providing the best value for the investment. Two additional sites are approved for implementation in FY15.

Table 11. Capital Cost Projection for Tier 2 Program ($000s)

FY	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Tier 2 Critical Site Protection	-	6,807	2,887	7,070	5,517	7,307	4,131	-	-	-	**36,775**
TOTAL	**-**	**6,907**	**5,787**	**7,070**	**5,517**	**7,307**	**4,131**	**-**	**-**	**-**	**39,775**

3.4 Protection of Tier 3 Sites

Based on the updated prioritization scheme which takes into account threat and security system effectiveness information, funding is being proposed for protection of three Tier 3 sites prior to finishing out the Tier 2 protection program. It is proposed that one Tier 2 site implementation be delayed by a year in FY16 to allow for implementation of these Tier 3 sites.

One Tier 3 substation, experiencing ongoing criminal activity, is being considered for security fence upgrade and security lighting. In the last 3 years this site has experienced multiple and repetitive intrusions into the substation's energized yard and the spares storage yard. Law enforcement access has been provided to the non-energized areas and an increase in patrols has been established. However, intrusions continue to be a problem for this site. BPA security continues to work with federal law enforcement officials to address systemic metals theft activity in the area.

[10] *The "Before" state assumes Level 1 and NERC CIP systems up to CIP 006 Version 3.*

BPA risk tolerance from theft is fairly high. However, collateral damage resulting from attempted theft of copper grounds and other substation cables and wiring is known to have a substantially higher consequence than the underlying simple theft. Therefore, risk tolerance for that kind of event is very low. In 2009 over one million dollars in damage, not including loss of transmission capability, occurred after a similar ongoing series of criminal events at another site.

Two sites were previously protected with higher level security systems due to their relative importance in the Northern Washington, King County area. These sites were assessed in 2003 and in subsequent security risk assessments along with a Tier 2 site covered above as a triad of regionally critical sites not withstanding current NERC CIP assessment methodologies and requirements. Both sites do currently meet NERC CIP requirements if CCA's were to be activated. The two Tier 3 sites in question have experienced a significant decrease in security system reliability and effectiveness due to aging and malfunctioning of non-NERC security systems. In order to achieve recommended levels of security for these sites security fencing and security lighting should be installed.

This delay establishes an exposure for; a) ongoing high maintenance and repair costs for systems that are not aligned to our current protection strategy for Tier 3 sites, b) lack of risk mitigation against criminal activity and intrusion into the energized yards, c) regional criticisms from local utilities and state government regarding the protection of regionally critical facilities which are vital to local critical infrastructure and economy.

Table 12. Capital Cost Projection for Tier 3 Program ($000s)

FY	2014	2015	2016	2017	2018	2019	2020	2021	2022	Total
Tier 3 Critical Site Protection	-	250	2,850	-	-	-	-	-	-	**3,100**
TOTAL	**-**	**250**	**2,850**	**-**	**-**	**-**	**-**	**-**	**-**	**3,100**

3.5 Other Essential Infrastructure Protection

This section is to cover protection of operationally essential facilities such as BPA Headquarters in Portland, OR and electrical facilities which may not rise to a Tier 2 or Tier 3 level but experience recurring criminal activity requiring attention.

BPA Headquarters has undergone significant security upgrades for access controls, video surveillance system upgrades, and barrier technology in the last 5 to 10 years. BPA Headquarters has no current capital requirements. However, in anticipation of future needs, funding has been set aside in FY21.

Table 13. Corporate and Tier IV Site Protection ($000s)

FY	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Essential Facilities	-	-	-	-	-	-	-	500	500	500	**1,500**
TOTAL	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**500**	**500**	**500**	**1,500**

3.6 Other Considerations

Management of Tier 2 and 3 capital program is going to transition to FAM starting in FY15. This process change is expected to yield operational efficiencies by handling project management through established standards. There may be an added benefit of aligning and grouping facility and security projects to minimize overhead costs and impact to substation operations.

BPA Physical Security Subject Matter Expert's will continue to act as the technical experts in setting requirements and standards, conduct assessments, propose improvements and facilitate business case development for funding this important risk mitigation program.

4. Investment Recommendations - Expense

In accordance with DOE order 473.3, the objective of the SPAP program is to identify essential security system elements, conduct regular system performance tests and maintenance, with corrective maintenance occurring commensurate with the level of criticality and location of the system.

Security asset maintenance activities are broken out into four categories, under Initiatives 4 and 5, as follows:

- ***Initiative 4. Performance Testing & Preventative Maintenance***
    1. Site visits by Physical Security Specialists to conduct site security testing and security conditions survey to ensure continued system effectiveness
    2. Site visits by the maintenance vendor to assess asset conditions, conduct preventative maintenance, and install planned updates of critical components
- ***Initiative 5. Replacement & Renewal Program***
    3. Phased upgrade of obsolete systems to a new, technologically improved standard
    4. Replacement upon failure and/or corrective maintenance in response to performance tests or malfunctioning system components

The maintenance strategy has changed from individual component maintenance and upgrade to a more holistic approach of upgrading entire security infrastructure at a site based on a new and developing design standard. Updating analog and obsolete systems one component at a time is no longer practical, or feasible, as the supporting infrastructure needs to be upgraded to support the new technology.

To help offset the cost of deploying a new design standard OSCO is reconsidering its high use of cameras. It is believed that OSCO can decommission a large number of outdated cameras with minimal to no impact to security system effectiveness. This approach is in part due to the implementation of different security technologies, such as glass break sensors, that provide security in depth and maintains assessment capability without the expense of extensive video surveillance systems. Furthermore, OSCO expects to find efficiencies by combining security work with facility projects at sites requiring more substantial upgrades.

Each maintenance activity is broken out into Transmission and Corporate based on the funding stream. Security systems at transmission owned sites are funded by Transmission Field (TF) budget, while systems installed at Headquarter building are paid for out of the corporate cost center. Maintenance activities for non-electrical transmission facilities, such as those on the Ross Complex, are paid out of the Transmission Field budget as well. This division and cost allocation ensures that Power Services funds asset activities in accordance with its use and benefits.

4.1 Performance Testing & Preventative Maintenance – Initiative 4

The DOE order requires security systems to be performance tested at least every two calendar years. The requirements for testing and maintenance under NERC is every three years.

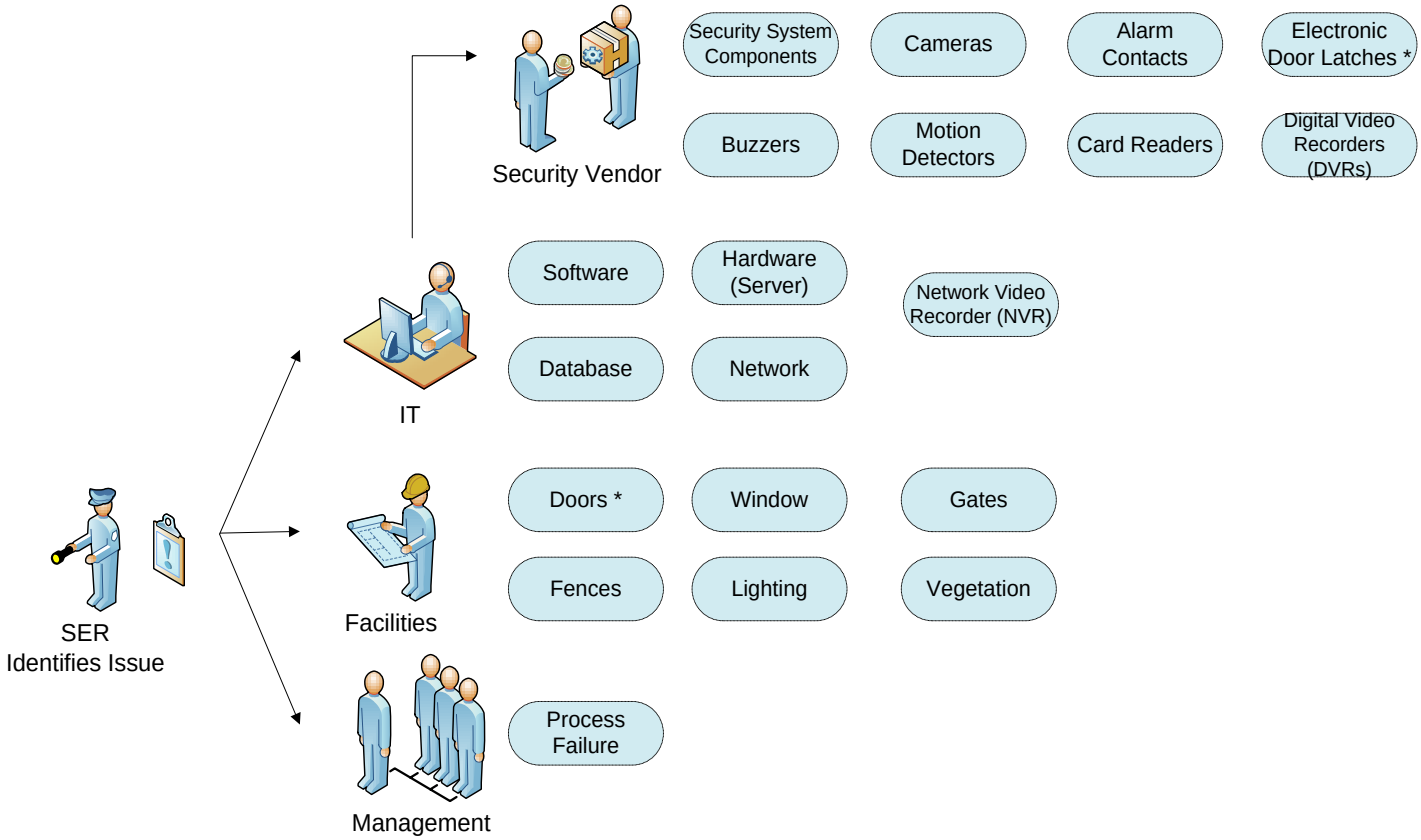
Security system performance is ensured in the following ways:

- Physical Security team conducts the performance testing at approximately one half of the sites per year (about 32 sites as of November 2013)
- Physical Security team issues corrective actions and recommendations
- Vendor supported preventative maintenance (PM) as a general rule is on a two year cycle by site. Some sites may need to be visited more often based on environmental conditions or in support of fence intrusion detection system maintenance (4 sites) which is two visits per year
- Maintenance vendor conducts preventative maintenance of critical components
- Alarm Monitoring Station randomly reviews surveillance footage 24 hours a day

- Any issues impacting the performance of the security system are reported to the group responsible for addressing the issue in accordance with requirements identified in DOE O 473.3 Attachment 3, Section A, Chapter V. Maintenance.

Figure 2, below, shows most common issues and routing protocols.

Figure 2. Corrective Action Routing



The cost associated with this program only cover maintenance vendor charges and are estimated based on the vendor contract solicitation and Statement of Work (SOW). The contract has not yet been awarded; therefore the estimates are subject to change. Any cost for repair or replacement is documented under Initiative 5 – 4.2.2 "Cost of Replacement Upon Failure", Table 16.

Table 14. Projected Costs for SPAP Program ($000s)

FY	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
TRANSMISSION Site Visits & Preventative Maintenance	40	41	42	44	45	46	48	49	51	52	459
CORPORATE Preventative Maintenance	7	7	7	8	8	8	8	9	9	9	80
TOTAL	**47**	**48**	**50**	**51**	**53**	**54**	**56**	**58**	**60**	**61**	**539**

4.2 Replacement and Renewal Program – Initiative 5

4.2.1 Deployment of New Standard

In FY14 BPA is initiating development and implementation of a new risk informed protection design standard for upgrading security systems currently deployed at Tier 3 sites. The systems deployed at these sites use obsolete outdated technology. If not managed strategically the maintenance costs could double in FY15 due to large number of systems failing because they were all installed within a short window of time with approximately 40% exceed mean-time to failure by at least 3 years in FY14. Ongoing maintenance of over 700 cameras is the primary driver behind this anticipated spike in maintenance cost.

The new video design calls for fewer cameras which will allow BPA to strategically decommission a large number of cameras as they fail (without replacement) and minimize the financial impact for maintaining an outdated design. Physical Security experts believe that reduction in cameras can be achieved with minimal to no impact on the security system effectiveness. This approach is in part due to the implementation of different security technologies such as glass break sensors in combination with motion detection and door contact alarms that provide security in depth and maintains assessment capability without the expense of extensive video surveillance systems. The decommissioning of video cameras and the installation of glass break sensors will be a concurrent effort. The benefit of this approach can be noted by:

- Reduced cost from ongoing maintenance replacement and upgrade of expensive video systems
- Reduced cost from relatively inexpensive glass break sensors intended to provide security in depth and maintain alarm assessment capability
- Initial implementation cost for this approach is expected to be substantially less costly than the long term costs associated with maintenance, replacement and upgrades to existing video systems

Another avenue of increasing security system efficiency has been identified by simplifying the security systems installed at individual sites. This involves the removal of “Arm / Disarm” panels (Vista Panels) which have been the focal point for employees making mistakes in arming and disarming the system, thus creating potential security violations and increased risk due to sites being left unarmed. In FY14 we anticipate six sites will be configured with the new “Vista-Less” configuration. These sites will be individually tested upon completion, and observed and tracked for at least 90 days to determine the operational impacts and to confirm security system operations are adequate.

This project will:

- Reduce the long term expense of maintaining and replacing Vista Panels
- Reduce or eliminate alarm system arming failures and employee mistakes related to arming and disarming alarm panels
- Increase the overall reliability of the security systems
- Decrease risk associated with failure to maintain compliance.

Since the standard has not been finalized, it is difficult to say the exact cost per site. Some early estimates assume cost per site around $75,000. If this assumption holds, BPA may need to increase expense budged to complete this initiative without increasing risks to compliance and projection due to critical system failures. With current funding, only 20 of the nearly 60 critical sites can be addressed through the FY17 rate period.

Table 15. Projected Costs for New Security Standard Deployment Program ($000s)

FY	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
TRANSMISSION New Standard Implementation	285	476	407	323	337	321	248	238	145	112	2,892
TOTAL	**285**	**476**	**407**	**323**	**337**	**321**	**248**	**238**	**145**	**112**	**2,892**

4.2.2 Replacement Upon Failure

BPA's security system design was developed as a layered system to minimize a single point of failure. A layered security system leverages the various components, technologies, and manual intervention to help ensure continuous protection coverage. When using this approach, there are a limited number of system components whose failure would result in immediate elevation of risk requiring an immediate response. The layered security system supports a "break/fix" strategy or replacement upon failure approach.

Current estimate budget on 180 estimated call outs in FY13 at $1200 average cost for one day. That amount is expected to decrease as sites are updated to new standard.

Table 16 . Cost of Replacement Upon Failure ($000s)

FY	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
TRANSMISSION Replacement Upon Failure	216	218	220	223	225	227	229	232	234	236	2,260
CORPORATE Replacement Upon Failure	11	11	12	12	13	13	14	15	15	15	131
TOTAL	**227**	**229**	**232**	**235**	**238**	**240**	**243**	**247**	**249**	**251**	**2,391**

4.2.3 Maintaining Tier 2 Site Enhancements

As described under Section 3.3, Initiative 2 will result in large scale security system enhancements at BPA's most critical transmission sites. The maintenance requirements have been estimated as follows:

- Year 1 – Covered under warranty
- Year 2 – $5,000 for maintenance
- Year 3 – $10,000 for maintenance and minor repairs/replacements
- Year 4 – $30,000 for maintenance and increased number of repairs/replacements
- Year 5 – $50,000 for maintenance and increased number of repairs/replacements
- Year 6 – $5,000 for maintenance
- Year 7 – Repeating cycle from year 2

Based on the recommended implementation schedule (Section 3.3 - Table 11) maintenance costs are estimate in Table 17. As the implementation takes place, and the individual components are added to the inventory, the maintenance activities will be incorporated into the "Replacement & Renewal" program.

Table 17. Tier2 Maintenance Projection ($000s)

FY	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
TRANSMISSION Tier 2 Maintenance	-	5	10	40	80	95	195	205	220	250	1,100
TOTAL	**-**	**5**	**10**	**40**	**80**	**95**	**195**	**205**	**220**	**250**	**1,100**

5. Summary of Recommended Investments

The Security Infrastructure Asset Management Strategy seeks to balance compliance and protection initiatives to provide BPA with the most risk appropriate security, applying sound asset management principles and efficiency studies to manage costs and maximizing the use of rate payer dollars. Process improvements and new design standards are the highlights of the current approach and will set the direction for the next decade.

5.1 Proposed Capital Plan for FY2014 – FY2023

OSCO is proposing a capital model which funds:

- NERC CIP required protection with place holder funding beyond the current NERC CIP version at $500K per year starting in FY16
- Graded security and critical infrastructure protection at Tier 1, 2 and 3 sites
  - Finishing up installation of an enhanced security protective system for the Munro Control Center Complex, a Tier 1 critical asset
  - Implementation of graded risk-informed security standard at Tier 2 critical substations
  - Funding protection for at-risk Tier 3 critical substations
- Anticipated work in the future for essential infrastructure protection such as Headquarter building.

This proposal ensures timely funding for the required security enhancements with minimal risk exposure especially as it relates to: a) ongoing high maintenance and repair costs for systems that are not aligned to our current protection strategy, b) risks posed by criminal activity and intrusion into the energized yards, c) regional criticisms from local utilities and state government regarding the protection of regionally critical facilities which are vital to local critical infrastructure and economy.

Table 18. Proposed Capital Plan from FY 2014 – FY 2023 ($000s)

FY	2012 Actual	2013 Actual	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total FY14-23
Immediate Threat Mitigation	-	-	-	-	-	-	-	-	-	-	-	-	-
Regulatory Compliance	482	2,290	3,197	1,500	500	500	500	500	500	500	500	500	8,697
Tier 1 Critical Site Protection	-	351	304	-	-	-	-	-	-	-	-	-	304
Tier 2 Critical Site Protection	2,923	133	-	6,661	3,033	7,070	5,517	7,307	4,131	-	-	-	33,719
Tier 3 Critical Site Protection	-	-	-	250	2,850	-	-	-	-	-	-	-	3,100
Essential Facilities	-	534	-	-	-		-	-	-	500	500	500	1,500
TOTAL CAPITAL	**3,405**	**3,309**	**3,501**	**8,411**	**6,383**	**7,570**	**6,017**	**7,807**	**4,631**	**1,000**	**1,000**	**1,000**	**47,320**

5.2 Proposed Expense Plan for FY 2014 - FY 2023

Maintenance strategy has shifted from individual component maintenance and upgrade to a more holistic approach of upgrading entire security infrastructure at a site based on to a new standard.

The maintenance and update activities are funded from two sources. Security systems at transmission sites are funded by Transmission Field (TF) budget, while systems installed at Headquarter building is paid for out of the corporate cost center. Funding estimates to achieve the proposed maintenance objectives are summarized in Table 19.

Table 19. Expense Plan for Security System Maintenance from FY 2014 – FY 2023 ($000s)

FY	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Transmission Funds										
Performance Testing & Maintenance	41	42	44	45	46	48	49	51	52	459
Replacement Upon Failure	218	220	223	225	227	229	232	234	236	2,260
New Standard Deployment	476	407	323	337	321	248	238	145	112	2,892
Tier 2 Maintenance	5	10	40	80	95	195	205	220	250	1,100
Trans. Sub-Total	**740**	**680**	**630**	**687**	**689**	**720**	**723**	**650**	**650**	**6,710**
Corporate Funds										
Performance Testing & Maintenance	7	7	8	8	8	8	9	9	9	80
Replacement Upon Failure	11	12	12	13	13	14	15	15	15	131
Corp. Sub-Total	**18**	**19**	**20**	**21**	**21**	**22**	**24**	**24**	**24**	**211**
TOTAL	**758**	**699**	**649**	**708**	**711**	**743**	**747**	**674**	**674**	**6,922**

APPENDIX A - RISK REDUCTION

Over the last 13 years BPA has conduct hundreds of security and risk assessments using several industry accepted methodologies. As a result, risk assessment information has been captured in a streamlined security risk assessment document outlining all the various risk conditions and reduction calculations for the several different security system configurations employed by BPA.

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 over one million dollars in damage. The NERC CIP requirements had no risk reduction against general criminal activity.

Figure RR-1.1 Collateral Damage from Attempted Metals Theft

Beginning in 2001 BPA began to implement security improvements based on risk assessments. The improvements were developed in progressively increasing levels of 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 from implementing compliance driven security systems.

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 2010 the Streamlined Security Risk Assessment Strategy was developed in order to facilitate a continuing risk based security assessment process to identify the effectiveness of security systems and risk reduction. 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.

Security Asset Management Strategy

All currently identified Tier 1, 2, and 3 sites containing Critical Cyber Assets meet NERC CIP compliance requirements. Tier 2 and 3 sites, not currently identified as having Critical Cyber Assets but are anticipated to be so identified at a later date, are also provided with systems sufficient to meet compliance with the exception that several sites are undergoing additional assessment for security infrastructure installation to address newly identified gaps in the physical security perimeter.

Below are two scale tools and two risk tables provided to illustrate risk reduction resulting for critical sites if they had no security systems installed and, for comparison, current Tier 2 and Tier 3 security enhancements at sites that also have all NERC CIP security requirements completed.

The scale tools illustrate where on the risk continuum *very low, low, medium, high* and *very high* are placed with respect to a .01 to .99 scale range. The threat scale differs only in that it has a set of numbers below the line representing "points" achieved during the threat assessment. The scale tool for consequence and system effectiveness need no such numbers.

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 RR-1.2 Threat Assessment Scale Tool

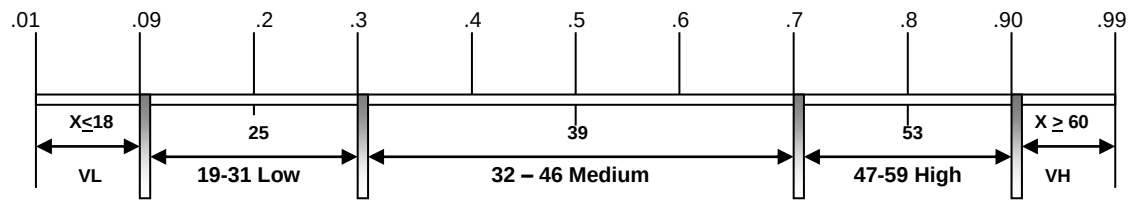


Figure RR-1.3 Consequence and Security System Effectiveness Scale Tool

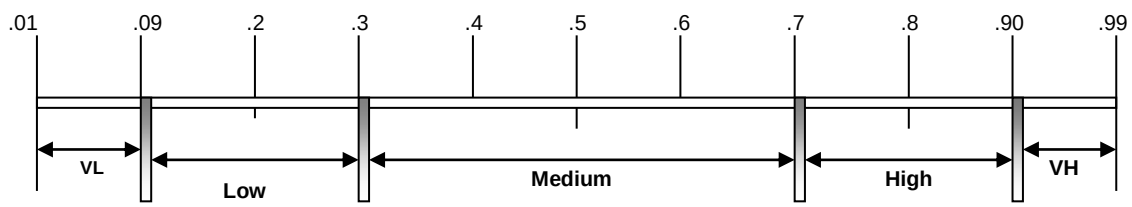


Table RR-1.1, below, shows an estimation of security risk according to previous conditions wherein no security enhancements had been installed. This data was retrieved from risk assessments conducted from 2001-2008 and updated in the SSRA.

Table RR -1.1 Estimated Risk for 500kV Critical Substations- <u>No Security Enhancements</u>

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

Table RR-1.2, below, represents estimated risk levels for Tier 2 sites with all NERC CIP requirements satisfied. It is derived directly from the SSRA. It reflects risk reduction when compared to Table RR-1.1 having no security systems installed. Tier II security improvements include penetration resistant fences. The entire perimeter, including the control house, is fenced with automated card key operated vehicle gates with integrated fence intrusion detection system *or* a motion detection video analytic system with infrared capability, security lighting with outward pointing high intensity motion sensor activated lighting.

Table RR-1.2 Estimated Risk Reduction for 500kV site with Tier 2 and NERC CIP 006 Versions 1-3

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Numerical	Risk Range
International Terrorist	.5	.99	.2	.39	Medium
Eco Terrorist/Special Interest	.5	.9	.3	.3	Medium
Criminal Activity	.9	.5	.55	.2	Low
Vandal	.8	.5	.6	.16	Low
Insider	.5	.5	.5	.13	Low

Table RR-1.3, below, represents estimated risk levels for Tier 3sites with all NERC CIP requirements satisfied. This table reflects risk reduction when compared to Table RR-1.1 having no security systems installed. Tier 3 security improvements include penetration resistant fences. The entire perimeter, including the control house, is fenced with automated card key operated vehicle gates security lighting.

Table RR-1.3 Estimated Risk Reduction for 500kV site with Tier 3 and NERC CIP 006 Versions 1-3

Threat	Threat (Pa)	Consequence (c)	Security (Pe)	Risk Numerical	Risk Range
International Terrorist	.5	.99	.15	.42	Medium
Eco Terrorist/Special Interest	.5	.9	.2	.36	Medium
Criminal Activity	.99	.5	.5	.25	Medium
Vandal	.8	.5	.5	.2	Medium
Insider	.5	.5	.5	.13	Low
Insider	.5	.5	.5	.13	Low

Financial Disclosure

This information has been made publicly available by BPA on February 18, 2014 and contains information not reported in BPA financial statements.