



**Security Infrastructure Asset Management Strategy**  
**FY2012 through FY2021**

November 2, 2012

## Table of Contents

|  |    |
|--|----|
| Executive Summary .....  | 3  |
| Introduction .....   | 3  |
| Purpose and Scope of Strategy .....                                      | 4  |
| Key Accomplishments and Historic Backdrop .....                          | 5  |
| Drivers, Initiatives and Risks .....                                     | 6  |
| Prioritization.....  | 8  |
| Approved Capital Plan for FY 2012 - FY 2021 .....                        | 9  |
| Optimized Capital Plan for FY 2012 - FY 2021 .....                       | 9  |
| Summary .....  | 11 |
| 1. Asset Management Objectives, Scope and Strategic Direction .....      | 12 |
| 1.1. Objectives .....  | 12 |
| 1.2. Service Provided.....   | 12 |
| 1.3. Strategy.....   | 13 |
| 2. Asset Category Overview .....   | 16 |
| 2.1. Definition.....   | 16 |
| 2.2. Inventory Management.....   | 16 |
| 2.3. Primary Asset Types and Groupings .....                             | 17 |
| 2.4. Roles and Responsibilities .....                                    | 19 |
| 2.5. Summary of Critical Infrastructure, Systems and Components .....    | 20 |
| 2.5.1. Critical Infrastructure .....                                     | 20 |
| 2.5.2. Critical Systems and Components .....                             | 20 |
| 2.6. Prioritization .....  | 21 |
| 2.7. Risks .....   | 22 |
| 2.8. Metrics .....   | 23 |
| 3. Capital Investment Recommendations.....                               | 25 |
| 3.1. Critical Asset Security Plan (CASP) - Initiatives 1, 2 and 3.....   | 25 |
| 3.1.1. Protection of Control Centers.....                                | 25 |
| 3.1.2. Protection of Most Critical Transmission Assets.....              | 25 |
| 3.1.3. NERC CIP Compliance Implementation .....                          | 27 |
| 3.1.4. Essential Infrastructure Protection .....                         | 28 |
| 4. Investment Recommendations - Expense .....                            | 30 |
| 4.1. HSPD-12 Compliance – Initiative 1 .....                             | 30 |
| 4.2. Performance Testing & Preventative Maintenance – Initiative 4 ..... | 30 |
| 4.3. Replacement and Renewal Program – Initiative 5.....                 | 31 |
| 4.3.1. Replacement upon Failure.....                                     | 31 |
| 4.3.2. Planned Replacement .....   | 32 |
| 4.3.3. Maintaining Tier II Site Enhancements .....                       | 33 |
| 4.4. System Reliability Projects – Initiative 6.....                     | 33 |
| 4.5. Access Credential Management – Initiative 7 .....                   | 34 |
| 5. Summary of Recommended Investments.....                               | 36 |
| Appendix .....   | 38 |
| A-1 Comparison of Risk Reduction .....                                   | 38 |

## Executive Summary

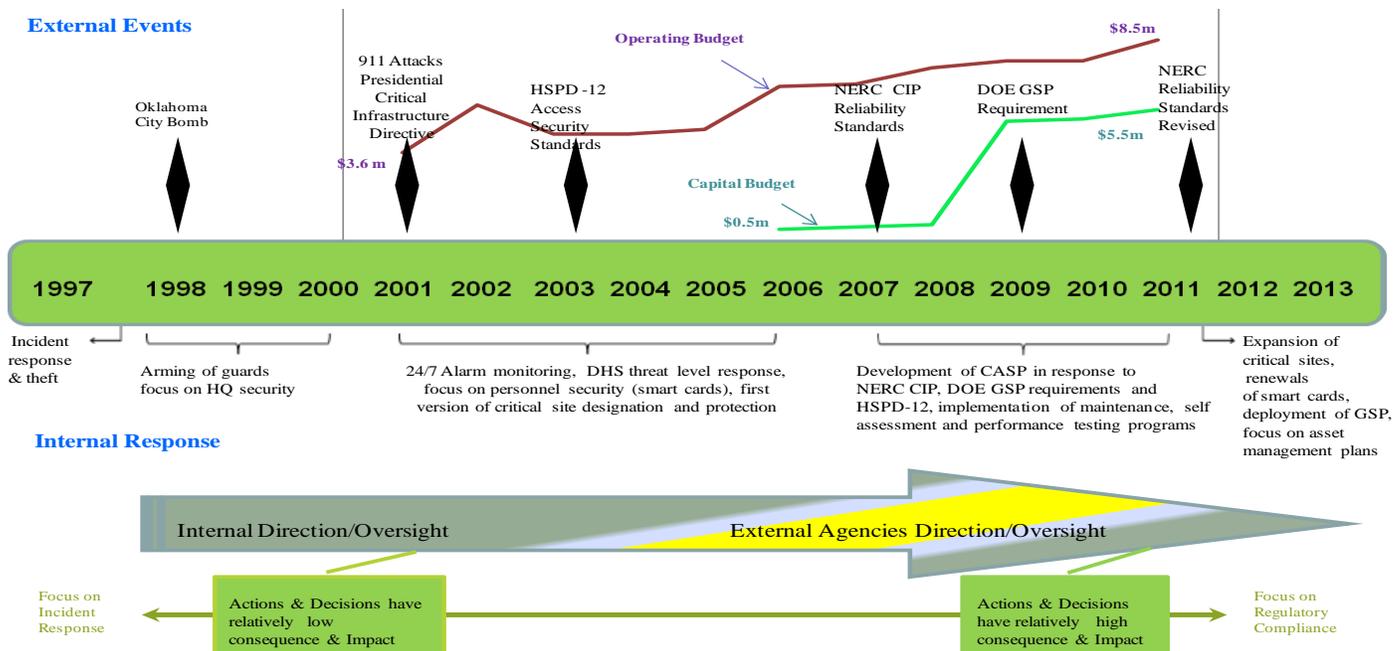
### Introduction

BPA is committed to managing its security system infrastructure and implementing security enhancement project plans through risk informed processes, while minimizing the overall costs under prudent asset life-cycle management strategies. Consistent with the public’s expectations, BPA protects its workforce, systems, information and facilities that are integral to accomplishment of its mission while ensuring that its security system planning strategies do not pose undue risks or costs to the interests of customers and citizens of the Pacific Northwest.

The Office of Security and Continuity of Operation (OSCO) is accountable for the protection of BPA assets comprised of more than 300 facilities, with a total value estimated at \$4.9 billion dollars<sup>1</sup>. OSCO also provides protection and security to approximately 5,000 employees and contractors, as well as thousands of visitors each year. OSCO is ultimately responsible for the design and efficacy of the security infrastructure that must be compliant with ever-evolving regulatory requirements yet balanced with the operational needs and acceptance of the infrastructure owner (e.g., Transmission Services (TF)). Further, the proposed protection strategies must be included within the operations and maintenance scope of Information Technology (IT) and Facilities Asset Management (FAM) groups who are considered the “asset owners” of the individual components that make up the security system. Close to 100 facilities contain security systems, which require ongoing maintenance to ensure performance and protection standards are in line with security policies and compliance requirements. This number continues to grow with new BPA infrastructure construction and identification/categorization of new critical or high priority facilities that require protection.

Keeping a balance among risk-based protection programs, compliance driven initiatives and costs has been a growing challenge for BPA. Capital enhancements are dominated by methodologies prescribed by regulatory entities, leaving little room for risk-informed protection strategies or in response to reported security incidents.

Figure A. Evolution of Security



<sup>1</sup> Asset value is based on FY 2011 FCRPS – Combining Balance Sheets (Unaudited). Excludes costs outside the scope of the security program

## Purpose and Scope of Strategy

The purpose of BPA’s Security Infrastructure Asset Management Strategy is to integrate management of the security systems with prioritization and resourcing strategies that support BPA and stakeholder interests, while ensuring that the design, installation and maintenance of physical and personnel security systems for BPA’s critical infrastructure are consistent with 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.

The Security Infrastructure Asset Management Strategy will accomplish its objectives of *Compliance, Risk-Informed Protection, Security System Reliability and Cost Management* through a prioritized deployment of both initial security system installation as well as subsequent life-cycle maintenance to address the ever changing security threats and compliance requirements, while balancing sound business and asset management principles.

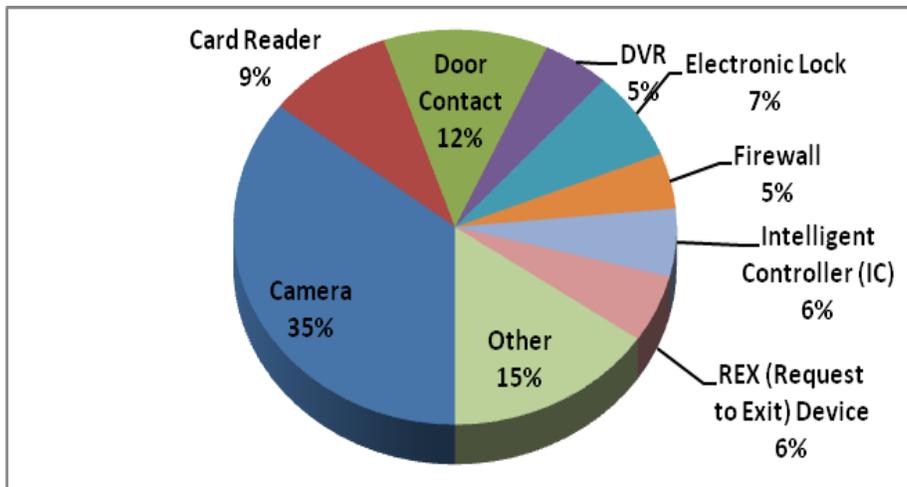
BPA defines a *security asset* as material, equipment, software or hardware that is used for the primary purpose of providing security. These assets or components make up systems that collectively provide various levels of physical security and personnel security as demonstrated by the table below.

**Table A. Systems and Component Overview**

| Systems                             | Purpose   | Asset Types Include   |   |
|-------------------------------------|---|---|---|
| <b>Protective Barrier</b>           | Provide a physical barrier between adversary and target. Protective barriers delay an adversary’s attempts to gain entry or cause damage to critical components.                              | <ul style="list-style-type: none"> <li>• Fence</li> <li>• Gate</li> <li>• Padlock</li> </ul>                                      | <ul style="list-style-type: none"> <li>• Chains</li> <li>• Barbed wire</li> <li>• Door</li> </ul>                               |
| <b>Access Control</b>               | Allow for logging and monitoring of access, as well as secure site so it is less prone to forced entry.   | <ul style="list-style-type: none"> <li>• Card reader</li> <li>• Door contact</li> </ul>   | <ul style="list-style-type: none"> <li>• Electronic locks</li> <li>• Magnetic lock</li> </ul>                                   |
| <b>Intrusion Detection</b>          | Provide warning of pending intrusion and notification of an intrusion by unauthorized people.   | <ul style="list-style-type: none"> <li>• Motion detectors</li> <li>• Fence detection systems</li> </ul>                           | <ul style="list-style-type: none"> <li>• Motion sensing cameras</li> </ul>  |
| <b>Surveillance</b>                 | Video surveillance systems allow for the real time viewing of activity as well as the ability to review activity in the past to assess alarms related to inputs.                              | <ul style="list-style-type: none"> <li>• Fixed cameras</li> <li>• PTZ cameras</li> </ul>  | <ul style="list-style-type: none"> <li>• DVR/NVR</li> <li>• Protective covers, domes</li> </ul>                                 |
| <b>Lighting</b>                     | Lighting used specifically to address a security need, whether after dark camera operation or to illuminate an area of security concern.  | <ul style="list-style-type: none"> <li>• Entrance or gates</li> <li>• Camera lights</li> </ul>                                    | <ul style="list-style-type: none"> <li>• Perimeter lights</li> <li>•</li> </ul>   |
| <b>Early Intrusion Detection</b>    | Extension of the intrusion detection system which includes capability to detect activity outside the perimeter of the facility and provides early warning of potentially malevolent activity. | <ul style="list-style-type: none"> <li>• High definition (HD), infrared (IR), motion detection (MD) video surveillance</li> </ul> | <ul style="list-style-type: none"> <li>• Seismic detection</li> <li>• Exterior MD</li> <li>• Outward facing lighting</li> </ul> |
| <b>IT Support Systems</b>           | Underlying IT infrastructure that supports security systems and information.  | <ul style="list-style-type: none"> <li>• Servers Network</li> </ul>   | <ul style="list-style-type: none"> <li>• Applications</li> <li>• Database</li> </ul>  |
| <b>Access Credentials</b>           | Ensures that only authorized individuals have access to BPA facilities, information, and assets.  | <ul style="list-style-type: none"> <li>• Local site security only (LSSO) badge</li> </ul>   | <ul style="list-style-type: none"> <li>• Smart Cards</li> </ul>   |
| <b>Access Credential Production</b> | Equipment that supports record storage and production requirements for access credentials.  | <ul style="list-style-type: none"> <li>• Printing station</li> <li>• Electric file system</li> </ul>                              | <ul style="list-style-type: none"> <li>• Light activation station</li> <li>• Finger print station</li> </ul>                    |
| <b>Screening</b>                    | Ensure that contraband such as weapons, firearms, controlled substances are not brought into BPA facilities.  | <ul style="list-style-type: none"> <li>• X ray machines</li> </ul>  | <ul style="list-style-type: none"> <li>• Metal detectors</li> </ul>   |
| <b>ER Equipment</b>                 | Supplies and materials that outfit first responders and building wardens with the tools to do their jobs during emergencies.  | <ul style="list-style-type: none"> <li>• Warden supplies (e.g. flashlights)</li> </ul>  | <ul style="list-style-type: none"> <li>• First responder supplies</li> </ul>  |

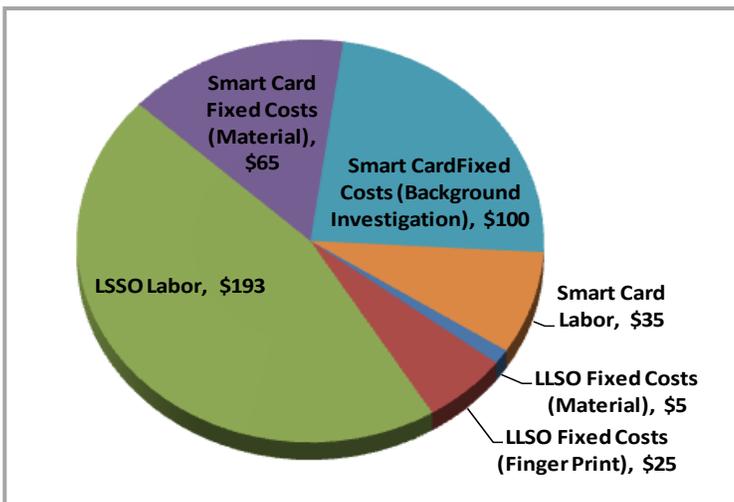
**Chart A. Physical Security System Chart A Components Overview by Type**  
 (Percentage based on total number of inventoried components)

BPA has undergone several waves of security enhancements which resulted in the deployment of physical security assets. Chart A depicts the array of physical security components currently being operated and maintained. Criticality of a system or component is determined by the impact of its failure on maintaining security compliance (e.g. NERC CIP, HSPD-12, etc.) and security system effectiveness (e.g.



identified by the System Performance Assurance Program (SPAP)). Currently, there are approximately 780 components that have been identified as critical for maintaining security compliance and security system effectiveness. Currently, 20 percent of total critical components are past their manufacturer’s recommended service life. By FY 2015, 100 percent will reach their mean-time-to-failure (MTTF) as the majority have an estimated service life of 5 years and were installed in FY 2009.

**Chart B. Smart Card Production Cost Detail**



In addition to physical security assets, BPA’s Office of Security and Continuity is managing more than 5,000 access credentials (i.e., Smart Cards) for BPA employees and contractors in support of HSPD-12 and NERC CIP. Additionally, there are approximately 1,300 local site security only (LSSO) access credentials that must be managed. Each Smart Card and LSSO has an initial production cost, as well as maintenance and replacement fees, which are supported by OSCOs budget. Smart Cards also have update and replacement cycles dictated by the General Services Administration (GSA). Under ideal conditions, a Smart Card costs \$311 to

produce. This amount includes the cost of initial LSSO badge as detailed in Chart B. The annual program cost is currently around \$330,000.

**Key Accomplishments and Historic Backdrop**

BPA has made great strides in strengthening its security posture by initiating several operational excellence projects, which include 1) organizational realignment supporting a newly developed security strategy; 2) process redesign to support security’s capital program; 3) creation of an IT support team dedicated to meeting ongoing needs of security as it transitions from mechanical and analog systems to IT based and network dependent systems; 4) improved security asset inventory tracking system allowing for better trending and maintenance planning. These initiatives, which will provide a long term benefit, did

require a temporary delay in starting the Tier II<sup>2</sup> critical infrastructure protection. This resulted in under spending of FY 2010 and FY 2011 security capital. In FY 2012, OSCO increased its rate of capital spending and began deploying the proof-of-concept for protecting Tier II level sites.

Prior to 2011, physical security system maintenance costs covered within OSCO’s security budget were limited to repairs and replacements completed in the Headquarters, Van Mall, and Ross Complex facilities. Substation security maintenance was managed by Transmission Services. In 2011, maintenance funding was made available to OSCO from Transmission Services security budget in support of security system performance testing and security system maintenance activities for the field sites. This change better aligns the security subject matter expertise with direct oversight of the security maintenance, design, performance testing, and vendor activities supporting a complex and ever-evolving security system.

**Chart C. Historic Physical Security System Maintenance**

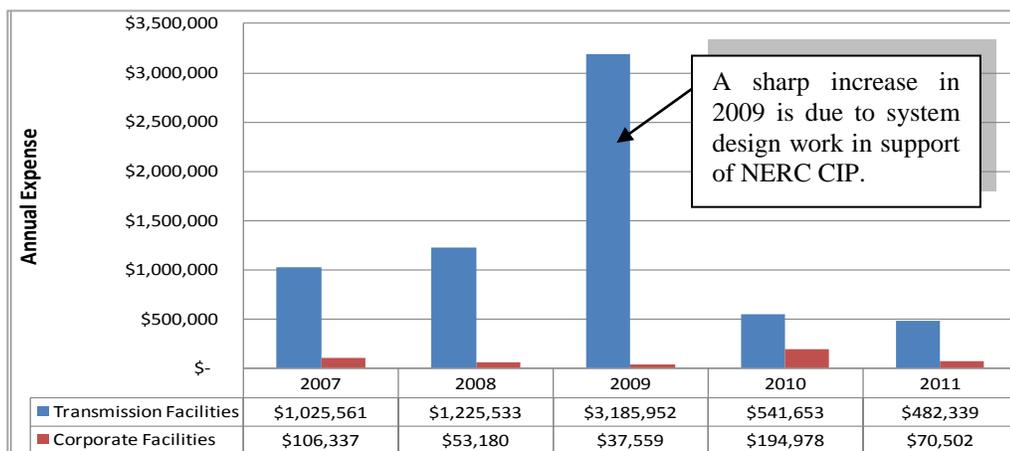


Chart C provides historic maintenance costs paid collectively by OSCO and Transmission for maintaining physical security systems. (Note: A sharp increase in 2009 is due to one-time system design work in support of NERC CIP.)

**Chart D. Historic Activity for Access Credentials**

As evident by Chart D, BPA has experienced an increase in the number of access credentials issued year-over-year as measured by the number of personnel identity verifications conducted. The primary driver behind this trend has been an increase in the number of contract staff supporting new transmission construction projects. This trend is expected to level out starting in FY2013.



**Drivers, Initiatives and Risks**

The drivers behind the asset strategy are protection requirements identified in the following BPA plans and policies:

<sup>2</sup> Tier II is a designation of level of criticality of the site in accordance with DOE’s graded security policy where Tier 1 is most critical and Tier IV is essential

- **Critical Asset Security Plan (CASP)** – The CASP integrates all security compliance requirements (i.e. NERC CIP, HSPD-12, DOE’s GSP) related to protection of critical infrastructure into a comprehensive implementation strategy.
- **System Performance Assurance, Component Testing and Preventative Maintenance Program (SPAP)** – In accordance with DOE O 473.3, the purpose of BPAs performance testing program is to ensure the 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.
- **Personal Identify Verification (PIV) and Personal Risk Assessment (PRA) Policy** – As required by HSPD-12, the intent of this policy is to ensure an entrusted workforce to protect BPA assets from harm or misuse.

Seven initiatives have been identified for meeting the strategic objectives and reducing variety of risks. Table B summarizes each initiative qualified by the risk exposure from forgoing or delaying implementation.

**Table B. Strategic Initiatives, Risks and Costs**

| Drivers  | Initiatives  | Risks of Foregoing Implementation   | 10 Year Cost<br>Capital / Expense |          |
|--|--|---|-----------------------------------|----------|
| <b>BPA Critical Asset Security Plan (CASP)</b> | <b>1. Compliance</b><br>Ensure compliance with security regulation by applying mandatory security enhancements as required by NERC, DHS, DOE, etc.   | <b>Financial and Reputational Risk Due to Regulatory Non-Compliance:</b> Findings by regulatory entities within one year leading to a) possible financial sanctions, b) mandated policy changes and c) public criticism.  | \$7.33 M                          | \$0.08 M |
|  | <b>2. Critical Infrastructure Protection</b><br>Installation of security systems designed to provide the appropriate level of protection for critical infrastructure with a Tier I <sup>3</sup> , Tier II or Tier III criticality level designation. | <b>Financial and Operational Risk Due to Terrorist/Criminal Activity:</b> Continual exposure to “medium risk <sup>4</sup> ” 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. | \$36.09 M                         |          |

<sup>3</sup> Tier II is a designation of level of criticality of the site in accordance with DOE’s graded security policy where Tier I is most critical and Tier IV is essential

<sup>4</sup> DHS has 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.

|   |  |   |                      |                      |
|---|--|---|----------------------|----------------------|
|   | <p><b>3. Essential Infrastructure Protection</b><br/>Improving or enhancing security systems at essential sites using risk informed protection strategies to address security threats and gain efficiencies.</p>   | <p><b>Financial and Operational Risk Due to Criminal Activity:</b> a) Increased exposure to criminal activity and potential collateral damage impacting Bulk Electrical System (BES). Historically, this costs the Agency \$270,000 per year<sup>5</sup> on the low range, as well as risks system reliability by the possibility of collateral damage to transmission equipment during an incident such as vandalism or theft.<br/>b) Inability to replace or update obsolete security systems compromising protection of essential facilities such as the Headquarter building.<br/>c) Using more costly guard force contract labor to protect facilities as apposed to automated systems which cost less over time and provide equal or greater level of protection.</p> | <p>\$3.80 M</p>      |                      |
| <p><i>BPA System Performance Assurance, Testing and Preventative Maintenance Program (SPAP)</i></p> | <p><b>4. Performance Testing &amp; Preventative Maintenance</b><br/>Annual assessment of security systems through performance tests, leading to repair or replacement of components that may impact security system reliability or compliance.</p>   | <p><b>Financial and Reputational Risk Due to Inadequate Maintenance:</b> 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.</p>  |                      | <p>\$1.54 M</p>      |
|   | <p><b>5. Replacement &amp; Renewal Program</b><br/>Replacement of critical components in anticipation of failure<sup>6</sup>. Replacement upon failure of non-critical components. Strategic phase-out of components no longer technological viable (e.g., analog to digital conversion).</p>    | <p><b>Operational and Reputational Risk Due to Inadequate Maintenance:</b> Failing or faulty security systems and equipment leading to a) compromised protection of critical infrastructure; b) strain on limited resources to support O&amp;M activity; and c) criticism by regulatory entities due to unplanned outages of critical security systems.</p>   | <p>\$1.90 M</p>      | <p>\$5.23 M</p>      |
|   | <p><b>6. System Reliability &amp; Efficiency Projects</b><br/>Ensure security system reliability and efficient operation through projects designed to close gaps identified by technical team (e.g. Uninterruptable Power Systems (UPS)), implement automation project to gain efficiencies.</p> | <p><b>Operational and Reputational Risk Due to Inadequate Maintenance:</b> Gaps in current systems and processes preventing or delaying execution of implementation or O&amp;M projects to address weaknesses in the current security infrastructure. This can result in a) compromised protection of critical infrastructure; and b) criticism by regulatory entities due to failure of critical security system.</p>  |                      | <p>\$0.39 M</p>      |
| <p><i>BPA PIV and PRA Policy</i></p>  | <p><b>7. Access Credentials (Smart Cards)</b><br/>Continually assess, forecast and plan for fluctuations in Smart Card activity, with focus on risk mitigation and uninterrupted access of cleared workforce.</p>  | <p><b>Operational and Reputational Risk Due to Inadequate Maintenance:</b> Exposure of BPA people, critical assets, facilities and information to access by individuals with intent to harm or misuse them. Risk of being non-compliant with HSPD-12 and NERC CIP resulting in severe, observable impact and orders for substantial corrective action, including some mandatory changes in BPA operation or administration.</p>   |                      | <p>\$3.93 M</p>      |
| <b>TOTAL</b>  |  |   | <p><b>\$50 M</b></p> | <p><b>\$11 M</b></p> |

**Prioritization**

All initiatives are prioritized so that once all mandated compliance obligations are met, the focus is on risk-informed protection.

<sup>5</sup> Annual loss of \$270,000 is calculated using total reported loss of \$2.2 million in eight years. Loss value excludes labor.

<sup>6</sup> Life cycle based on manufacturer recommendations and fail rates.

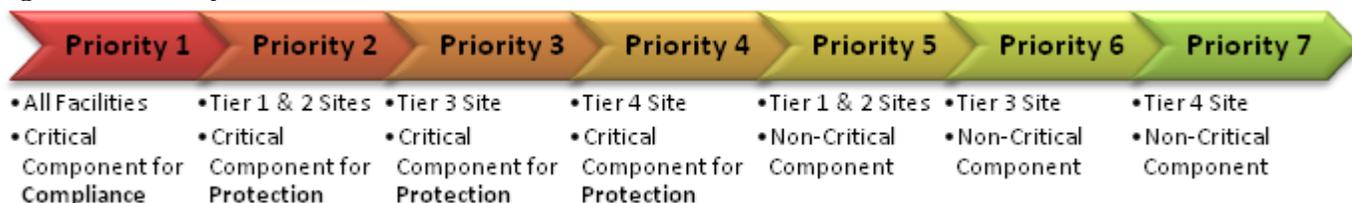
When prioritizing risk-informed capital investment, three factors are considered:

- The criticality of the facility as measured by the impact of its loss on BPA’s ability to achieve its mission.
- Real-time security threat information.
- Efficiencies to be gained by investment

This strategy provides flexibility to maneuver in an environment where the security conditions are ever-changing, yet ensures that assets are protected commensurate with the level of criticality. Dedicating a fraction of the budget to efficiency measures allows OSCO to manage increasing costs and minimize the impact on the rate payers.

Maintenance activities are also prioritized by the level of criticality of the facility as well as the criticality of the protection system or component. Criticality of a system or component is determined by the impact of its failure on maintaining security compliance (e.g. NERC CIP, HSPD-12, etc.) and security system effectiveness (e.g. identified by the SPAP). Figure C shows the maintenance and upgrade priority matrix.

**Figure C. Priority Matrix**



**Approved Capital Plan for FY 2012 - FY 2021**

The capital funding approved during the FY 2010 planning cycle was insufficient to meet minimum compliance requirements as proposed by the NERC CIP version 5. In anticipation of this requirement, OSCO recommended reshaping the base over 10 years and adding another \$10 million dollars to the base to meet the compliance obligation and sustain protection initiatives. The recommendation was approved following the FY 2012 Capital Investment Review (CIR) process and provided funding for the initiatives identified in Table C:

**Table C. Capital Plan Approved During CIR(\$000s)**

|                                   | FY 2012      | 2013         | 2014          | 2015         | 2016         | 2017         | 2018         | 2019         | 2020         | 2021         | Total         |
|-----------------------------------|--------------|--------------|---------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|---------------|
| Tier II Critical Site Protection  | 2,900        | 3,377        | 4,153         | 3,200        | 5,887        | 7,070        | 5,710        | 4,145        | -            | -            | 36,442        |
| Tier III Critical Site Protection | -            | -            | -             | -            | -            | -            | -            | -            | 1,000        | 1,000        | 2,000         |
| NERC CIP Version 2 & 3 (NOAV)     | 450          | -            | -             | -            | -            | -            | -            | -            | -            | -            | 450           |
| NERC CIP Version 2 & 3            | 840          | 800          | -             | -            | -            | -            | -            | -            | -            | -            | 1,640         |
| NERC CIP Version 4                | -            | 4,125        | -             | -            | -            | -            | -            | -            | -            | -            | 4,125         |
| NERC CIP Version 5                | -            | -            | 12,500        | -            | -            | -            | -            | -            | -            | -            | 12,500        |
| Essential Sites Protection        | -            | 500          | 500           | -            | 500          | 500          | 500          | 500          | -            | 500          | 3,500         |
| Capital update of failing systems | -            | -            | -             | 900          | -            | -            | -            | -            | 1,000        | -            | 1,900         |
| <b>TOTAL CAPITAL</b>              | <b>4,190</b> | <b>8,802</b> | <b>17,153</b> | <b>4,100</b> | <b>6,387</b> | <b>7,570</b> | <b>6,210</b> | <b>4,645</b> | <b>2,000</b> | <b>1,500</b> | <b>62,557</b> |

**Optimized Capital Plan for FY 2012 - FY 2021**

Since the recommendation of the model in Table D, there have been several new developments influencing OSCO’s capital forecast for FY 2013 through FY 2015. The first and most significant is that the NERC, in its most recent release of CIP Version 5, has omitted the requirement that all openings of 96 square inches or greater be secured. This one change will save BPA an estimated \$12.5 million in FY

2015. NERC's decision is believed to be influenced by the comments received from BPA and other utilities.

In addition to returning \$12.5 million, we propose to reshape the current capital funding for the period of FY 2013 through FY 2015 to:

- Fund an enhanced security protective system for the Munro Complex, a Tier I critical asset. By adopting a risk-informed security approach that encompasses the Munro Complex instead of each building separately, the Agency will avoid approximately \$250,000 in annual costs, realizing a savings in three years.
- Validate the proof of concept for the Tier II critical asset protection solution deployed at our Raver Substation in FY 2012.
- Provide necessary funding to automate the Ross Complex main entries. This automation will improve the current security posture and is estimated to save BPA \$250,000 of expense annually, realizing a return on investment in just over one year.

The table D shows the approved and optimized funding models side-by-side, with a net delta of \$12.5 million.

**Table D. Optimized Capital Plan (\$000s) – \$12.5 million reduction and reshaping FY 2013-FY 2015**

|                                      | Budget       | Actual       | Approved     | Proposed     | Approved      | Proposed     | Approved     | Proposed     | Approved      | Proposed      |
|--------------------------------------|--------------|--------------|--------------|--------------|---------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|---------------|---------------|
| Approved Budget (000's)              | 4,190        |              | 8,802        |              | 17,153        |              | 4,100        |              | 6,387        | 7,570        | 6,210        | 4,645        | 2,000        | 1,500        | 62,557        |               |
| FY                                   | 2012         | 2012         | 2013         | 2013         | 2014          | 2014         | 2015         | 2015         | 2016         | 2017         | 2018         | 2019         | 2020         | 2021         | Total         | Total         |
| Tier I Critical Site Protection      | -            | -            | -            | 300          | -             | 450          | -            | -            | -            | -            | -            | -            | -            | -            | -             | 750           |
| Tier II Critical Site Protection     | 2,900        | 2,819        | 3,377        | 200          | 4,153         | -            | 3,200        | 7,507        | 5,887        | 7,070        | 5,710        | 4,145        | -            | -            | 36,442        | 33,338        |
| Tier III Critical Site Protection    | -            | -            | -            | -            | -             | -            | -            | -            | -            | -            | -            | -            | 1,000        | 1,000        | 2,000         | 2,000         |
| NERC CIP Version 2 & 3 (NOAV)        | 450          | 431          | -            | -            | -             | -            | -            | -            | -            | -            | -            | -            | -            | -            | 450           | 431           |
| NERC CIP Version 2 & 3               | 840          | 2            | 800          | 4,347        | -             | -            | -            | -            | -            | -            | -            | -            | -            | -            | 1,640         | 4,349         |
| NERC CIP Version 4                   | -            | -            | 4,125        | -            | -             | 2,551        | -            | -            | -            | -            | -            | -            | -            | -            | 4,125         | 2,551         |
| NERC CIP Version 5                   | -            | -            | -            | -            | 12,500        | -            | -            | -            | -            | -            | -            | -            | -            | -            | 12,500        | -             |
| Essential Infrastructure Protection  | -            | -            | 500          | 800          | 500           | 500          | -            | -            | 500          | 500          | 500          | 500          | -            | 500.00       | 3,500         | 3,800         |
| Capital update of failing systems    | -            | -            | -            | -            | -             | -            | 900          | 900          | -            | -            | -            | -            | 1,000        | 0            | 1,900         | 1,900         |
| <b>TOTAL CAPITAL</b>                 | <b>4,190</b> | <b>3,252</b> | <b>8,802</b> | <b>5,647</b> | <b>17,153</b> | <b>3,501</b> | <b>4,100</b> | <b>8,407</b> | <b>6,387</b> | <b>7,570</b> | <b>6,210</b> | <b>4,645</b> | <b>2,000</b> | <b>1,500</b> | <b>62,557</b> | <b>50,057</b> |
| <i>Delta (approved vs. proposed)</i> |              |              |              | -3,155       |               | -13,652      |              | 4,307        | -            | -            | -            | -            | -            | -            | -             | -12,500       |

### **Expense Plan for FY 2012 - FY 2021**

The expense budget has also been influenced by recent developments, including:

- Mandatory card reader upgrades required to meet new HSPD-12 compliance.
- Increase in the number of annual site visits and performance tests due to a more inclusive definition of what is considered a critical asset under NERC CIP Version 4.
- Increasing cost of replacement components.
- Vendor contract re-compete influencing earlier estimates<sup>7</sup>.

The expense budget as originally proposed called for total funding of \$11.0 million through FY 2021, assuming that system-wide upgrades could not be capitalized and \$9.2 million if the upgrade could be capitalized. The current estimate, which includes the added compliance requirements, is \$11.2 million. It also shows that camera upgrades scheduled for FY 2015 and FY 2020 cannot be capitalized as previously assumed. The \$156,000 shortfall from current funding (based on original proposal) will be covered by

<sup>7</sup> Vendor pricing is still subject to change as the contract has not yet been awarded.

Transmission's field security maintenance budget. This budget is traditionally held for repairs caused by malicious activity and to offset increasing cost of security requirements similar to those impacting OSCO's expense budget now.

**Table E. Expense Plan for FY 2012 – FY 2021(\$000s): UPDATED**

| FY                                | 2012  | 2013  | 2014 | 2015  | 2016 | 2017 | 2018  | 2019  | 2020  | 2021  | Total  |
|-----------------------------------|-------|-------|------|-------|------|------|-------|-------|-------|-------|--------|
| Compliance                        | 43    | 37    | -    | -     | -    | -    | -     | -     | -     | -     | 80     |
| Performance Testing & Maintenance | 38    | 157   | 137  | 157   | 163  | 167  | 172   | 177   | 183   | 188   | 1,539  |
| Replacement Upon Failure          | 228   | 200   | 211  | 190   | 197  | 202  | 209   | 215   | 222   | 229   | 2,103  |
| Planned Replacement               | 162   | 232   | 212  | 406   | 52   | 200  | 217   | 224   | 400   | 237   | 2,342  |
| Tier 2 Maintenance                | -     | -     | -    | 5     | 10   | 40   | 110   | 95    | 255   | 265   | 780    |
| System Reliability Projects       | 287   | 100   | -    | -     | -    | -    | -     | -     | -     | -     | 387    |
| Physical Security Subtotal        | 758   | 726   | 560  | 758   | 422  | 609  | 708   | 711   | 1,060 | 919   | 7,231  |
| Personnel Security Subtotal       | 330   | 350   | 340  | 580   | 450  | 390  | 370   | 370   | 340   | 410   | 3,930  |
| Grand Total                       | 1,088 | 1,076 | 900  | 1,338 | 872  | 999  | 1,078 | 1,081 | 1,400 | 1,329 | 11,161 |

If OSCO had to operate within the initial baseline, the added cost for mandatory HSPD-12 updates, site visits and performance tests would be covered by delaying planned replacement of those components beyond the manufacture recommended shelf life, which would impact OSCO's ability to manage spending due to costly vendor call outs.

### **Summary**

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. Compared to the initial draft proposal, the capital spending has been reduced by \$12.5 million. A \$156,000 increase in the expense budget due to new compliance requirement has been absorbed by reprioritizing security related funding across BPA with minimal risk.

# 1. Asset Management Objectives, Scope and Strategic Direction

---

## 1.1. Objectives

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, to ensure 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.
- **Security System Reliability** – Installed systems are assessed and maintained on a regular basis to mitigate the risk of unplanned security system outages or failures that could result in compromised protection or compliance violations.
- **Cost Management** – Program costs are managed to minimize impact on rate payers.

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

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

## 1.2. Service Provided

Transmission Services is a primary client of OSCO. Although more than 90 percent of maintenance activities and budget are dedicated to supporting critical transmission infrastructure protection and issuance of access credentials (LSSOs and Smart Cards) to Transmission workforce, BPA has dedicated resources for Tier IV essential facilities such as the Headquarters building, Ross Complex, Van Mall, Eugene Starr Complex, etc.

Security assets provide the following services to its 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
- Emergency and evacuation aid

### 1.3. Strategy

The strategy for achieving the goals of *Compliance, Risk-Informed Protection, Security System Reliability and Cost Management* is the prioritized implementation of protection requirements identified in the following BPA plans and policies:

- **Critical Asset Security Plan (CASP)** – The CASP integrates all security compliance requirements (i.e. NERC CIP, HSPD-12, DOE’s GSP) related to protection of critical infrastructure into a comprehensive implementation strategy.
- **System Performance Assurance, Component Testing and Preventative Maintenance Program (SPAP)** – In accordance with DOE O 473.3, the purpose of BPA’s performance testing program is to ensure the security systems are tested and maintained on a regular basis, with corrective maintenance addressed commensurate with the level of criticality of system and location of system.
- **Personal Identify Verification (PIV) and Personal Risk Assessment (PRA) Policy** – As required by HSPD-12 and NERC CIP standards, the intent of this policy is to ensure an entrusted workforce to protect BPA assets from harm or misuse.

Strategic initiatives to meet the asset management objectives are identified in Table 2, qualified by risks associated with foregoing implementation.

*Table 1. Strategic Initiatives, Risks Addressed and Costs*

| Drivers  | Initiatives  | Risks of Foregoing Implementation   | 10 Year Cost Capital / Expense |          |
|--|--|---|--------------------------------|----------|
| <b>BPA Critical Asset Security Plan (CASP)</b> | <b>1. Compliance</b><br>Ensure compliance with security regulation by applying mandatory security enhancements as required by NERC, DHS, DOE, etc.   | <b>Financial and Reputational Risk Due to Regulatory Non-Compliance:</b> Findings by regulatory entities within one year leading to a) possible financial sanctions, b) mandated policy changes and c) public criticism.  | \$7.33 M                       | \$0.08 M |
|  | <b>2. Critical Infrastructure Protection</b><br>Installation of security systems designed to provide the appropriate level of protection for critical infrastructure with a Tier I <sup>8</sup> , Tier II or Tier III criticality level designation. | <b>Financial and Operational Risk Due to Terrorist/Criminal Activity:</b> Continual exposure to “medium risk <sup>9</sup> ” 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. | \$36.09 M                      |          |

<sup>8</sup> Tier II is a designation of level of criticality of the site in accordance with DOE’s graded security policy where Tier I is most critical and Tier IV is essential

<sup>9</sup> DHS has 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) | <p><b>3. Essential Infrastructure Protection</b><br/>                 Improving or enhancing security systems at essential sites using risk informed protection strategies to address security threats and gain efficiencies.</p>  | <p><b>Financial and Operational Risk Due to Criminal Activity:</b> a) Increased exposure to criminal activity and potential collateral damage impacting Bulk Electrical System (BES). Historically, this costs the Agency \$270,000 per year<sup>10</sup> on the low range, as well as risks system reliability by the possibility of collateral damage to transmission equipment during an incident such as vandalism or theft.<br/>                 b) Inability to replace or update obsolete security systems compromising protection of essential facilities such as the Headquarter building.<br/>                 c) Using more costly guard force contract labor to protect facilities as apposed to automated systems which cost less over time and provide equal or greater level of protection.</p> | \$3.80 M |          |          |
|   | <p><b>4. Performance Testing &amp; Preventative Maintenance</b><br/>                 Annual assessment of security systems through performance tests, leading to repair or replacement of components that may impact security system reliability or compliance.</p>  | <p><b>Financial and Reputational Risk Due to Inadequate Maintenance:</b> 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.</p>   |          | \$1.54 M |          |
|   | <p><b>5. Replacement &amp; Renewal Program</b><br/>                 Replacement of critical components in anticipation of failure<sup>11</sup>.<br/>                 Replacement upon failure of non-critical components. Strategic phase-out of components no longer technological viable (e.g., analog to digital conversion).</p> | <p><b>Operational and Reputational Risk Due to Inadequate Maintenance:</b> Failing or faulty security systems and equipment leading to a) compromised protection of critical infrastructure; b) strain on limited resources to support O&amp;M activity; and c) criticism by regulatory entities due to unplanned outages of critical security systems.</p>  | \$1.90 M | \$5.23 M |          |
|   | <p><b>6. System Reliability &amp; Efficiency Projects</b><br/>                 Ensure security system reliability and efficient operation through projects designed to close gaps identified by technical team (e.g. Uninterruptable Power Systems (UPS)), implement automation project to gain efficiencies.</p>                    | <p><b>Operational and Reputational Risk Due to Inadequate Maintenance:</b> Gaps in current systems and processes preventing or delaying execution of implementation or O&amp;M projects to address weaknesses in the current security infrastructure. This can result in a) compromised protection of critical infrastructure; and b) criticism by regulatory entities due to failure of critical security system.</p>   |          |          | \$0.39 M |

<sup>10</sup> Annual loss of \$270,000 is calculated using total reported loss of \$2.2 million in eight years. Loss value excludes labor.

<sup>11</sup> Life cycle based on manufacturer recommendations and fail rates.

|                               |   |   |              |               |
|-------------------------------|---|---|--------------|---------------|
| <i>BPA PIV and PRA Policy</i> | <p><b>7. Access Credentials (Smart Cards)</b><br/>Continually assess, forecast and plan for fluctuations in Smart Card activity, with focus on risk mitigation and uninterrupted access of cleared workforce.</p> | <p><b>Operational and Reputational Risk Due to Inadequate Maintenance:</b> Exposure of BPA people, critical assets, facilities and information to access by individuals with intent to harm or misuse them. Risk of being non-compliant with HSPD-12 and NERC CIP resulting in severe, observable impact and orders for substantial corrective action, including some mandatory changes in BPA operation or administration.</p> |              | \$3.93 M      |
|                               |   |   | <b>TOTAL</b> | <b>\$50 M</b> |

## 2. Asset Category Overview

---

### 2.1. Definition

Unlike most assets, security assets are owned by other organizations. The assets collectively make up security systems and overarching security infrastructure, with OSCO providing oversight and security expertise. In some cases, such as Smart Cards, an external organization dictates the maintenance requirements, and BPA's business needs drive the volume, while OSCO budgets and plans for production and maintenance activities.

OSCO is ultimately accountable for the security infrastructure performance and its strategic deployment to provide the most effective protection for Agency assets. For this purpose, OSCO has the responsibility of development of the asset management strategy to the reliability of the system.

For the purpose of this document, a **security asset** is defined as material, equipment, software or hardware that is used for the primary purpose of providing security.

Information Technology systems (e.g., network infrastructure, servers, software, etc.) are currently covered under IT asset management strategies. These systems are considered outside the scope of this document.

### 2.2. Inventory Management

To better forecast, manage and coordinate maintenance activities, BPA initiated an effort to develop a security asset tracking system. Phase 1 of this effort was completed in FY2011 by cataloging each component in a SharePoint inventory list. This allowed for better tracking of associated maintenance activities. Collection of data, such as installation date, life cycle, component criticality rating and replacement cost allowed for better planning and projection of future cost estimates.

Figure 1 below shows some of the categories tracked for each component.

**Figure 1. Inventory categories**

| Description & Technical Details  | Maintenance Requirements   | Performance Test History  |
|--|--|---|
| <ul style="list-style-type: none"> <li>• ID</li> <li>• Site</li> <li>• Location</li> <li>• Item Category</li> <li>• Manufacturer</li> <li>• Model</li> <li>• Serial #</li> <li>• Description</li> <li>• IP Address</li> <li>• Status</li> <li>• Asset Tag</li> </ul> | <ul style="list-style-type: none"> <li>• Install Date</li> <li>• Out of Warranty Date</li> <li>• Replacement Cost</li> <li>• Expected Life Cycle</li> <li>• Year product is past its life cycle</li> </ul> | <ul style="list-style-type: none"> <li>• Asset Owner</li> <li>• Site Criticality</li> <li>• PM Required</li> <li>• Perf. Test Date</li> </ul> |

Nearly 2,000 components are categorized by criticality in accordance with the Security Performance Assurance Program, which helps support the prioritization strategy for future maintenance and replacement.

To continue to build on this foundation, OSCO in partnership with IT has initiated a joint effort to automate security asset tracking which will allow for:

- Integration of maintenance data in support of better trending, planning, and calculating mean time to failure (MTF) based on BPA use.
- When practical, integration with Transmission service cycles.

- Prioritization of strategic replacement of critical components near end of life cycle to prevent unplanned outages and reduce the risk of compliance violations.

Until an automated solution is available, the current database will serve as the official repository and will be used to track the changing condition of each asset over time.

### 2.3. 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 1 describes typical systems and components within those systems:

**Table 2. 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  |
|----------------------------|--|--|---|---------------|
| <b>Protective Barrier</b>  | 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.   | <ul style="list-style-type: none"> <li>• Fence</li> <li>• Gate</li> <li>• Padlock</li> <li>• Chains</li> <li>• Barbed wire</li> <li>• Door</li> <li>• Bullet resistant glass</li> <li>• Window protection</li> <li>• Vehicle Barriers</li> </ul> | <ul style="list-style-type: none"> <li>• Low maintenance</li> <li>• Long life-cycle</li> <li>• Generally not replaced in its entirety. Usually repairs and upkeep involve small sections of fence, gate repair, etc.</li> <li>• O&amp;M is low, but replacement of an entire fence or gate can be very high.</li> </ul> | FAM           |
| <b>Access Control</b>      | <p>Access control systems provide multiple functions:</p> <ul style="list-style-type: none"> <li>• Provide records of who and when people access a facility</li> <li>• Increase security by decreasing the number of hard keys in circulation</li> <li>• Decrease the vulnerability of door lock mechanisms because card key electronic locks are less prone to forced entry</li> <li>• Reduces vulnerability by immediately deactivating card keys that are lost or stolen and reduces the requirement to change locks after hard keys are lost.</li> </ul> <p>Access controls support NERC CIP compliance for monitoring and logging access.</p> | <ul style="list-style-type: none"> <li>• Card reader</li> <li>• Door contact</li> <li>• Electronic locks</li> <li>• Magnetic lock</li> <li>• Request to exit sensors</li> <li>• Associated wiring, circuitry, and power supplies</li> </ul>      | <ul style="list-style-type: none"> <li>• Medium maintenance</li> <li>• Long life cycle</li> <li>• Low replacement costs</li> <li>• Electro mechanical locking mechanisms require most frequent service visits dependent of frequency of use</li> </ul>  | FAM<br>IT-NJS |
| <b>Intrusion Detection</b> | Intrusion detection systems are intended to provide 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 supports NERC CIP compliance by  | <ul style="list-style-type: none"> <li>• Motion detectors</li> <li>• All “access control” components</li> <li>• Fence detection systems</li> <li>• Motion sensing cameras</li> <li>• Motion activated lights</li> </ul>                          | <ul style="list-style-type: none"> <li>• Maintenance varies by component, but most will fall between Low/Medium</li> <li>• Medium lifecycle</li> <li>• Low costs with the exception of a few select</li> </ul>  | IT-NJS        |

|                                     |  |   |   |
|-------------------------------------|--|---|---|
|                                     | <p>monitoring for and detecting unauthorized access. Intrusion detection supports faster and more effective law enforcement response.</p>  | <ul style="list-style-type: none"> <li>• Tamper alarms</li> </ul>   | <p>cameras and fence detection systems</p> <ul style="list-style-type: none"> <li>• Camera O&amp;M will be noted in Surveillance section.</li> </ul>  |
| <b>Surveillance</b>                 | <p>Surveillance systems are used in connection with intrusion detection, and access control systems. Video surveillance systems allow for the real time viewing and assessment of activity as well as the ability to review activity in the past to assess alarms related to inputs from the access control systems and the intrusion detection systems. The information provided is vital to an informed decision regarding response to a facility.</p> | <ul style="list-style-type: none"> <li>• Fixed cameras</li> <li>• PTZ cameras</li> <li>• DVR/NVR</li> <li>• Mounting structures, hardware, wiring, and circuitry</li> <li>• Protective covers, domes</li> </ul>   | <ul style="list-style-type: none"> <li>• High maintenance</li> <li>• Short/Medium life-cycle</li> <li>• High replacement costs (as a system, i.e., multiple cameras + NVR, and peripherals)</li> <li>• Individually, cameras/DVRs are not significantly high cost.</li> </ul> <p>IT-NJS</p> |
| <b>Lighting</b>                     | <p>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.</p>  | <ul style="list-style-type: none"> <li>• Entrance or gates</li> <li>• Camera lights</li> <li>• Perimeter lights</li> <li>• Special area lights</li> </ul>   | <ul style="list-style-type: none"> <li>• Medium maintenance</li> <li>• Short life cycle for conventional lights.</li> <li>• Long life cycle for modern technology such as LED.</li> <li>• Medium replacement cost</li> </ul> <p>FAM</p>   |
| <b>Early Intrusion Detection</b>    | <p>Early intrusion detection is an extension of the intrusion detection system. This includes capability to detect activity outside the perimeter of the facility and provide early warning of potentially malevolent activity.</p>  | <ul style="list-style-type: none"> <li>• High definition (HD), infrared (IR), motion detection (MD) video surveillance and detection systems:</li> <li>• Seismic detection</li> <li>• Exterior MD</li> <li>• Outward facing lighting</li> </ul>   | <ul style="list-style-type: none"> <li>• High maintenance</li> <li>• Short life cycle</li> <li>• Individual replacement cost is moderate</li> </ul> <p>IT-NJS<br/>FAM</p>   |
| <b>IT Support System</b>            | <p>Underlying IT infrastructure that supports security systems and information.</p>  | <ul style="list-style-type: none"> <li>• Servers (Primary and Failover)</li> <li>• Network (LAN/WAN)</li> <li>• Applications (ProWatch &amp; Rapid Eye)</li> <li>• Database &amp; Backup</li> <li>• ProWatch Reporting Information Security &amp; Compliance Monitoring (i.e., RSA, Tripwire, Firewalls)</li> </ul> | <ul style="list-style-type: none"> <li>• Maintenance for these systems is covered under the IT Asset Management Plan</li> </ul> <p>IT-NJS/<br/>NJSO/<br/>NJNN</p>   |
| <b>Access Credentials</b>           | <p>Ensures that only authorized individuals have access to BPA facilities, information, and assets.</p>  | <ul style="list-style-type: none"> <li>• LSSOs</li> <li>• Smart Cards</li> </ul>  | <ul style="list-style-type: none"> <li>• Low maintenance</li> <li>• Short life-cycle</li> <li>• Low replacement cost</li> </ul> <p>OSCO</p>   |
| <b>Access Credential Production</b> | <p>Equipment that supports record storage and production requirements for access credentials.</p>  | <ul style="list-style-type: none"> <li>• Printing station</li> <li>• Electriever file system</li> <li>• Light activation station</li> <li>• Finger print station</li> </ul>   | <ul style="list-style-type: none"> <li>• Low maintenance</li> <li>• Long life-cycle</li> <li>• High replacement cost</li> </ul> <p>OSCO<br/>FAM</p>   |
| <b>Screening</b>                    | <p>Ensure that contraband such as weapons, firearms, controlled substances are not brought into BPA facilities.</p>  | <ul style="list-style-type: none"> <li>• X ray machines</li> <li>• Metal detectors</li> </ul>   | <ul style="list-style-type: none"> <li>• Low maintenance</li> <li>• Long life-cycle</li> <li>• High replacement cost</li> </ul> <p>OSCO</p>   |
| <b>ER Equipment</b>                 | <p>Supplies and materials that outfit first responders and building wardens with the necessary tools to do their jobs during emergencies.</p>  | <ul style="list-style-type: none"> <li>• Warden supplies (e.g. vests, flashlights, etc.)</li> <li>• First responder supplies</li> <li>• Emergency supply lockers</li> </ul>   | <ul style="list-style-type: none"> <li>• Low maintenance</li> <li>• Short life cycle</li> <li>• Low replacement cost</li> </ul> <p>OSCO</p>   |

## 2.4. Roles and Responsibilities

Managing these services requires a coordinated effort between OSCO, Transmission Services, Facilities and IT. With rapid evolution of the security system from analog to digital, BPA has established a specialized team within IT's NJS organization, called ITPACS, whose primary function is to support IT-based security systems and applications. High-level roles and responsibilities for each organization are listed below.

### *OSCO*

---

- Development of requirements based on protection priorities and compliance obligations
- System testing
- Design review and approval
- Overall system accountability
- Information owner
- Identification, prioritization and tracking of corrective actions
- Liaise/consult with TS, FAM and ITPACS to ensure security systems and designs meet all compliance requirements
- Administrative operation of access control system
- Identity verification and personnel risk assessments
- Issuance and accountability of access credentials
- COTR responsibilities in support of transmission projects affecting security systems
- Budget management
- Business case development and approval

### *ITPACS*

---

- Implement quality assurance standards and procedures (projects & enhancements)
- Ensure quality control of installed security system components (break fix & installations)
- Ensure security system interoperability, reliability and performance
- Software application maintenance, development and support
- Cyber security management, audit and compliance (e.g., BPA IT, FISMA, NERC CIP, OIG)
- Vendor management and contracts (i.e., invoice, statement of work, RFP)
- Operations and maintenance, as well as research and development of systems and components in Table 2, where ITPACS is identified as the asset owner (e.g. cameras, DVRs, access control system components, communication systems, etc.)
- Address corrective actions identified by OSCO
- COTR duties, including those with security vendors in relation to maintenance activities
- Design change review and approval (Information System Owner/System Security Manager)

### *Transmission Services*

---

- Identify and prioritize critical infrastructure
- Assist with prioritization of project completion
- Assist with funding
- Ensure that all new construction or any transmission construction project is designed and funded with security requirements in mind

### *Facilities Asset Management*

---

- Operations and maintenance of systems and components in Table 2, 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
- Design review and approval where FAM assets are involved

*Maintenance Vendor (works with ITPACS)*

- Annual maintenance of security system
- Break/fix based on ITPACS COTR call-out
- NERC CIP upgrades (card readers, UPS, visitor access, etc.)
- Address corrective actions issued by OSCO

*Installation Vendor (Works with ITPACS, OSCO, FAM, and Transmission)*

- Installation of security enhancements based on approved design
  - New builds
  - Transmission projects (seismic upgrades)
  - NERC CIP upgrades (card readers, UPS, visitor access, etc.)
- Provide updated blue prints (post installation)

*Design Vendor (Works with ITPACS, OSCO, FAM, and Transmission)*

- Provides security design based on BPA construction standards and requirements provided by ITPACS, Transmission Services, Facilities and OSCO.

## 2.5. Summary of Critical Infrastructure, Systems and Components

### 2.5.1. 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 IV ranking, depending on security risk assessments and conditions.

*Table 3. Infrastructure Criticality Ranking*

| Criticality Ranking    | Facility                  | Protection Requirements   |
|------------------------|---------------------------|---|
| Tier I                 | Control Centers           | Armed guards, perimeter protection, access control, visitor control   |
| Tier II                | Most Critical Substations | Robust fence, early detection, intrusion detection, surveillance, communication, and access & visitor control |
| Tier III <sup>12</sup> | Critical Substation       | Robust fence, intrusion detection, surveillance, communication, and access & visitor control                  |
| Tier IV                | Essential Facilities      | Protection based on site specific risk assessment   |

### 2.5.2. Critical Systems and Components

Criticality of a security system or component is influenced by deployment and interdependency with other systems. The table below shows all items in the current inventory<sup>13</sup> with indication of criticality to NERC CIP compliance and performance assurance based on “Protection Program Essential Elements”

<sup>12</sup> Protection requirements for Tier 3 sites are based on the FY2011 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.

<sup>13</sup> Last updated 8/30/2011.

documented in Appendix A of the SPAP. Only three of the components require planned replacement based on their impact on the security system effectiveness.

**Table 4. Critical Security Components**

| Item Category                       | Count | NERC CIP Required | Critical (SPAP) | Requires Planned Replacement |
|-------------------------------------|-------|-------------------|-----------------|------------------------------|
| Camera                              | 673   | x                 | x               |                              |
| Card Reader                         | 176   | x                 |                 |                              |
| Door Contact                        | 228   | x                 | x               |                              |
| DVR                                 | 92    |                   | x               | x                            |
| Electronic Lock                     | 138   | x                 |                 |                              |
| Firewall                            | 86    | x                 |                 |                              |
| Motion Sensors/Detectors            | 27    | x                 | x               |                              |
| Network switch                      | 6     | x                 |                 |                              |
| PW-6000 Intelligent Controller (IC) | 105   | x                 |                 | x                            |
| REX (Request to Exit) Device        | 105   | x                 |                 |                              |
| RSA Primary / Failover              | 3/2   | x                 | x               |                              |
| Serial to IP Converter              | 57    | x                 | x               | x                            |
| Terminal Server Primary / Failover  | 3/2   | x                 | x               |                              |
| UPS (Uninterruptible Power Supply)  | 15    | x                 |                 |                              |

## 2.6. Prioritization

Asset management initiatives, programs and projects are prioritized so that once regulatory compliance obligations are met, the focus shifts to risk-informed protection initiatives. When prioritizing risk-informed capital investment, three factors are considered:

- The criticality of the facility as measured by the impact of its loss on BPA’s ability to achieve its mission.
- Real-time security threat information.
- Efficiencies to be gained by investment (ROI).

Security components are further prioritized for maintenance based on the level of criticality of the facility where it is located, as well as the impact the component or system has on maintaining security compliance (e.g. NERC CIP, HSPD-12, etc.) and security system effectiveness (e.g., identified by the SPAP).

**Table 5. Priority Matrix**

| Priority Level | Asset Location                | Asset Type                                  |
|----------------|-------------------------------|---|
| 1              | All Locations                 | Critical System or Component for Compliance |
| 2              | Most Critical (Tier I and II) | Critical System or Component for Protection |
| 3              | Critical (Tier III)           | Critical System or Component for Protection |
| 4              | Essential (Tier IV)           | Critical System or Component for Protection |
| 5              | Most Critical (Tier I and II) | Non-critical System or Component            |
| 6              | Critical (Tier III)           | Non-critical System or Component            |
| 7              | Essential (Tier IV)           | Non-critical System or Component            |

## 2.7. Risks

Risks addressed by security assets are covered in relation to strategic initiatives in Table 1. Three Agency level risks are quantified in more detail below.

**Table 6. Agency Level Risks**

|                     |   |
|---------------------|---|
| <b>Risk 1:</b>      | <b>Experiencing terrorist type attacks at a critical transmission sites.</b>  |
| <b>Likelihood:</b>  | Possible based on DHS assessment of “Medium Risk” of terrorist attack for critical energy infrastructure similar to those owned by BPA.   |
| <b>Consequence:</b> | <p>1) <b>System Reliability:</b> Extreme – Loss of a single critical site such as Raver would impact the stability of the Bulk Electric System through loss of reactors and capacitors, significant loss of East to West generation integration, and capacity to move excess of 6,000 MW during peak seasons.</p> <p>2) <b>Legal/Regulatory Obligation:</b> Extreme – Loss or significant damage to any BPA critical assets would result in financial, regulatory, and regional accountability consequences. This would lead to severe, observable impact and orders for substantial corrective action, including some mandatory changes in BPA operation or administration.</p> <p>3) <b>Business/Finance:</b> Major – As a subsequent impact of the losses identified under “System Reliability” there would be an impact to BPA customers and local economy. The level of impact has not been quantified. Long-term loss of critical transmission facilities can reasonably be expected to have a major economic impact to regional customers.</p> |
| <b>Risk 2:</b>      | <b>Failure to meet compliance obligations</b>   |
| <b>Likelihood:</b>  | Possible within 1 year  |
| <b>Consequence:</b> | 1) <b>Legal/Regulatory Obligation:</b> Major to Extreme – Violation or non-compliance would lead to severe, observable impact and orders for substantial corrective action, including some mandatory changes in BPA operation or administration (e.g. Remedial Action Directives (RADs)). Noncompliance could bring national, regional, and local attention and criticism by entities such as DOE IG and GAO, as well financial sanction by NERC.   |
| <b>Risk 3:</b>      | <b>Continual exposure to criminal activity</b>  |
| <b>Likelihood:</b>  | Probable <sup>14</sup> within one year  |
| <b>Consequence:</b> | <p>1) <b>System Reliability:</b> Major – Collateral damage to transmission system as a result of criminal activity such as burglary or theft.</p> <p>2) <b>Legal/Regulatory Obligation:</b> Minor – If loss or significant damage occurred to any BPA critical asset or NERC CIP site it could result in financial, regulatory, and regional accountability consequences.</p> <p>3) <b>Business/Finance:</b> Major – Annual financial loss due to criminal activity cost the Agency at least in the range of \$100,000 to \$1 million per year.</p>   |

<sup>14</sup> On average there are 77 security incidents annually reported to OSCO.

## 2.8. Metrics

BPA’s OSCO has established performance targets for all core areas of its operation. A large number of measures in the FY 2012 and FY 2013 Balance Score Card (BSC) for physical security and personnel security directly support the asset management initiatives. A detailed description of current measures, including quarterly progress indicators, can be found in NN – Security and Continuity of Operations BSC located at the BPA Strategic Planning SharePoint site:

<http://internal.bpa.gov/sites/corp-strat/StrategicPlanning/Pages/StrategyMapsBalancedScorecards.aspx>

Table 7 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 7. Performance Metrics**

| Initiative   | FY2012 Targets  | FY13 & Future Target  |
|--|---|---|
| <b>1. Compliance</b>   | (Not in BSC) 1) Security system enhancement in support of NERC CIP Versions 2 and 3 (NOAV).   | 1) Complete security system enhancement in support of NERC CIP Version 3 and 4 by April 2014, within scope and budget.<br>2) No NERC-CIP violations as a result of inadequate or malfunctioning Physical Security assets (e.g. Card Readers, Door Contacts, etc.)   |
| <b>2. Critical Infrastructure Protection</b>                 | 1) A Tier II proof of concept completed on schedule and within budget by September 30, 2012.<br>2) Develop Tier II implementation policy/strategy that supports a long-term programmatic execution.<br>3) Complete Physical Security capital program redesign which results in effective agreements, processes and procedures between SER, TS and IT to meet Security’s out year capital program in accordance with the requirements of CASP. | 1) Validate Proof of Concept for Tier II protection<br>2) Finalize programmatic implementation of critical site enhancements to include funding, scheduling, and refinement of supporting processes.<br>2) Reduced number of security incidents at treated sites.   |
| <b>3. Essential Infrastructure Protection</b>                | 1) (not in BSC) Complete assessment of corporate facilities to identify opportunities for improving protection and or gaining efficiencies through automation   | 1) Security System Enhancements are installed at essential corporate sites and Tier IV substations with notable reduction in crime and or financial return.<br>2) Improve analysis or crime statistics.<br>3) Complete assessment of Tier IV facilities to identify opportunities for improving protection and/or gaining efficiencies through automation |
| <b>4. Performance Testing &amp; Preventative Maintenance</b> | 1) Complete SPAP <sup>15</sup> site visits, performance tests and PMs as scheduled.<br>2) Streamline corrective action processes and tracking.  | 1) 100% of all critical sites are tested annually by the maintenance vendor with at least 20% of those sites receiving no-notice performance tests by Physical Security team members<br>2) Explore efficiency gains by coupling SPAP site visits with other activities, such as planned replacement of  |

<sup>15</sup> Performances tests are designed in accordance with DOE O 473.3.

|   |   |  |
|---|---|--|
| <p><b>5. Replacement and Renewal Program</b></p>            | <p>1) Joint measure between OSCO and ITPACs team to develop an automated security asset management system:<br/>2) (Not in BSC) Replace outdated critical components based on identified asset strategy (section 3.3.2)</p>  | <p>components.<br/>2) Reduced number of corrective actions noted during visit (e.g. less than 2 per site).<br/>1) Planned replacements are completed as defined by asset plan.<br/>2) Reduced number of call outs as a percentage of system components.</p>  |
| <p><b>6. System Reliability Projects</b></p>                | <p>Joint measures between OSCO and ITPACs to:<br/>1) Establish a testing platform and plan<br/>2) Develop interim security protection to be used in lieu of full enhancement<br/>3) Improve power reliability for PACS</p>  | <p>1) Plan and implement interim solution<br/>2) Establish and adhere to service level agreement between IT and Security for system and component testing in support of project schedule.</p>  |
| <p><b>7. Access Credentials (Smart Cards and LSSOs)</b></p> | <p>1) On-boarding paperwork is processed; employees and contractors are cleared to work, and issued a Local Site Specific Only (LSSO) badge within 14 days.<br/>2) Update all digital certificates prior to expiration, with no more than 2-3% expiration allowance for instances of known variances, such as employees out of the country or on extended leave.<br/>3) Eligible applicants are processed for Smart Cards and are ready for pick up within 45 days from the point of enrollment.<br/>4) Ensure that employees with access to NERC CIP sites go through recurring background checks every 7 years.<br/>5) Implement a new process for short-term CFTE on-boarding where the responsibility of pre-employment background investigations falls on the contracting company rather than BPA.</p> | <p>1) Zero reportable PRA NERC CIP violations.<br/>2) Identify Credential and Access Management Initiate Bonneville ICAM (BICAM) group, establish charter, goals and objectives and obtain Executive Sponsorship.<br/>3) Reduced percentage of allowance for expirations for digital certificates.</p> |

### 3. Capital Investment Recommendations

The following sections provide the investment recommendations for FY12 to FY21 that support the strategic initiatives targeted for meeting key security asset management objectives. New implementation 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). The concise comparison of risk reductions is covered in Appendix 5.1.

#### 3.1. Critical Asset Security Plan (CASP) - Initiatives 1, 2 and 3

The CASP was developed to enhance the reliability and protection of the transmission system and to address all security requirements related to protection of critical assets, 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.

Due to rapidly evolving security compliance requirements for critical infrastructure protection, the implementation of the CASP has resulted in three initiatives: 1) comprehensive protection of most critical assets, 2) implementation of security systems in response to new compliance obligations (e.g., NERC CIP), and 3) protection of facilities essential to operation.

##### 3.1.1. Protection of Control Centers

BPA's most critical facilities are its control centers. They are classified as Tier I facilities. Monroe 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 a more efficient setup which in the long run will save BPA \$250K annually on guard force deployment.

OSCO has developed a proposal designed to leverage security systems and infrastructure in a manner that will effectively utilize minimal protective security force personnel while meeting physical protection needs and compliance requirements. 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 8 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 had show return on investment after three years.

**Table 8. Capital Cost Projection for Monroe Complex - Tier I Protection**

| FY                              | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | Total |
|---------------------------------|------|------|------|------|------|------|------|------|------|------|-------|
| Tier I Critical Site Protection | -    | 300  | 450  | -    | -    | -    | -    | -    | -    | -    | 750   |
| TOTAL                           | -    | 300  | 450  | -    | -    | -    | -    | -    | -    | -    | 750   |

##### 3.1.2. Protection of Most Critical Transmission Assets

The objective of this program is the installation of security systems that provide the recommended solution for protecting BPA's most critical assets. A sites' relative criticality is captured in Transmission's Risk Based Assessment Methodology (RBAM). Sites are also evaluated for consequence level by using the RAM-T site criticality and ranking method. This provides a well balanced indication of the severity of impact to national defense, customers and the Northwest economy in the event the site is significantly damaged or loss due to criminal activity.

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. 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 and voltage stability, causing loss of revenue due to path constraints, and possible rate increases for the customers, as a result of replacing a substantially damaged substation.

The program supports security enhancements for BPA's most critical transmission substations (Tier II). 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, remote communication, surveillance, and early intrusion detection outside the perimeter.

The estimated risk reduction as a result of this implementation is quantified in the Table 9.

**Table 9. Estimated Security Risk Impact - Tier II Protection**

(Note: The "Before" state assumes Level 1<sup>16</sup> and NERC CIP systems up to CIP 006 Version 3.)

| Threat                           | Before Tier II Treatment |            | After Tier II Treatment |            | % Risk Reduction <sup>17</sup> |
|----------------------------------|--------------------------|------------|-------------------------|------------|--------------------------------|
|                                  | Risk Numerical           | Risk Range | Risk Numerical          | Risk Range |                                |
| 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%                             |

Although the current capital allocation allows for implementation of the proposed design at a rate of at least one per year, we propose to delay the next installation until FY2015 to fully validate the proof of concept being deployed at Raver Substation. Implementation of the proof of concept Tier II design at Raver is nearly complete and is scheduled for thorough systems assessment and performance testing in FY 2013. This study will be used to validate the proof of concept, make adjustments to the design as necessary, thus providing the best value for the investment. We believe that we can find efficiencies in the design that would at the minimum absorb the cost of inflation experienced over the two year pause.

The updated schedule is outlined in Table 10. In addition to allowing time for design validation, the proposal aligns future builds with Transmission's planning cycle creating efficiency and ensuring successful execution. If OSCO's proposal to reshape the budgets for FY 2013 through FY2015 is approved, all critical sites will be protected by FY 2019 as originally planned. Otherwise, the final site deployment will be pushed out to FY2021.

**Table 10. Capital Cost Projection with Alternative Funding Model (RECOMMENDED) (\$000s)**

| FY                                | 2012         | 2013       | 2014     | 2015         | 2016         | 2017         | 2018         | 2019         | 2020         | 2021         | Total         |
|-----------------------------------|--------------|------------|----------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|---------------|
| Tier II Critical Site Protection  | 2,819        | 200        | -        | 7,507        | 5,887        | 7,070        | 5,710        | 4,145        | -            | -            | 33,338        |
| Tier III Critical Site Protection | -            | -          | -        | -            | -            | -            | -            | -            | 1,000        | 1,000        | 2,000         |
| <b>TOTAL</b>                      | <b>2,819</b> | <b>200</b> | <b>-</b> | <b>7,507</b> | <b>5,887</b> | <b>7,070</b> | <b>5,710</b> | <b>4,145</b> | <b>1,000</b> | <b>1,000</b> | <b>35,338</b> |

To help mitigate risks associated with the delay in schedule, OSCO has identified a cost effective interim protection solution scheduled to be deployed at Teir 2 critical sites where adequate cell coverage is

<sup>16</sup> Level 1 – Baseline security system includes fenced Control House, one automated vehicle gate, camera at the vehicle gate.

<sup>17</sup> Percentage of risk reduction is based on maximum Risk Numerical value of 1.

available. The system to be deployed has already been purchased and is scheduled to be deployed in FY 2013 for \$35,000.

### 3.1.3. NERC CIP Compliance Implementation

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-to-four year window.

#### *NERC CIP 006 Versions 2 and 3*

The physical security requirements from NERC CIP 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 logging and monitoring.

As indicated by risk comparison in Table 11, this investment reduces the security risk posed by the insider threat, however has limited risk reduction on other threat categories.

**Table 11. Security Risk Rating Impact of Tier II Protection**

(Note: The “Before” state assumes Level 1<sup>18</sup>)

| Threat                              | Before NERC CIP Version 3 |            | After NERC CIP Version 3 |            | % Risk Reduction <sup>19</sup> |
|-------------------------------------|---------------------------|------------|--------------------------|------------|--------------------------------|
|                                     | Risk Numerical            | Risk Range | Risk Numerical           | Risk Range |                                |
| International Terrorist             | 0.49                      | Medium     | 0.49                     | Medium     | 0%                             |
| Eco Terrorist /<br>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 FY 2012 BPA enhanced access control at 17 transmission sites in order to facilitate activation of this equipment for Transmission’s operational compliance.

#### *NERC CIP 006 Versions 4*

NERC CIP Version 4 was finalized in April of 2012. Version 4 expanded the criteria for identifying critical assets. Based on this more inclusive definition, BPA assets requiring NERC CIP enhancement increased by an estimated 28<sup>20</sup> sites.

With the exception of a few sites, there are no security systems at these newly identified facilities, as they were assigned relatively lower level of criticality based on both RAM-T and Transmission’s RBAM.

Estimated cost for implementation is \$125,000 per site at the Version 4 sites and only \$30,000 per site for facilities identified under Versions 2 and 3.

<sup>18</sup> Level 1 – Baseline security system includes fenced Control House, one automated vehicle gate, camera at the vehicle gate.

<sup>19</sup> Percentage of risk reduction is based on maximum Risk Numerical value of 1.

<sup>20</sup> Transmission is doing a more thorough assessment and the number of sites is subject to change.

The relative risk reduction from the base condition is demonstrated in Table 12.

**Table 12. Estimated Security Risk Rating Impact of CIP Version 4 Protection**

(Note: The “Before” state assumes no security systems.)

| Threat                           | Before NERC CIP<br>Version 4 |            | After NERC CIP<br>Version 4 |            | % Risk Reduction |
|----------------------------------|------------------------------|------------|-----------------------------|------------|------------------|
|                                  | Risk Numerical               | Risk Range | Risk Numerical              | Risk Range |                  |
| International Terrorist          | 0.4                          | Medium     | 0.40                        | Medium     | 0%               |
| Eco Terrorist / Special Interest | 0.37                         | Medium     | 0.37                        | Medium     | 0%               |
| Criminal Activity                | 0.39                         | Medium     | 0.35                        | Medium     | 4%               |
| Vandal                           | 0.36                         | Medium     | 0.32                        | Medium     | 4%               |
| Insider                          | 0.23                         | Low        | 0.13                        | Low        | 10%              |

A business case has been approved and funding allocated for treating 61 facilities across BPA in response to NERC CIP Versions 2 through 4. This project will expand BPA’s logging and monitoring capability by installing exterior cameras, door contacts, interior motion detection alarms, card readers and sirens. Furthermore, to ensure “continuous monitoring” capability 52 sites will have an alternate communications path. This project is scheduled to be completed by April 2014. Table 13 shows anticipated spending per year based on the business case and project schedule.

**Table 13. Capital Cost for NERC CIP through Versions 4**

| FY                            | 2012       | 2013         | 2014         | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | Total        |
|-------------------------------|------------|--------------|--------------|------|------|------|------|------|------|------|--------------|
| NERC CIP Version 2 & 3 (NOAV) | 431        | -            | -            | -    | -    | -    | -    | -    | -    | -    | 431          |
| NERC CIP Versions 2 - 4       | 2          | 4,347        | 2,551        | -    | -    | -    | -    | -    | -    | -    | 6,900        |
| <b>TOTAL</b>                  | <b>433</b> | <b>4,347</b> | <b>2,551</b> | -    | -    | -    | -    | -    | -    | -    | <b>7,331</b> |

### NERC CIP 006 Versions 5

Early drafts of NERC CIP Version 5 called for protection of all openings 96 square inches or greater, which was estimated to cost BPA \$12.5 million in FY 2015. In its most recent release of CIP Version 5, circulated in September 2012, NERC has omitted this requirement. NERC’s decision is believed to be influenced by the comments received from BPA and other utilities. Although, Version 5 is not yet final, the great consensus is that this requirement will not be reintroduced.

## **3.1.4. Essential Infrastructure Protection**

### Corporate Facilities

Based on a recent assessment of the BPA Headquarters security system, it was determined that, although functional, many of the security systems are no longer technologically viable (e.g., limited parts availability, replacement units no longer available, etc.). Most of the building’s exterior cameras are of older, analog technology and past their service life. The various aspects of the 905 building’s security systems were installed at different periods of time. The installations range from as early as 1988 to the present, resulting in a diverse network of security equipment, of varying technology, that may be as much as 24 years old.

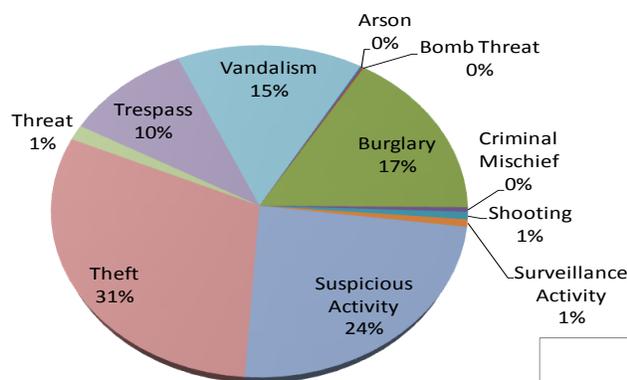
In a joint effort with ITPACS, OSCO is developing a holistic, updated design, utilizing current technologies designed to work together as an integrated system for greater effectiveness and efficiency.

Development of a new design, together with upgraded security equipment, will enable improved system performance with the integration of system component functionality. First phase of the headquarter upgrade will be the redesign of the lobby. A business case is near completion and the total cost is estimated at \$500,000.

Additionally, a security survey of the Ross Complex indicates that if the underlying physical security infrastructure were upgraded to include automated systems, additional fencing, lights, video surveillance and intermediate level vehicle barriers, the number of guard hours could be significantly reduced. The Agency currently spends \$394,000 per year guarding the main entrance to the complex. This could be reduced to \$140,000 per year for an annual savings of \$254,000. A business case is being prepared for this project. The total direct cost is \$300,000, meaning that BPA will realize a return on investment in just over one year.

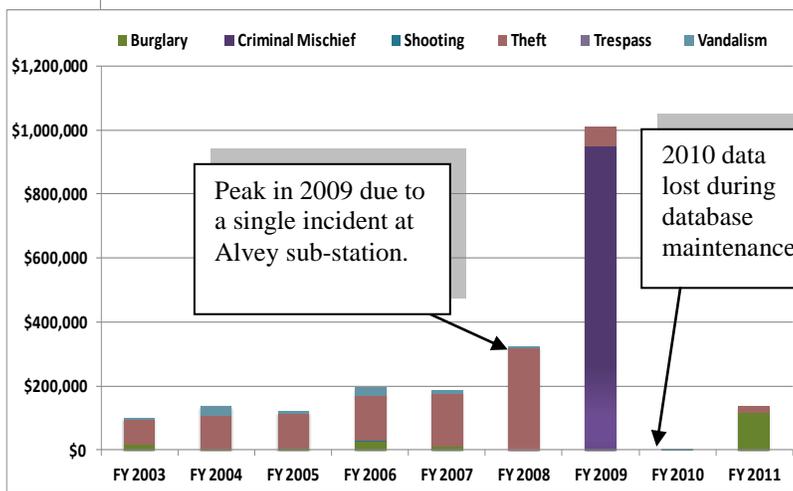
*At Risk Transmission Facilities*

**Chart 1. Reported Security Incidents (2003-2011)**



The Agency loses nearly \$270,000 per year due to criminal activity. This estimate is extremely conservative as it excludes time and labor and does not account for unreported damages addressed locally by the substation operation. Chart 1 shows incidents by type.

**Chart 2. Material Loss Due to Security Incidents**



The majority of these incidents take place at Tier IV level transmission substations. Due to increasing value of copper and other heavy metals, the criminal activity is on the rise. Chart 2 shows total loss per year reported to OSCO.

Risk assessments and crime statistics are used to identify the facilities requiring enhanced security protection. Table 14 shows the funding allocation for corporate and Tier IV facilities through FY 2021.

**Table 14. Corporate and Tier IV Site Protection**

| FY   | 2012 | 2013       | 2014       | 2015 | 2016       | 2017       | 2018       | 2019       | 2020 | 2021       | Total        |
|--|------|------------|------------|------|------------|------------|------------|------------|------|------------|--------------|
| Essential Infrastructure Protection (HQ Lobby)     | -    | 500        | -          | -    | -          | -          | -          | -          | -    | -          | 500          |
| Essential Infrastructure Protection (Ross Complex) | -    | 300        | -          | -    | -          | -          | -          | -          | -    | -          | 300          |
| Essential Infrastructure Protection                | -    | -          | 500        | -    | 500        | 500        | 500        | 500        | -    | 500        | 3,000        |
| <b>TOTAL</b>                                       | -    | <b>800</b> | <b>500</b> | -    | <b>500</b> | <b>500</b> | <b>500</b> | <b>500</b> | -    | <b>500</b> | <b>3,800</b> |

## 4. Investment Recommendations - Expense

Initiatives funded under expense include upgrades, updates and ongoing maintenance activities. Funding is broken out by Corporate and Transmission to account for funding provided under the Transmission umbrella through direct funding.

### 4.1. HSPD-12 Compliance – Initiative 1

DOE is heading up an initiative to advance the implementation of Homeland Security Presidential Directive-12 (HSPD-12) through Identify, Credential and Access Management Initiatives (ICAM). This initiative requires better utilization of the smart credential (Smart Card) technology across agencies as the common means of authentication for access to facilities, networks, and information systems. To maintain HSPD-12 compliance and follow DOE guidance, BPA is required to update its existing card readers with more current technology. Updated technology will be able to authenticate access for Smart Card holders from other agencies. It will eliminate the need for BPA staff to carry both a Smart Card and a Prox Card to gain access at various sites.

*Table 15. Projected Costs for Card Reader Upgrades HSPD-12 Compliance (\$000s)*

| FY  | 2012      | 2013      | 2014     | 2015     | 2016     | 2017     | 2018     | 2019     | 2020     | 2021     | Total     |
|---|-----------|-----------|----------|----------|----------|----------|----------|----------|----------|----------|-----------|
| <b>TRANSMISSION</b><br>HSPD-12 Compliance |           | 34        | -        | -        | -        | -        | -        | -        | -        | -        | 34        |
| <b>CORPORATE</b><br>HSPD-12 Compliance    | 43        | 3         | -        | -        | -        | -        | -        | -        | -        | -        | 46        |
| <b>TOTAL</b>                              | <b>43</b> | <b>37</b> | <b>-</b> | <b>80</b> |

### 4.2. Performance Testing & Preventative Maintenance – Initiative 4

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, and see that corrective maintenance is addressed in accordance with the criticality of the site or system. The DOE requires security systems to be performance tested on an annual basis. The requirements for testing and maintenance under NERC is every three years.

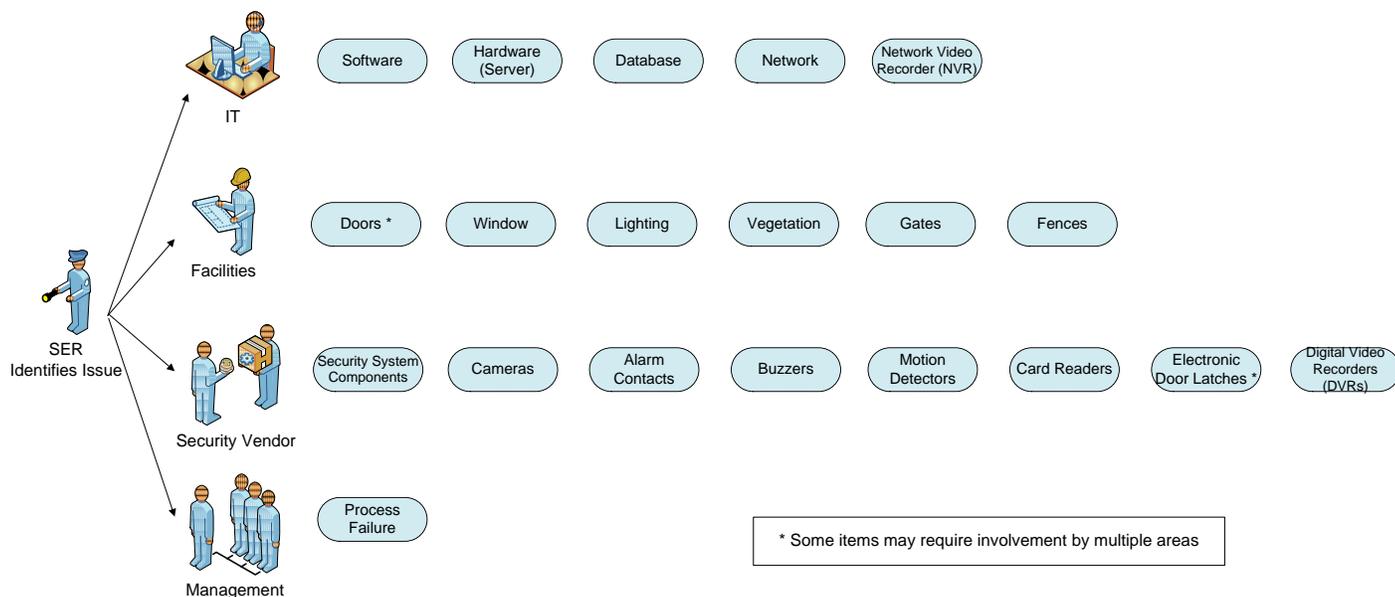
Historically, Physical Security team has conducted the performance testing. Starting in FY 2013 this function will be incorporated into the maintenance contract, with 20% of the sites being audited by physical security specialists.

Security system performance is ensured in the following ways:

- Maintenance vendor conducts performance tests annually at all critical transmission facilities.
- Physical Security team conducts performance tests at 20% of BPA’s critical assets to ensure vendor adherence to the standards.
- ITPACS and Maintenance vendor conducts preventative maintenance of critical components.
- Alarm Monitoring Station reviews surveillance footage around the clock.
- 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 shows most common issues and routing protocols.

**Figure 2. Corrective Action Routing**



The cost associated with this program is estimated based on the vendor contract solicitation 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 4. In FY2014 the number of sites requiring an SPAP visit is expected to increase to approximately 90. (Note: The higher cost estimate in FY2013 is due to an increase in total site visits to support HSPD-12 compliance enhancements).

**Table 16. Projected Costs for SPAP Program (\$000s)**

| FY   | 2012      | 2013       | 2014       | 2015       | 2016       | 2017       | 2018       | 2019       | 2020       | 2021       | Total        |
|--|-----------|------------|------------|------------|------------|------------|------------|------------|------------|------------|--------------|
| <b>TRANSMISSION</b>  |           |            |            |            |            |            |            |            |            |            |              |
| Performance Testing & Preventative Maintenance (Site Visits) | -         | 150        | 130        | 150        | 155        | 159        | 164        | 169        | 174        | 179        | 1,430        |
| <b>CORPORATE</b>   |           |            |            |            |            |            |            |            |            |            |              |
| Performance Testing & Preventative Maintenance               | 38        | 7          | 7          | 7          | 8          | 8          | 8          | 8          | 9          | 9          | 109          |
| <b>TOTAL</b>   | <b>38</b> | <b>157</b> | <b>137</b> | <b>157</b> | <b>163</b> | <b>167</b> | <b>172</b> | <b>177</b> | <b>183</b> | <b>188</b> | <b>1,539</b> |

### 4.3. Replacement and Renewal Program – Initiative 5

#### 4.3.1. 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.

Based on historic billing from the maintenance vendor for “break/fix” activities, the average annual spending for O&M is \$400,000 at transmission facilities, and \$40,000 at non-transmission facilities. With the new planned replacement strategy described in section 3.3.2 below, it is estimated that the new combined annual cost for non-critical component replacement and repair using break/fix approach is around \$200,000 per year. Table 17 projects this cost over time with three percent inflation as well as a

15 percent increase in 2014 due to addition of new assets as a result of NERC CIP Version 4 described in Section 3.1.2.<sup>21</sup>

**Table 17. Cost of Replacement Upon Failure (\$000s)**

| FY                       | 2012       | 2013       | 2014       | 2015       | 2016       | 2017       | 2018       | 2019       | 2020       | 2021       | Total        |
|--------------------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|--------------|
| <b>TRANSMISSION</b>      |            |            |            |            |            |            |            |            |            |            |              |
| Replacement Upon Failure | 172        | 190        | 200        | 179        | 185        | 190        | 196        | 202        | 208        | 214        | 1,936        |
| <b>CORPORATE</b>         |            |            |            |            |            |            |            |            |            |            |              |
| Replacement Upon Failure | 56         | 10         | 11         | 11         | 12         | 12         | 13         | 13         | 14         | 15         | 167          |
| <b>TOTAL</b>             | <b>228</b> | <b>220</b> | <b>211</b> | <b>190</b> | <b>197</b> | <b>202</b> | <b>209</b> | <b>215</b> | <b>222</b> | <b>229</b> | <b>2,103</b> |

### 4.3.2. Planned Replacement

Currently, only four components have been identified as requiring an exception to the “break/fix” approach. Digital video recorders (DVRs), analog to IP converters, intelligence controllers (IC), and cameras require systematic replacement. DVRs, converters, and ICs are considered critical security system components, whose failure could severely impact the ability to assess alarm activities. Without this capability it would be necessary to call out local law enforcement and field employees to respond to alarms.

Cameras are recommended for a systematic replacement because, with the break / fix approach, there is a high risk of multiple failures within a short time, causing an unmanageable strain on resources. This risk is exacerbated by the fact that cameras constitute 35 percent of all physical security components, with a large number installed in a short period of time.

It is recommended that:

- DVRs and analog to IP converters be replaced at 25 percent per year after exceeding expected life-cycle<sup>22</sup>, with the fifth year supporting a system-wide replacement of intelligence controllers. Intelligence controllers do not fit a phased replacement model because they typically have a new version release every five years which requires a system-wide replacement.
- Cameras replaced on a break/fix basis with a minimum of 10 percent replacement per year for four years<sup>23</sup>.
- IC replacement be capitalized and coupled with system wide update of cameras that are past life-cycle or no longer technologically viable (e.g., analog).

Table 18 shows the projected spending for the planned replacement strategy.

**Table 18. Projected Costs for Planned Replacement (\$000s)**

| FY                  | 2012       | 2013       | 2014       | 2015       | 2016      | 2017       | 2018       | 2019       | 2020       | 2021       | Total        |
|---------------------|------------|------------|------------|------------|-----------|------------|------------|------------|------------|------------|--------------|
| <b>TRANSMISSION</b> |            |            |            |            |           |            |            |            |            |            |              |
| Planned Replacement | 95         | 206        | 212        | 406        | 52        | 200        | 217        | 224        | 503        | 237        | 2,078        |
| <b>CORPORATE</b>    |            |            |            |            |           |            |            |            |            |            |              |
| Planned Replacement | 67         | 27         | -          | -          | -         | -          | -          | -          | 170        | -          | 264          |
| <b>TOTAL</b>        | <b>162</b> | <b>233</b> | <b>212</b> | <b>406</b> | <b>52</b> | <b>200</b> | <b>217</b> | <b>224</b> | <b>673</b> | <b>237</b> | <b>2,342</b> |

<sup>21</sup> NERC CIP Version 4 will increase the number of facilities by nearly 40%. The financial impact of maintaining these additional assets is estimated at 15 % of current spending because most components have a greater than ten year life cycle.

<sup>22</sup> Life-cycle based on manufacturer recommendations and fail rates experienced by BPA.

<sup>23</sup> Exception to the 10% is FY2012 which will only support a 5% replacement

### 4.3.3. Maintaining Tier II Site Enhancements

As described under section 3.1.1, initiative 1 will result in large scale security system enhancements at the 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 – \$80,000 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 3.1.2 - Table 10) maintenance costs are estimate in the Table 19. Due to a significant betterment of the security infrastructure and a spike in costs very five years, it is recommended that replacement and renew program costs be capitalized in FY2015 and FY2020. As the implementation takes place and the individual components are added to the inventory, the maintenance activities will be incorporated into the “Replacement Upon Failure” and “Planned Replacement” budgets.

**Table 19. Tier II Maintenance Projection (\$000s)**

| FY                  | 2012 | 2013 | 2014 | 2015     | 2016      | 2017      | 2018       | 2019      | 2020       | 2021       | Total      |
|---------------------|------|------|------|----------|-----------|-----------|------------|-----------|------------|------------|------------|
| <b>TRANSMISSION</b> |      |      |      |          |           |           |            |           |            |            |            |
| Tier II Maintenance | -    | -    | -    | 5        | 10        | 40        | 110        | 95        | 255        | 265        | 780        |
| <b>Total</b>        | -    | -    | -    | <b>5</b> | <b>10</b> | <b>40</b> | <b>110</b> | <b>95</b> | <b>255</b> | <b>265</b> | <b>780</b> |

### 4.4. System Reliability Projects – Initiative 6

The OSCO and ITPACS teams have identified the following gaps that impact system reliability:

- Lack of formal testing procedures (to include acceptance, approval steps) and change management documentation (FISMA/ATO, NERC CIP) for new security equipment
- Need for protecting critical assets in the short-term, while the full enhancement program is completed
- Need for an automated inventory management system
- Need to improve power reliability to security systems

The two teams have committed to addressing these gaps by following joint balance scorecard measures.

- Testing Platform and Plan - A testing platform and plan is developed to test and approve IT based security equipment.
- Interim Security Protection - A plan is developed and accepted by stakeholders to support an interim solution for the protection of critical assets.
- Asset Management Plan Automation - An automated asset management tool is identified, and a proposal is provided to decision makers to sponsor technical design and implementation for FY2013.
- Power Reliability for PACS - UPS hardware standard is selected and implemented at a pilot site.

In addition to the current effort, it is projected that funding is going to be required for another two years in order to fully address system reliability needs. Costs associated with this initiative are documented in Table 20.

**Table 20. ITPAC System Reliability Projects (\$000s)**

| FY   | 2012       | 2013       | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | Total      |
|--|------------|------------|------|------|------|------|------|------|------|------|------------|
| <b>TRANSMISSION</b><br>System Reliability Projects | 287        | 100        | -    | -    | -    | -    | -    | -    | -    | -    | 387        |
| <b>Total</b>                                       | <b>250</b> | <b>100</b> | -    | -    | -    | -    | -    | -    | -    | -    | <b>387</b> |

#### 4.5. Access Credential Management – Initiative 7

OSCO is currently managing over 5,500 access credentials (4,200 Smart Cards and 1,300 LSSOs) for all BPA employees and contractors. This function was implemented in 2005 in support of HSPD-12. This directive requires executive agencies to verify identity for all individuals being considered for access to government facilities and information, and outlines a common credential requirement (Smart Card).

In accordance with HSPD-12 and NERC CIP, prior to a new employee or contractor starting work at BPA he or she must undergo personnel risk assessment (PRA) and personal identity verification (PIV) to receive a government issued Smart Card and authorized access to critical cyber assets. OSCO is responsible for managing all costs associated with Smart Cards. Additionally, OSCO runs a full service enrollment center requiring equipment purchase and ongoing maintenance.

All costs associated with background investigations (BI) for HSPD-12 and NERC CIP PRAs are paid to Office of Personnel Management (OPM). Smart Card production and maintenance fees are paid to DOE. Both Smart Cards and PRAs have mandatory re-processing cycles. Smart Cards are only valid for five years requiring a reissue of a new card prior to expiration to maintain access. PRAs require employees to undergo background reinvestigation every seven years to maintain authorized access to critical cyber assets.

Additionally, BPA has a population of approximately 60 employees that possess an access authorization (clearance). These employees are required by DOE to undergo a recurring background investigation every five and 10 years depending on the level of clearance.

Lastly, approximately 400 federal employees are categorized as “public trust” and require initiation of a higher background investigation. An estimated 200 employees remain to complete the process. It is expected that the remaining employees will be completed over the next four years at a rate of 50 per year.

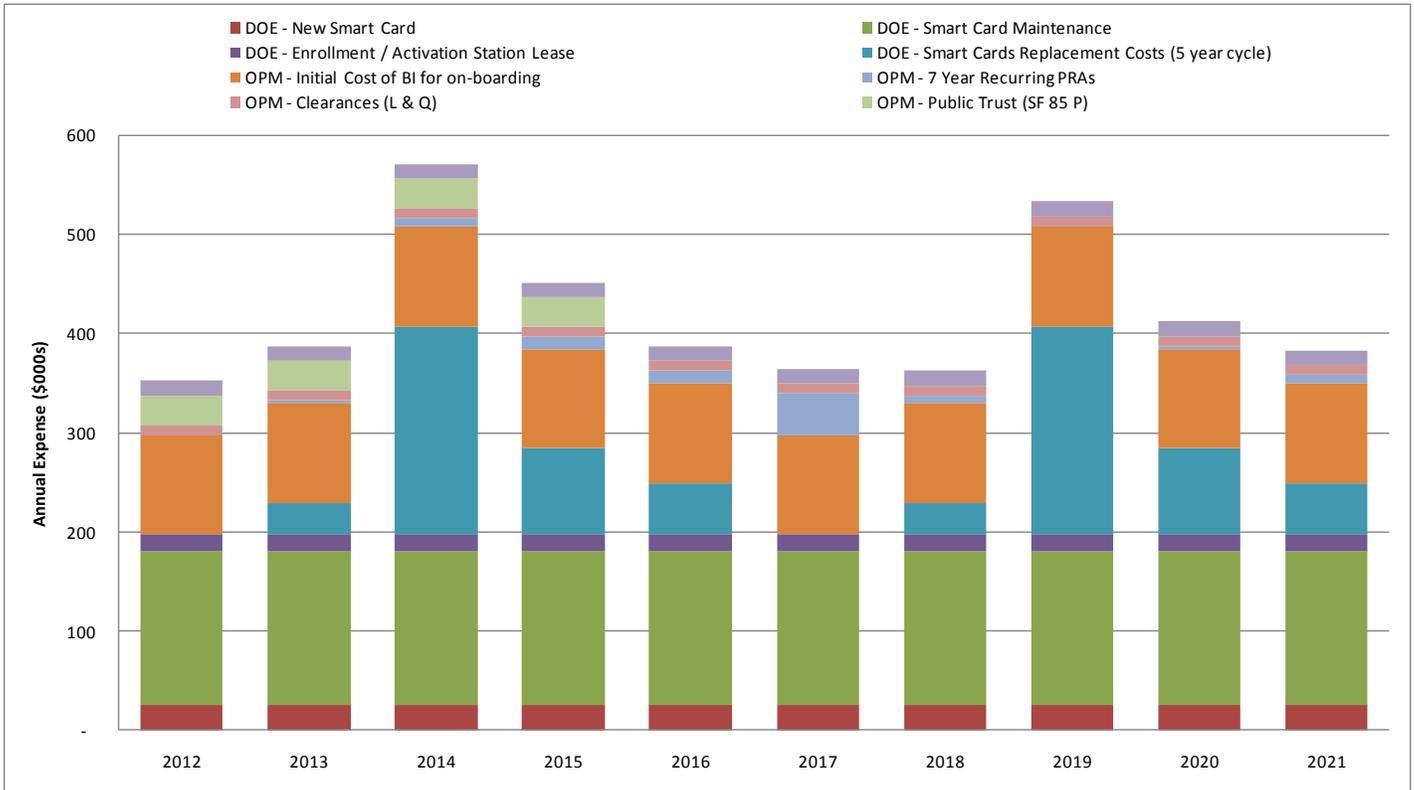
Costs for these activities are presented in Table 21 and Chart 5. Fluctuations are primarily driven by Smart Card replacement cycles with peak activity in FY2014 and FY2019.

**Table 21. Access Credential Costs<sup>24</sup>**

| FY  | 2012       | 2013       | 2014       | 2015       | 2016       | 2017       | 2018       | 2019       | 2020       | 2021       | Total        |
|---|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|--------------|
| DOE - New Smart Card                        | 25         | 25         | 25         | 25         | 25         | 25         | 25         | 25         | 25         | 25         | <b>277</b>   |
| DOE - Smart Card Maintenance                | 155        | 155        | 155        | 155        | 155        | 155        | 155        | 155        | 155        | 155        | <b>1,701</b> |
| DOE - Enrollment / Activation Station Lease | 17         | 17         | 17         | 17         | 17         | 17         | 17         | 17         | 17         | 17         | <b>189</b>   |
| DOE - Smart Cards Replacement Costs (5 yr)  | -          | 32         | 211        | 87         | 52         | -          | 32         | 211        | 87         | 52         | <b>769</b>   |
| OPM - Initial Cost of BI for on-boarding    | 100        | 100        | 100        | 100        | 100        | 100        | 100        | 100        | 100        | 100        | <b>1,100</b> |
| OPM - 7 Year Recurring PRAs                 | 1          | 3          | 9          | 13         | 13         | 43         | 8          | 1          | 3          | 9          | <b>102</b>   |
| OPM - Clearances (L & Q)                    | 10         | 10         | 10         | 10         | 10         | 10         | 10         | 10         | 10         | 10         | <b>110</b>   |
| OPM - Public Trust (SF 85 P)                | 30         | 30         | 30         | 30         | -          | -          | -          | -          | -          | -          | <b>123</b>   |
| Printing Materials for LSSOs                | 15         | 15         | 15         | 15         | 15         | 15         | 15         | 15         | 15         | 15         | <b>165</b>   |
| <b>Total</b>                                | <b>353</b> | <b>387</b> | <b>571</b> | <b>452</b> | <b>388</b> | <b>365</b> | <b>363</b> | <b>533</b> | <b>412</b> | <b>383</b> | <b>4,536</b> |

<sup>24</sup> Estimates are based on the assumption that population of Smart Card holders will remain steady at 4,500 ± 200 and on-boarding rates will remain fairly constant as compared to FY2011.

**Chart 3. Access Credential Management Costs**



## 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. Compared to the initial draft proposal, the capital spending has been reduced by \$12.5 million. A \$156,000 increase in the expense budget due to new compliance requirement has been absorbed by reprioritizing security related funding across BPA with minimal risk.

### Capital Plan for FY 2012 - FY 2021

The changes influencing OSCO’s capital forecast from what was initially proposed for FY 2013 through FY 2015 include:

- Change in NERC CIP Version 5 requirements
- Enhanced protection need for Munro Complex, a Tier I Critical Site
- Delayed implementation for Tier II critical sites, allowing time to validate proof-of-concept deployed at Raver

**Table 22. Optimized Capital Plan (\$000s) – \$12.5 million reduction and reshaping FY 2013-FY 2015**

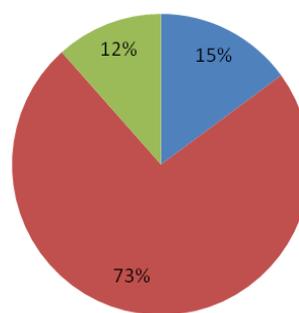
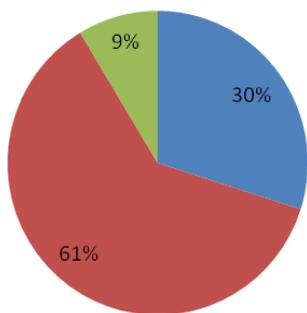
|                                      | Budget       | Actual       | Approved     | Proposed     | Approved      | Proposed     | Approved     | Proposed     | Approved      | Proposed      |
|--------------------------------------|--------------|--------------|--------------|--------------|---------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|---------------|---------------|
| Approved Budget (000's)              | 4,190        |              | 8,802        |              | 17,153        |              | 4,100        |              | 6,387        | 7,570        | 6,210        | 4,645        | 2,000        | 1,500        | 62,557        |               |
|                                      | FY 2012      | 2012         | 2013         | 2013         | 2014          | 2014         | 2015         | 2015         | 2016         | 2017         | 2018         | 2019         | 2020         | 2021         | Total         | Total         |
| Tier I Critical Site Protection      | -            | -            | -            | 300          | -             | 450          | -            | -            | -            | -            | -            | -            | -            | -            | -             | 750           |
| Tier II Critical Site Protection     | 2,900        | 2,819        | 3,377        | 200          | 4,153         | -            | 3,200        | 7,507        | 5,887        | 7,070        | 5,710        | 4,145        | -            | -            | 36,442        | 33,338        |
| Tier III Critical Site Protection    | -            | -            | -            | -            | -             | -            | -            | -            | -            | -            | -            | -            | 1,000        | 1,000        | 2,000         | 2,000         |
| NERC CIP Version 2 & 3 (NOAV)        | 450          | 431          | -            | -            | -             | -            | -            | -            | -            | -            | -            | -            | -            | -            | 450           | 431           |
| NERC CIP Version 2 & 3               | 840          | 2            | 800          | 4,347        | -             | -            | -            | -            | -            | -            | -            | -            | -            | -            | 1,640         | 4,349         |
| NERC CIP Version 4                   | -            | -            | 4,125        | -            | -             | 2,551        | -            | -            | -            | -            | -            | -            | -            | -            | 4,125         | 2,551         |
| NERC CIP Version 5                   | -            | -            | -            | -            | 12,500        | -            | -            | -            | -            | -            | -            | -            | -            | -            | 12,500        | -             |
| Essential Infrastructure Protection  | -            | -            | 500          | 800          | 500           | 500          | -            | -            | 500          | 500          | 500          | 500          | -            | 500.00       | 3,500         | 3,800         |
| Capital update of failing systems    | -            | -            | -            | -            | -             | -            | 900          | 900          | -            | -            | -            | -            | 1,000        | 0            | 1,900         | 1,900         |
| <b>TOTAL CAPITAL</b>                 | <b>4,190</b> | <b>3,252</b> | <b>8,802</b> | <b>5,647</b> | <b>17,153</b> | <b>3,501</b> | <b>4,100</b> | <b>8,407</b> | <b>6,387</b> | <b>7,570</b> | <b>6,210</b> | <b>4,645</b> | <b>2,000</b> | <b>1,500</b> | <b>62,557</b> | <b>50,057</b> |
| <i>Delta (approved vs. proposed)</i> |              |              |              | -3,155       |               | -13,652      |              | 4,307        | -            | -            | -            | -            | -            | -            | -             | -12,500       |

The charts below show the level of investment into compliance as compared to protection initiatives.

**Approved in FY12 -FY13 Planning Period**  
(Total Budget of \$63M for 10 years)

**Optimized Proposal for FY12 -FY13 Planning Period**  
(Total Budget of \$50M for 10 years)

■ Compliance ■ Critical Asset Protection ■ Protection & Efficiency



**Expense Plan for FY 2012 - FY 2021**

The expense budget has also been influenced by recent developments, including:

- Mandatory card reader upgrades required to meet new HSPD-12 compliance.
- Increase in the number of annual site visits and performance tests due to a more inclusive definition of what is considered a critical asset under NERC CIP Version 4.
- Increasing cost of replacement components.
- Vendor contract recomplete influencing earlier estimates<sup>25</sup>.

The expense budget as originally proposed called for total funding of \$11.0 million through FY 2021, assuming that system-wide upgrades could not be capitalized and \$9.1 million if the upgrade could be capitalized. The current estimate, which includes the added compliance requirements, is \$11.2 million. It also shows that camera upgrades scheduled for FY 2015 and FY 2020 cannot be capitalized as previously assumed. The \$156,000 shortfall from current funding (based on original proposal) will be covered by Transmission's field security maintenance budget. This budget is traditionally held for repairs caused by malicious activity and to offset increasing cost of security requirements similar to those impacting OSCO's expense budget now.

**Table 23. Expense Plan for FY 2012 – FY 2021(\$000s): UPDATED**

| FY                                | 2012  | 2013  | 2014 | 2015  | 2016 | 2017 | 2018  | 2019  | 2020  | 2021  | Total  |
|-----------------------------------|-------|-------|------|-------|------|------|-------|-------|-------|-------|--------|
| Compliance                        | 43    | 37    | -    | -     | -    | -    | -     | -     | -     | -     | 80     |
| Performance Testing & Maintenance | 38    | 157   | 137  | 157   | 163  | 167  | 172   | 177   | 183   | 188   | 1,539  |
| Replacement Upon Failure          | 228   | 200   | 211  | 190   | 197  | 202  | 209   | 215   | 222   | 229   | 2,103  |
| Planned Replacement               | 162   | 232   | 212  | 406   | 52   | 200  | 217   | 224   | 400   | 237   | 2,342  |
| Tier 2 Maintenance                | -     | -     | -    | 5     | 10   | 40   | 110   | 95    | 255   | 265   | 780    |
| System Reliability Projects       | 287   | 100   | -    | -     | -    | -    | -     | -     | -     | -     | 387    |
| Physical Security Subtotal        | 758   | 726   | 560  | 758   | 422  | 609  | 708   | 711   | 1,060 | 919   | 7,231  |
| Personnel Security Subtotal       | 330   | 350   | 340  | 580   | 450  | 390  | 370   | 370   | 340   | 410   | 3,930  |
| Grand Total                       | 1,088 | 1,076 | 900  | 1,338 | 872  | 999  | 1,078 | 1,081 | 1,400 | 1,329 | 11,161 |

If OSCO had to operate within the initial baseline, the added cost for mandatory HSPD-12 updates, site visits and performance tests would be covered by delaying planned replacements of components exceeding manufacture recommended shelf life, which would impact OSCO's ability to manage spending due to costly vendor call outs.

<sup>25</sup> Vendor pricing is still subject to change as the contract has not yet been awarded.

## 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 I, II, III, and IV as well as the NERC CIP required systems.

**Table A-1.1 Systems Installed 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.*

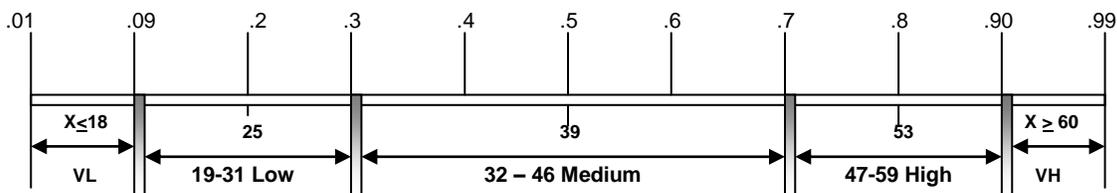
Part 2 covers sites that would be included in “NERC CIP 002 –Critical Cyber Asset Identification Version 4” (V-4).

Risk rating is calculated using the following equation:

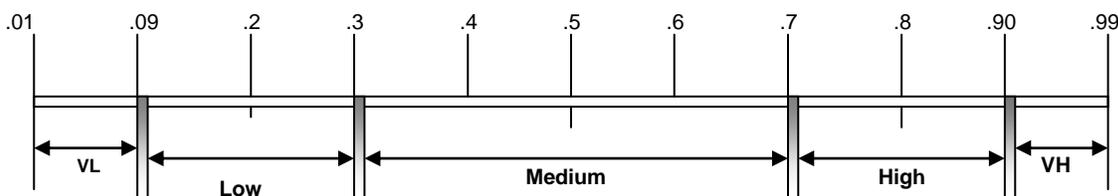
$$\text{Risk} = \text{Threat (Pa)} \times \text{Consequence (c)} \times (1 - \text{Security system effectiveness (Pe)})$$

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           | $.5 \times .99 \times (1-.01)$ | .49            | Medium     |
| Eco Terrorist/Special Interest | .5          | .9              | .01           | $.5 \times .9 \times (1-.01)$  | .45            | Medium     |
| Criminal Activity              | .99         | .5              | .1            | $.99 \times .5 \times (1-.1)$  | .45            | Medium     |
| Vandal                         | .9          | .5              | .1            | $.9 \times .5 \times (1-.1)$   | .4             | Medium     |
| Insider                        | .5          | .5              | .1            | $.5 \times .5 \times (1-.1)$   | .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 in 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           | $.5 \times .99 \times (1-.01)$ | .49            | Medium     |
| Eco Terrorist/Special Interest | .5          | .9              | .01           | $.5 \times .9 \times (1-.01)$  | .45            | Medium     |
| Criminal Activity              | .99         | .5              | .1            | $.99 \times .5 \times (1-.1)$  | .45            | Medium     |
| Vandal                         | .9          | .5              | .1            | $.9 \times .5 \times (1-.1)$   | .4             | Medium     |
| Insider                        | .5          | .5              | .5            | $.5 \times .5 \times (1-.5)$   | .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 II 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 II 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 II 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 II 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 rationale 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           | $.5 \times .8 \times (1-.01)$  | .4             | Medium     |
| Eco Terrorist/Special Interest | .5          | .75             | .01           | $.5 \times .75 \times (1-.01)$ | .37            | Medium     |
| Criminal Activity              | .99         | .4              | .1            | $.99 \times .4 \times (1-.1)$  | .35            | Medium     |
| Vandal                         | .9          | .4              | .1            | $.9 \times .4 \times (1-.1)$   | .32            | Medium     |
| Insider                        | .5          | .5              | .1            | $.5 \times .5 \times (1-.1)$   | .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           | $.5 \times .8 \times (1-.01)$  | .4             | Medium     |
| Eco Terrorist/Special Interest | .5          | .75             | .01           | $.5 \times .75 \times (1-.01)$ | .37            | Medium     |
| Criminal Activity              | .99         | .4              | .1            | $.99 \times .4 \times (1-.1)$  | .35            | Medium     |
| Vandal                         | .9          | .4              | .1            | $.9 \times .4 \times (1-.1)$   | .32            | Medium     |
| Insider                        | .5          | .5              | .5            | $.5 \times .5 \times (1-.5)$   | .13            | Low        |