

STRATEGIC ASSET MANAGEMENT PLAN

This Strategic Asset Management Plan for OSCO and Physical Security current state and maturity of the overall program and provides alignment between NERC and US DOE's Critical Infrastructure Protection, the Agency strategy, stakeholder requirements, organizational objectives and resulting asset management objectives to ensure physical security assets are managed and measured in creating and delivering value.

*Office of Security &
Continuity of
Operations
(OSCO) and Physical
Security*

Table of Contents

1.0	EXECUTIVE SUMMARY	4
2.0	ACKNOWLEDGEMENTS	5
2.1	Senior Ownership	6
2.2	Strategy Development Approach.....	6
2.2.1	Key Contributors.....	6
2.2.2	Key Activities.....	6
3.0	STRATEGIC BUSINESS CONTEXT	7
3.1	Alignment of SAMP with Agency Strategic Plan	7
3.2	Scope.....	8
3.3	Asset Description and Delivered Services.....	9
3.4	Demand Forecast for Services.....	11
3.5	Strategy Duration	11
4.0	STAKEHOLDERS.....	11
4.1	Asset Owner and Operators	11
4.2	Stakeholders and Expectations	13
	<i>Table 4.2-1, Stakeholders.....</i>	13
5.0	EXTERNAL AND INTERNAL INFLUENCES	14
	<i>Table 5.0-1, External and Internal Influences.....</i>	15
5.1	SWOT Analysis	16
6.0	ASSET MANAGEMENT CAPABILITIES AND SYSTEM.....	17
6.1	Current Maturity Level	17
6.2	Long Term Objectives.....	23
6.3	Current Strategies and Initiatives	25
6.4	Resource Requirements.....	26
7.0	ASSET CRITICALITY.....	27
7.1	Criteria.....	27
7.2	Usage of Criticality Model	29
8.0	CURRENT STATE.....	30
8.1	Historical Costs.....	30
8.2	Asset Condition and Trends	35
8.3	Asset Performance.....	36

8.4 Performance and Practices Benchmarking..... 38

9.0 RISK ASSESSMENT 39

10.0 STRATEGY AND FUTURE STATE..... 44

10.1 Future State Asset Performance..... 44

10.2 Strategy..... 45

10.2.1 Sustainment Strategy 45

10.2.2 Growth (Expand) Strategy 46

10.2.3 Strategy for Managing Technological Change and Resiliency 47

10.3 Planned Future Investments/Spend Levels 49

10.4 Implementation Risks..... 50

Table 10.4-1, Implementation Risks..... 52

10.5 Asset Conditions and Trends..... 53

10.6 Performance and Risk Impact 55

10.6.1 Safety Risk 56

10.6.2 Reliability Risk 57

10.6.3 Financial Risk 59

Table 10.6-3, Strategy, Risk Assessment Financial..... 59

10.6.4 Environment/Trustworthy/Stewardship..... 60

Figure 10.6-4, Strategy, Risk Assessment Environment/Trustworthy/Stewardship..... 60

10.6.5 Compliance Risk 61

Table 10.6-5, Strategy Risk Assessment Compliance..... 61

11.0 ADDRESSING BARRIERS TO ACHIEVING OPTIMAL PERFORMANCE..... 62

12.0 DEFINITIONS..... 63

1.0 EXECUTIVE SUMMARY

The Office of Security & Continuity of Operations (OSCO) Strategic Asset Management Plan (SAMP) documents the current state of BPA's physical security assets and describes planned asset management improvements, maturity and competencies needed to effectively and efficiently manage the entire lifecycle of BPA security system assets. The SAMP aims to provide alignment between the agency strategy, various business models, stakeholder requirements, organizational objectives and resulting asset management objectives to ensure assets are managed and measured in creating and delivering value to BPA. OSCO's capital and O&M programs were added as an asset category in 2021, and this is the first strategic asset management plan under the new format initiated in 2021.

OSCO is accountable for supporting Bonneville Power Administration's (BPA) mission and stakeholder interests by protecting BPA's people, facilities, critical systems, and information. The scope of the Physical Security Program covers multiple states across a broad service area, and includes more than 450 facilities, 15,000+ miles of high voltage transmission lines, over 5,000 employees and contractors, as well as thousands of visitors each year. OSCO implements physical security requirements as well as security system designs and standards BPA is compliant with regulatory requirements, guidelines, provisions and principles prescribed by the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), Federal Energy Regulatory Commission (FERC), the U.S. Department of Energy (DOE), and U.S. Department of Homeland Security (DHS).

There are three primary objectives to this strategy:

1. Reduce vulnerabilities and risk: The "One-BPA" (Transmission, Facilities, IT, and OSCO) adherence to NERC CIP, DOE's Design Basis Threat (DOE O 473.3C) coupled with implementation of security enhancements to reduce vulnerabilities and risk. For BPA, assets identified under NERC CIP 006 and 014 are a subset of the DOE Design Basis Threat (DBT), which addresses BPA's most vulnerable energy delivery facilities.
2. Continued execution of capital security enhancement initiatives: These initiatives provide sustainable and increased levels of security for BPA and are focused on our most critical assets.
3. Development of a lifecycle management program: Upgrading and/or replacing aging electronic security systems at both energized and non-energized BPA facilities is critical to the health of the security program and the safety and security of BPA assets and personnel.

OSCO's intent is to establish and maintain an adequate baseline level of security commensurate with criticality, as well as take into account the unpredictable nature of threat activity and resulting security conditions. As such, the physical security prioritization process must remain flexible and allow for implementation changes based on an environment where security threats or conditions can change with little advanced warning. Ensuring adequate protection of identified NERC CIP 006 and 014 high-voltage assets comprises the lion's share of effort to execute OSCO's respective capital security program and projects over the timeline of this strategy document.

This strategy also addresses the risks while remaining cognizant of staffing, rise of inflation for capital projects increasing the need for capital funding, and O&M/funding limitations. In the simplest terms, the older the security system asset the more costly it is to maintain and the more labor hours needed to perform maintenance. Aged security assets have longer downtimes, which influences already flat expense budgets and will more than likely cause outage restoration delays.

At current staffing and funding levels (Capital, O&M/expense), OSCO will only address short-term "break fix" needs, and will not be able to implement a more robust and necessary capital replacement program. This document will lay out, in detail, the current cost and trajectory as well as a path forward.

2.0 ACKNOWLEDGEMENTS

Our mission in the Chief Administrative Office (CAO) is to ensure that Bonneville Power Administration's (BPA) internal services are strategically aligned, that work is clearly prioritized and well executed, and communications are effective. Investments in facilities and delivery of business services are aligned with BPA strategic business objectives and support the safe performance of core business activities across the organization. We will demonstrate our commitment to asset management principles in the following ways:

- Align investment in assets and services in accordance with organizational objectives to support BPA's core business;
- Continuously improve awareness of asset management activities in order to execute day-to-day operations in a cost effective manner; and
- Make risk-informed decisions to maximize the value of our facilities and services while improving safety and environmental stewardship.

I am extremely proud of the work that our team achieved over the past year to develop our business in accordance with asset management principles. Looking forward, we see that the future brings challenges and opportunities for our organization. We welcome this opportunity to push ourselves and take major steps towards our goal of becoming a valued partner recognized for our operational excellence through improvements in asset management.

Robin Furrer
Chief Administrative Officer

2.1 Senior Ownership

The Chief Security Office staff as well as Facilities and Workplace Services, Software Development & Operations, and Transmission Services review the Office of Security & Continuity of Operations' (OSCO) Strategic Asset Management Plan (SAMP) internally. This document is the culmination of a holistic Agency strategy developed with key stakeholders to define the current and future state of the OSCO capital portfolio, resources and funding required reaching future state goals, and necessary data to inform, maintain and improve the health of the capital portfolio. The managers of each contributing stakeholders group reviewed and support the conclusions and recommendations contained in this document.

2.2 Strategy Development Approach

In order to provide the necessary lifecycle security planning, projects and services, this document was developed closely with a multitude of stakeholders, partnering organizations, and subject matter experts (SMEs) to ensure that the strategic approach is vetted, resourced, aligned with Agency goals and objectives, and visible to all stakeholders. Physical Security (NNT) is the leading author of the SAMP with focused contributions and refinements from the key contributors listed below. This is the first iteration of the OSCO SAMP and as such the process to refresh this document focused on the integration of contributors feedback, updates to tracked performance metrics and the resulting impacts to the portfolio health, a renewed focus on risk identification and risk based decision making, and an updated strategy that incorporated lessons learned gained by reviewing the impacts of the last strategy.

2.2.1 Key Contributors

- Manager, Office of Security & Continuity
- Supervisor, Physical Security
- Manager, Facilities and Work Place Services
- Supervisor(s), Facilities Planning and Projects
- Manager and Supervisor(s), Transmission Project Management
- Manager and Supervisor(s), Substation Engineering (Electrical, Civil/Structural, Telecom)
- Manager and Supervisor(s), Transmission Field
- Manager and Supervisor, Software Development and Operations
- Asset Strategist for Finance Capital Investment
- Enterprise Risk Management

2.2.2 Key Activities

- Identify assets
- Identify key stakeholders
- Assess the security capital asset management maturity level
- Develop strategy objectives
- Determine and document asset criticality levels
- Review and document the current health of security assets
- Benchmark program performance against industry standards
- Identify risk and risk based decision making process
- Target and document future state performance levels
- Develop strategies to get from current state performance levels to future state performance targets

- Identify challenges and gaps that need to be overcome to achieve optimal performance

3.0 STRATEGIC BUSINESS CONTEXT

3.1 Alignment of SAMP with Agency Strategic Plan

The SAMP outlines achievable strategies that maximize the value of the BPA’s security assets while mitigating the security, reliability, financial, vulnerability and compliance risks to the program posed by a lack of security infrastructure, an aged existing security infrastructure, and new security standards and requirements to the security portfolio. This plan establishes the framework used to align our next ten years of investments and protection strategies with the two four Agency strategic goals that encompasses best security practices: 1) Strengthen financial health, 2) Modernize assets and system operations. In addition, OSCO’s strategic focus includes: 3) P1) Providing effective, repeatable and sustainable security systems and services, and 4) P2) Meeting US DOE orders, NERC CIP standards, other Federal directives, and BPA’s external and internal critical infrastructure protection objectives and needs efficiently and responsively. The guidance defined in the SAMP informs the OSCO capital program and establishes the specific targeted efforts, resources, and schedules required to support the delivery of the Agency strategic goals and objectives.

To ensure alignment with the agency strategy, OSCO’s ascribes, aligns and adapts its capital program business practices to their main collaborative leaders: Transmission and its established Transmission Business Model (TBM); Facilities’ business model; and IT’s business model. These organizations have developed value propositions and focus areas with corresponding outcomes to facilitate the delivery of the Strategic Plan (Figure 3.1-1). Each of the organization’s focus areas and outcomes tie to one or more of the agency strategic objectives four goals in order to fulfill the intent of the agency strategy. While resources are allocated to achieving the specified outcomes, the Infrastructure and Long-Term Viability focus areas are key contributors to the efforts outlined in OSCO’s current SAMP. The Asset Management Strategies and Plans presented in this SAMP support the following Strategic Plan objectives:

Table 3.1-1, SAMP Alignment

OSCO Focus Areas	Supporting Strategy, Action or Process	Agency Strategic Plan Alignment
Infrastructure > Advanced Situational Awareness > Right-sized Investments > Value and Risk-Based Asset Management	Develop asset strategies and plans that are informed by asset condition, criticality, and risk: <i>Continuous (Supporting all-source asset efforts)</i> Manage mean-time to failure (lifecycle) costs to inform investment decisions based on best value and perform alternatives analyses that also consider total lifecycle costs: <i>Lifecycle cost analyses using the risk-to-spend efficiency assessments that integrate CHR to inform all decisions of the asset lifecycle. OSCO will continue to mature/automate in order to manage investments in a scalable/flexible manner – i.e. Portfolio Optimization, Asset</i>	Objective 1a: Improve cost-management discipline Objective 1b: Build Financial Resiliency Objective 2a: Administer a security-industry leading asset management program that takes into consideration asset condition, criticality, health & risk (CHR) Objective 2b: Modernize security system operations and supporting technology Objective 3a:

OSCO Focus Areas	Supporting Strategy, Action or Process	Agency Strategic Plan Alignment
	<p><i>Rebuilds, Discreet Asset Replacements, Maintenance & Sparing strategies</i></p> <p>Partner with cross-Agency organizations to align related policy/standards/requirements, processes and systems:</p> <p><i>Continuous (Supporting all-source asset efforts)</i></p>	<p>Address security requests by using flexible, scalable and efficient solutions</p>
<p>Long-Term Viability</p> <p>➤ Integrated & Efficient Processes</p> <p>➤ Data-Driven Decision Making</p> <p>➤ Innovation & Continuous Improvement</p>	<p>Develop and Implement Criticality, Health, and Risk criteria to inform how much maintenance should be done on a given system or asset, when investment decision should be taken, prioritizing highest values assets for an investment decision that considers all risk dimensions:</p> <p><i>Continuous (Development initiated in FY18).</i></p> <p>Develop performance metrics that informs asset investments and impacts to energy delivery and non-energy delivery facilities’ electronic and physical security objectives</p> <p><i>Development and Improvement of best security practices through: BPA’s Critical Asset Security Plan (CASP) that provides BPA’s strategy for the implementation of Department of Energy (DOE) Safeguards and Security (S&S) programs as they relate to protecting critical assets. Supports the implementation of the DOE Design Basis Threat (DBT) (DOE O 470.3C), NERC CIP – Standards 006 and 014, “Physical Security of Critical Cyber Assets, Department of Homeland Security Presidential Directive - 12 (HSPD-12), and BPA’s infrastructure protection policies, standards, and requirements.</i></p>	<p>Objective 1a: Improve cost-management discipline</p> <p>Objective 1b: Build Financial Resiliency</p> <p>Objective 2a: Administer a security-industry leading asset management program</p> <p>Objective 2b: Modernize security system operations and supporting technology</p> <p>Objective 3a Address security requests by using flexible, scalable and efficient solutions</p> <p>Objective 4b: Develop and Implement policies, standards, requirements, specifications to include cost estimation and out-year capital program forecast for Agency planning and optimization</p>

3.2 Scope

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

- Establish a security system lifecycle management program. Such expense program shall cover O&M needs for all facilities with electronic security systems.
- Manage security information (i.e video imaging, physical access logging, intrusion detection alarming) through the IT security management software
- Forecast, prioritize, fund, and implement a sustainable NERC CIP 006, electronic security system capital program for aging security infrastructure to effectively establish a security system lifecycle management program.

- Forecast, prioritize, fund, and implement a sustainable NERC CIP 014 security system, capital program that is economical, risk informed, and ensures reliable system performance.
- Transmission and Facilities upgrade projects and new construction projects incorporate Agency, DOE, and national level standards. .
- Upgrade projects and new construction by Transmission and Facilities incorporate required security measures and related costs into individual projects. All resulting security systems included in future asset lifecycle management planning as well as a sustainable maintenance program.

Outside the scope of this strategy are:

- OSCO does not physically own the IT hardware and software; nor the physical security parameters of BPA’s facilities (i.e. perimeter fence of a high voltage yard or maintenance headquarters and their associated gates)
- BES Cyber security systems
- IT infrastructure (networks, servers, etc.) associated with electronic security systems (ESS) used to operate the digital security components
- Administration, maintenance, and cyber security elements used to manage video and alarm data feeds

OSCO coordinates with Information Technology, Transmission, and Facilities to ensure the related physical security standards and requirements are addressed in the appropriate asset management plans.

3.3 Asset Description and Delivered Services

The purpose of security system assets is to implement BPA security requirements, standards, and industry best practices for the protection of BPA energy delivery and non-electrical facilities, assets, and personnel as well as meeting regulatory compliance requirements. BPA defines a *security asset* as material, equipment, software or hardware that is used for the primary purpose of providing physical security protection. Individual assets or components make up security systems that collectively provide various levels of physical security protection depending on the asset being protected. Table 3.3-1, Assets outlines the system functions, their purpose, and examples of the types of components included in each system.

Table 3.3-1, Assets



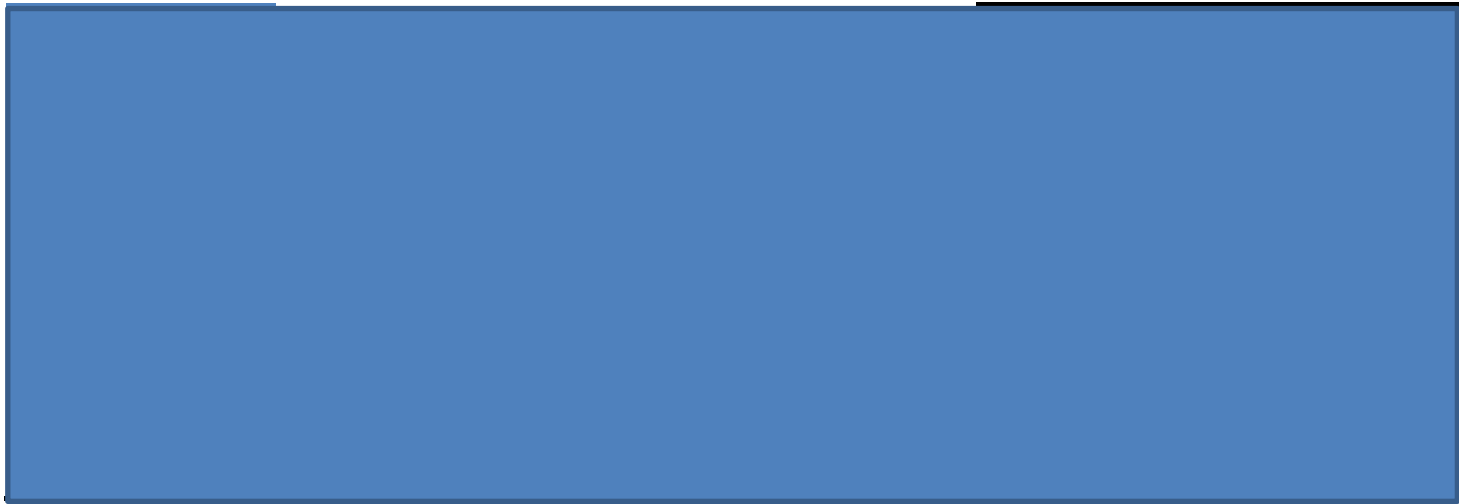
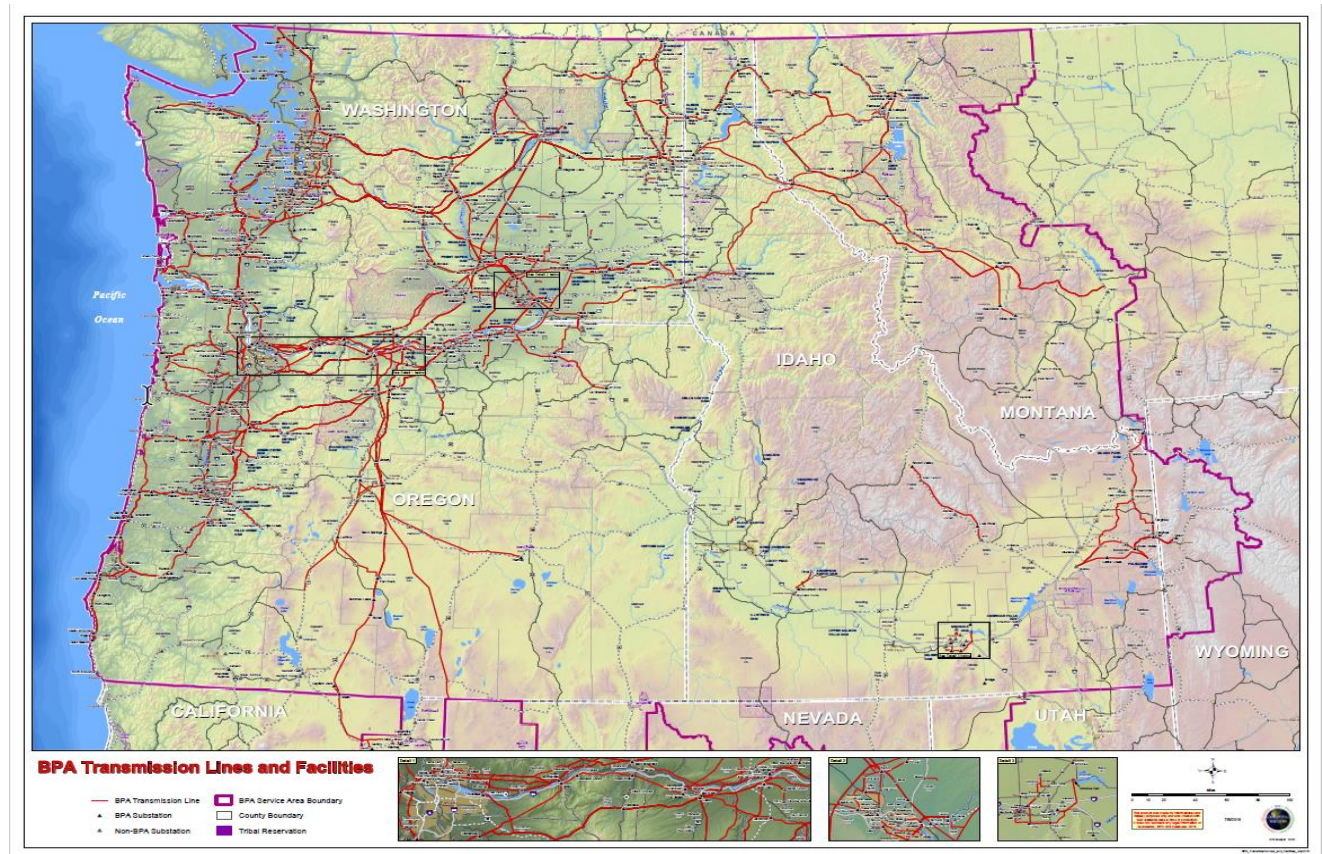


Figure 3.3-2, Asset Locations

BPA has currently built 13 sites supporting full or partial NERCCIP 014 security enhancements and is currently operating over 12,000 electronic security devices in the protection of over 115 separate facilities made up of NERCCIP Medium and Low energized substations, Maintenance Headquarters, Office Buildings, Aircraft Hangars, Control Centers, and three complexes (Ross, Munro, and Celilo).



Security assets seek to mitigate security risk for BPA sites through the holistic approach of deter, detect, delay, communicate, assess, and respond, which considers the totality of security systems, procedures, policies,

employee training, security outreach, continuous threat and intelligence awareness and other security related activities. When combined with the physical security system, the approach will reduce the risk associated with a physical attack posed by the criminal threat, which OSCO evaluates as having the highest probability of occurrence for BPA. Along with targeting a significant reduction in risk associated with criminal activity such as burglary, vandalism, and similar crimes, BPA gains peripheral risk reduction benefits against other evaluated elements of the threat spectrum. This approach is in alignment with BPA’s Critical Asset Security Plan (CASP) and the associated DOE, NERC, and HSPD-12 requirements the CASP addresses.

3.4 Demand Forecast for Services

OSCO’s physical security demand forecast and support includes its own planning and implementing of the capital program, asset modernization, expense O&M services, and “one-off” security project needs for full support established protection standards and best security practices. Demand for security-related services associated BPA’s Transmission and Facilities’ design/build capital forecast is expected to increase over the next 10 years based on the current rate of project execution and/or expected forecasted projects from Transmission and Facilities.

As BPA constructs new facilities or retrofits existing facilities, we will continue to see steady growth in the number electronic security system assets across BPA’s service area. For each current and future energized and non-energy delivery facility, corresponding forces affecting the demand for services and the dire need for a healthier expense budget include:

- Emerging Transmission and Facilities Business Requirements (Asset Modernization)
- US DOE Orders, NERC CIP Compliance, BPA Security Policy, Best Security Practices (Asset Regulations)
- Workforce Fluctuation (Asset Optimization)
- Asset Condition (“One-off” Needs, O&M Services)
- Ongoing lifecycle management

3.5 Strategy Duration

Duration of this SAMP is 5 years with a refresh every 2 years, unless there is a significant change in strategy at the annual review.

4.0 STAKEHOLDERS

4.1 Asset Owner and Operators

BPA security asset owners and operators are divided between Transmission, Facilities, Software Development & Operations, and OSCO serving all of BPA’s facilities. However, the majority of security measures support the Transmission Services operation of field sites.

In 2009, BPA’s NERCCIP 006 program led by OSCO began with the responsibility for funding, through Transmission, the installation, maintenance, replacement, and retirement of electronic security systems. While daily O&M actions are performed by Software Development & Operations staff, the expense funding for maintenance, repair and renewal is the responsibility of OSCO.

In 2014, BPA's NERCCIP 014 program led by OSCO began with the responsibility for capital funding, through Transmission, the expansion of protective measures at BPA's most critical facilities. These measures include the physical hardening of facilities against specific threats as well as an expansion of electronic security systems to substation yards. Once completed, physical improvements, such as fence lines, fall under daily O&M actions by Transmission, while the Software Development & Operations staff utilize expense funding for maintenance, repair and renewal of electronic security systems. Funding for electronic security system O&M is the responsibility of OSCO.

Office of Security & Continuity Office (OSCO) –

- Is the BPA programmatic office that develops BPA security policies, requirements, conducts risk assessments, prioritizes assets based on criticality and threat, and conducts system performance tests and final security system acceptance
- Identifies criticality of information contained on information systems in support of FISMA (Federal Information Security Management Act) requirements
- Information owner associated with electronic security system data
- Provides funding and program management of NERC CIP Capital Budget for CIP 006 and 014 security enhancements
- Provides funding in support of the day to day electronic security system maintenance activities
- Approves system access
- Prioritizes break/fix and project requests for electronic security systems

Software Development & Operations –

- Responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of information and electronic security systems
- Develops system design specifications to ensure the security and user operational needs are documented, tested, and implemented
- Ensures compliance with FISMA and NERC/CIP specific to the devices and supporting information systems
- Supports the information system owner in selecting security controls for the information system
- Participates in the selection of the organization's common security controls and in determining their suitability for use in the information system
- Reviews the security controls regarding their adequacy in protecting the information and information system

Transmission and Facilities –

- For each respective main organization and their capital out-year planning, will program/project manage the funding, scope, design, and construction of facilities incorporating US DOE, NERC, BPA, and best security practices within their programs and projects
- Identifies and prioritizes critical infrastructure in support of NERC CIP standards
- Provides NERC CIP oversight and guidance
- Provides security system estimating

Fences and gates capital and/or O&M program management responsibility consist of:

- OSCO – Delivers capital security perimeter fencing and gate upgrades for NERC CIP 014 sites and associated protection strategies, but does not fund or conduct O&M activities
- Transmission – Energy delivery sites’ perimeter fencing/gates for new build, lifecycle replacement, and maintenance (requires bonding/grounding)
- Transmission - Energy delivery sites’ interior fencing/gates for new build, lifecycle replacement, and maintenance (requires bonding/grounding)
- Facilities - Non-energy delivery facility/sites’ fencing for new build, lifecycle replacement, and maintenance (no bonding/grounding)

4.2 Stakeholders and Expectations

BPA security asset stakeholders are identified as managers, supervisors, employees, contractors and the facilities directly or indirectly impacted by the overall security program. During program management, project planning, and specialized work plan development, all stakeholders are identified and consulted. Our primary stakeholders are the BPA organizations with shared responsibility and/or approval authority for operational, capital/expense, and compliance requirements, e.g., tenants (Regional Managers/District Managers/staff), Transmission/IT/Facilities functional work groups, cross-agency Program Managers, and Subject Matter Experts from standards, compliance, and service organizations (Finance, Environmental, Historical, All-source Architecture and Engineering, Safety, Security, and IT).

Table 4.2-1, Stakeholders

Stakeholders	Expectations	Current Data Sources	Measures
Customers	Low Rates	Long Term Rates Forecasting Tool, Focus 2028	Rate Forecasts, Long-Term Planning
	Reliability	ISC-RMP, US DOE	Design Basis Threat, Facility Security Level
	Quality	Asset registry database	ASTM, FISMA, NERC CIP
BPA	Safety	Industry regulations and standards	Incident report records, documentation of non-compliance, facility safety actions
	Flexible Operations	ProjectWise, Procore Transmission Program Report System	Continuity, Forecast, and Operations Plans
	Competitive Costs	Financial system, Transmission Estimating	Audited and reporting of financials, historical estimating to forecast out-year projects
	Reliability	Ocularis, Prowatch, GIS	Security Alarm and VASS statistics; site plot plans

	Accountability	Key performance indicators Business cases	Annual staff and performance reviews Business case targets
	Compliance	Resolver	Internal/External Auditing, Decision Documentation, Self-Reports
	Environment	Industry regulations and standards (NEPA)	Environmental Assessments Pollution Abatement Clearances
	Trustworthy	Financial system	Risk and Vulnerability Assessments
	Stewardship	US DOE and BPA Security standards and requirements	
	Cultural Resource Stewardship	Industry regulations and standards (NEPA)	SHPO Programmatic Agreements and Memoranda of Agreement
	Risk Exposure	Risk analysis models in business cases	Risk ranking
NERC/WECC	Regulation Compliance	Resolver	Internal/External Auditing, Decision Documentation, Self-Reports
Staff	Health and Safety	Safety database	Incident statistics
	Job Security and Satisfaction	Administrative database	Staff survey results, turnover figures
	Training	Administrative database	Agreed professional development
	Safety	Industry regulations and standards	Safety Metrics (Lost Time Accident Rates, Days Away Restricted or Transferred, Total Case Incident Rate)
Public	Safety	Public safety management system	Non-conformance records
	Security	Security Incident Reports	Nefarious Activities, Complaints

5.0 EXTERNAL AND INTERNAL INFLUENCES

There are three main challenges that must be overcome for successful implementation of this strategy:

Rapidly evolving regulatory requirements

NERCCIP 014 is accepted as the latest NERC requirement to implement increased security at critical locations within BPA’s footprint. DOE Order 470.3C, Design Basis Threat (DBT), requires BPA to assess and use risk-based approaches for the protection of all facilities. If a new physical security standard is deployed that BPA must comply with, this strategy may need to be revised.

Aging and technologically obsolete systems

A large number of BPA’s security systems are failing, or are projected to fail in the coming years due to exceeding the asset’s lifecycle. If not managed, this will negatively affect NERC-CIP and US DOE DBT compliance, security system effectiveness, and cause a tremendous increase in maintenance fees and drain limited BPA and contracted resources.

The current situation is that many of our electronic security systems used to protect facilities are at end of life based on a seven-year life expectancy. Of our NERC-CIP 006 protected field sites, over 80% are at or beyond end of life expectancy.

Emerging Threat Environment

The security threat environment is always changing and new threats continue to emerge across BPA’s service area, as well as nationally. NNT monitors security threat activity through its Threat Awareness/Threat Management program with the intent on adjusting security operations as needed. Although changes in security operations or posture are typical tactical approach, more strategic approaches involving security assets may be needed to help mitigate risks to BPA from a long-term threat perspective.

Table 5.0-1, External and Internal Influences

External Influences	Affects and Actions
NERC and WECC mandatory reliability standards	Demonstrating compliance increases OSCOs operating cost and continues to demand significant human resources
Specialized material and engineering standards	Procurement and engineering costs are high
Modern security systems are more complex with integrated technology	Workforce design, construction and O&M competencies need to keep pace with the implementation of technology. This requires an investment in our people to keep them competent
Market conditions and constraints (Design/Build) due to an abundance of commercial/residential sector work	Higher bid prices on design/build limits the amount of work that can be performed with a fixed budget. Increased and shared capital funding across IPR windows would allow funding gaps in lean years to be applied in times of increased market pressure
Internal Influences	Affects and Actions
Increased O&M	As more facilities are built the increase in security system needs must be applied, increasing funding for O&M and “one-off” expense is mandatory
Construction and project delivery methods	BPA’s procurement regulations and delivery methods are challenged to keep pace with the private sector. This puts BPA at a disadvantage in today’s constrained construction market
Staffing constraints (number and skills, competitiveness of labor)	Contracting and project management staffing are limited for facility assets and represent a bottleneck for execution OSCO capital portfolio
Contracting processes	Availability and use of standardized project delivery methods, tools, and templates are lacking and inconsistent. Individual CO knowledge and practices also vary considerably, impacting the amount of work and rework needed for contract development
Funding Allocations	Resource tradeoffs are frequently made between addressing urgent and necessary break/fix O&M actions, “one-offs”, and planned renewal and replacement of security system assets. The lack of a adequate funding for security system O&M diverts human and fiscal resources away from lifecycle planning and renewal and ultimately perpetuates a reactionary approach to asset management

<p>Attraction and retention of high-quality talent will be challenged by an increasingly competitive, innovation-filled energy industry landscape</p>	<p>BPA’s workforce has been and continues to be a top enterprise risk. With high retirement rates and other attrition, BPA must provide greater opportunities and competitive pay to keep and attract a qualified workforce. Greater innovation and use of best industry practices will not only help with retention but will also reduce project cost and duration.</p> <p>Transmission, Software Development & Operations, and Facilities’ workforce is highly specialized, limiting opportunities to address workload peaks and adding cost to scoping and preliminary engineering activities. Subject matter expertise is needed and should be retained but BPA should also consider cross training and utilizing its talent more as generalists to increase engagement and reduce cost</p>
---	---

Standing requirements and to achieve best security practices and compliance with the following protection standards set by:

- BPA’s Critical Asset Security Plan (CASP). This document lays out BPA’s strategy for the implementation of Department of Energy (DOE) Safeguards and Security (S&S) programs as they relate to protecting BPA’s critical assets.
- The CASP supports the implementation of:
 - DOE Design Basis Threat (DBT) (DOE O 470.3C)
 - North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards – Standards 006 and 014
 - Department of Homeland Security Presidential Directive - 12 (HSPD-12)
 - BPA’s infrastructure protection policies, standards, and requirements.

5.1 SWOT Analysis

Table 5.1-1: SWOT

<i>Favorable</i>	<i>Unfavorable</i>
<i>Strengths</i>	<i>Weaknesses</i>
<ul style="list-style-type: none"> • Security: Increasing Agency-wide commitment to security-centric culture; where best security practices are a daily driver for decision making • Executive Support: Corporate and Transmission Senior Leadership has embraced and pushed forward security asset management as a key priority • Asset Management Capability Development: Asset Management initiatives are beginning to be used to help inform decision making from established planning to current and forecasted operation perspective • Standardization: OSCO has sponsored, developed, and established security-centered maintenance and design standards. As well has influenced other Transmission and Facilities based standards and requirements in regards to security system assets. This enables best practices and the ability to execute contracted work that necessitates quality controls while maintaining reliability • Continual improvement of Data: OSCO, Transmission, Software Development & Operations, and Facilities has developed ongoing effort to improve data quality using 	<ul style="list-style-type: none"> • Security: Resistance to certain security system standards and requirements where best security practices are to be served; creates an inability to fully influence security design/build culture • Rigid Financial vs Project Schedule: Current financial processes/policies vs project schedule are heavily influencing the execution and energization of a project. This limits the ability to be more flexible in program and project management decisions or new asset strategies • Staffing Limitations and Succession Planning: Majority of current Federal and Contracted security-SME workforce are within seven years of retirement and if not overlapped with new hires will leave a gap in knowledge transfer • Aging Infrastructure: Security systems are at end-of-life fosters an environment of increased security risks such as vandalism, property destruction, US DOE and NERC non-compliance, technological obsolescence, etc. Furthermore, deferring replacements limits BPA’s ability to control costs

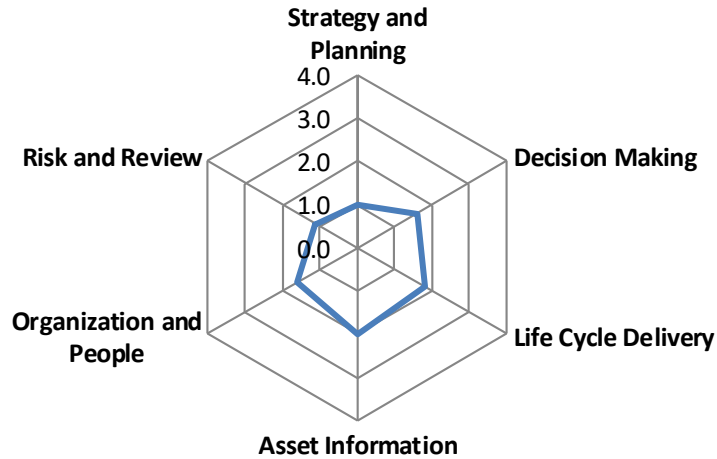
<p>historical projects to empower current and forecasted projects and best security practices</p>	<ul style="list-style-type: none"> • “After 10 Years”: Due to IT software, security system, and device technology changes and Mean Time to Failure rates of said technology; longer term planning of asset replacements/upgrades must be forecasted and funded. Subsequently more expense funding is needed to execute O&M tasking • Break/Fix and “One-off” Actions: Unplanned/tactical O&M and “one-off” actions routinely consume staff time and organizational budget detracting from strategic goals • Transmission vs. Facilities 1: Competing projects and process management systems between different business lines introduce complexity to security project teams • Transmission vs. Facilities 2: Multiple business line ownership of facilities assets prevents consistent delivery, results, and tracking of investment into energy vs non-electric delivery facilities
<p>Opportunities</p>	<p>Threats</p>
<ul style="list-style-type: none"> • Risk Based Planning & Prioritization: OSCO is mentored by Transmission on its path for its ongoing capability to understand asset Criticality, Health & Risk (CHR) to inform investment decisions and prioritize investments across a security system’s lifecycle • Secondary Capacity Model: Potential to improve security systems’ project scope/design/build, cost and delivery times through a adoption of alternative project delivery methods • Increase Capital Builds: As BPA increases capital builds for energy and non-energy delivery facilities, the need for more security systems are need for over-all compliance and best security practices 	<ul style="list-style-type: none"> • Increasing Capital Costs: Escalating software, hardware, design/build/maintenance contracted and operating costs are forecast to consume a growing portion of project financial health • Supply Chain and Labor Shortage: Short-term escalation in material and labor costs in availability due to economic conditions related to COVID-19 Pandemic • Staffing Limitations and Succession Planning: Federal and Contracted SME staff retention across project teams can negatively impact project continuity • Security Threats: Increasing cyber and physical security threats will always be prevalent; however up-to-date technology, tactics, and procedures must be in place to counter such threats • Compliance: Evolving compliance requirements from DOE, NERC, and national policies hinder solid security foundations for Agency needs

6.0 ASSET MANAGEMENT CAPABILITIES AND SYSTEM

The current state of OSCO’s security systems asset management capabilities is continuing to mature over time with a current overall maturity level of 1.5 as of this writing. The program assessment is conducted by the OSCO’s Chief Security Officer, Physical Security Supervisor, and Physical Security Specialist/Program Manager.

6.1 Current Maturity Level

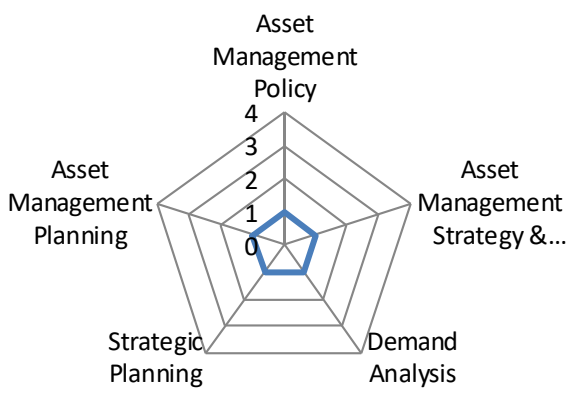
Asset Management Capabilities and Systems average a maturity level of **1.5** across all subject groups in the Institute of Asset Management (IAM) Asset Management Maturity model. The current Maturity Level score of OSCO’s security system asset operations, maintenance determinations, and management function, integrated with NERCCIP 006 and 014 asset project planning, renewal/replacement, and retirement often limits efforts to advance the security program to the Optimizing and Excellence levels. The results are a strategic choice-based execution in recent years, but primarily tends to be more of a reactive-centered program that addresses short-term needs dependent upon security and compliance situations.



Innocent	Aware	Developing	Competent	Optimising	Excellent
Maturity Level 0	Maturity Level 1	Maturity Level 2	Maturity Level 3	Beyond	
The organisation has not recognised the need for this requirement and/ or there is no evidence of commitment to put it in place.	The organisation has identified the need for this requirement, and there is evidence of intent to progress it.	The organisation has identified the means of systematically and consistently achieving the requirements, and can demonstrate that these are being progressed with credible and resourced plans in place.	The organisation can demonstrate that it systematically and consistently achieves relevant requirements set out in ISO 55001.	The organisation can demonstrate that it is systematically and consistently optimising its asset management practice, in line with the organisation's objectives and operating context.	The organisation can demonstrate that it employs the leading practices, and achieves maximum value from the management of its assets, in line with the organisation's objectives and operating context.

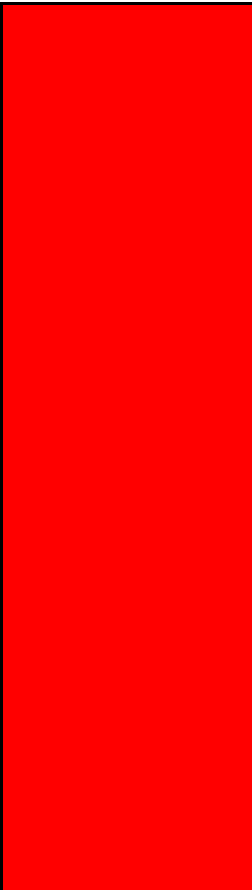
Table 6.1-1 Maturity Level

Subject Area	Maturity Level
Strategy & Planning	<p>Maturity level 1</p> <p>Strengths: Planning of O&M and capital security enhancements are integrated with budget forecasting and annual work plans. The site locations are bundled and developed, yet flexible if security needs arise, serving to inform resource requirements and sequencing needed to attain the targeted security asset health goals for its portfolio. OSCO and Software Development & Operations can respond to changes to its short and long-term project forecast with agility while understanding the downstream impacts to project sequencing and fiscal spend.</p> <p>Weaknesses: Competing Transmission and Facilities capital and O&M planning and projects can interfere with OSCO's security system planning and execution. Improvement with respect to Integrated Work</p>

	<p>Planning and interagency coordination, SME asset allocation, more consistent project scheduling and more predictable procurement timelines are needed to enhance the fidelity of strategic plans.</p> <p style="text-align: center;">Strategy and Planning</p> 
Decision Making	<p>Maturity level 1.6</p> <p>Strengths: OSCO follows the Transmission Capital Investment Acquisition (CIA) process which is in place and operational. Investments put forward are given advanced visibility within OSCO's Asset Plan, preliminarily scoped and vetted through the CAO office prior to inclusion and execution. Security system and device materials lifecycle cost analysis remain inconsistent.</p> <p>Weaknesses: Decisions to approve capital investments through the expense section of a business case do not flow fully to OSCO expense bins ensuring necessary expense required to maintain the assets in out years, and the OSCO expense budget is often scrutinized to achieve Agency expense targets leaving OSCO and Software Development & Operations with insufficient funds to maintain security system assets from investments.</p>

	<div style="text-align: center;"> <h3>Decision Making</h3> </div>
Life Cycle Delivery	<p>Maturity level 1.8</p> <p>Strengths: OSCO, for the last six (6) years, has ensured US DOE, NERC, and BPA’s best security practices, policy, standards, and requirements are a dequately defined and followed through a asset delivery to O&M scheduling. This is an ongoing process and improvements are made every year but standardization of the scoping/programming phase, implementation of change control processes, and quality management plans have given the capital and O&M programs positive drive, which is reflected in the current performance of OSCO’s capital security enhancement program’s lifecycle.</p> <p>Perimeter Fence –</p> <ul style="list-style-type: none"> • OSCO: Energized substation perimeter fencing upgrade (NERC CIP014 capital program sites only) • Transmission: Energized substation perimeter and interior fencing/gates lifecycle replacement (Energy delivery sites, requires bonding/grounding) • Facilities: Non-energized facility/site fencing lifecycle replacement (no bonding/grounding) <p>Weaknesses: Perimeter fencing standards and specifications are established yet a lack of cross-Agency cooperation for the lifecycle replacement of perimeter fences for energy and non-electric delivery facilities can lead to unsafe and unsecured BPA property.</p> <p>The lack of a centralized authority in regards to O&M and “one-off” expense activities impairs standardization and consistency across the portfolio. Increased pressure on available expense funding due to increases of security system builds. The lack of O&M funds will hinder the ability to invest in mid lifecycle renovations resulting in less than ideal asset lifespans. Software Development & Operations fund (through CIO/IT) the O&M budget and carry-on O&M activities with informs to OSCO, Transmission, and Facilities stakeholders.</p>

	<h3 style="text-align: center;">Life Cycle Delivery</h3>
<p>Asset Information</p>	<p>Maturity level 2</p> <p>Strengths: Currently Sunflower is the asset management system used for certain security/IT centric devices. Transmission Estimating tracks all cost information of electronic security systems and devices, and physical security systems (fences, gates, security poles, concrete, conduit, fiber/power, and scope/design/build/decommissioning) as a holistic security system for BPA facilities.</p> <p>Weaknesses: Transmission Estimating of security system cost-information are immature for it was established within the last six years. Software Development & Operations stores its data independently as per organizational process.</p> <h3 style="text-align: center;">Asset Information</h3>
<p>Organization & People</p>	<p>Maturity level 1.6</p> <p>Strengths: The full Cross-Agency security team consisting of Federal and Contract SMEs and staff is and provides a diverse range of skillsets and high level of engagement. The productivity of staff has remained consistently high. Procurement and supply chain processes are in place.</p> <p>Weaknesses: Asset management competencies and understanding is still new to OSCO. Lack of defining security asset management roles and responsibilities across BPA stakeholders slows the development of</p>

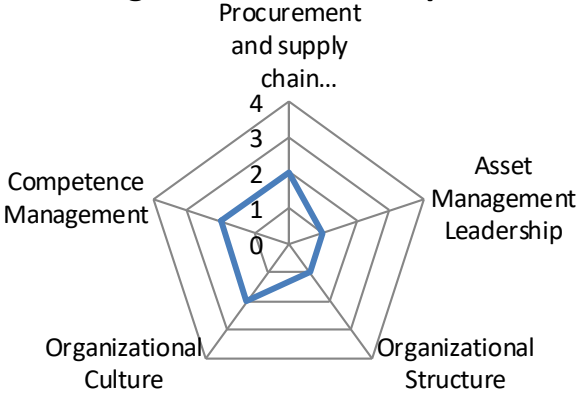


skills and competencies required to align with industry standards. Additionally, it allows for conflicting priorities that will lengthen the time it takes to understand and embrace IAM values and best practices.

OSCO capital security projects are executed in partnership with Facilities, Supply Chain, and Transmission. The partnering orgs reside in geographically different locations and OSCO work represents only a small portion of their workload. This introduces challenges to both workflow, communication and culture.

Staff retention has remained a consistent issue as SME support movement (contract officers, project/construction management, engineering, IT) limits the ability to hold gained ground on strategies and prioritization. This churn slows the maturation of the program and diverts focus from high priority planning issues.

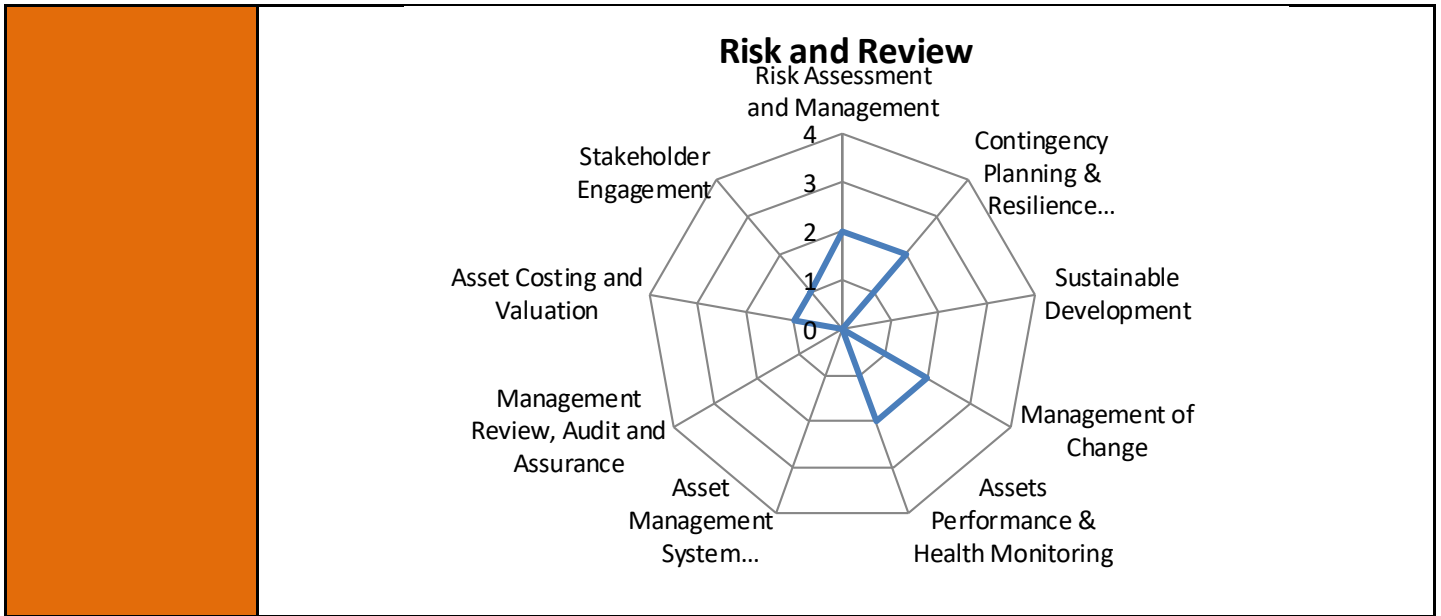
Organization and People



Risk & Review Maturity level 1.1

Strengths: Stakeholder engagement in regards to security needs are listened and adhered to however security integration priorities are not always in alignment. Discussions on how best to use resources are regularly held and there is mutual acknowledgement of each party's needs.

Weaknesses: Change management improvement is needed with respect to full understanding and acceptance of all-source security policy and standards for BPA facilities. Given the lack of BPA's full commitment to best security practices, limited fiscal and budgeting of security system will not be achieved. It is imperative that investment decisions prioritize security needs as a criticality program for proper IAM, best security practices, and US DOE and NERC compliance.



6.2 Long Term Objectives

OSCO’s primary long-term objective is to achieve asset Maturity Level 2 (Developing) in the area of **Life Cycle Delivery** by or before the second update to the SAMP (2024). Data tracking, security systems standardization, resourcing will assist and guide informed risk and decisions; improve and streamline capital forecasting and routine O&M; and resourcing at the right level will help to improve the lifecycle delivery of the capital and O&M portfolios by increasing the throughput of strategic initiatives.

OBJECTIVE 1: LIFE CYCLE DELIVERY

OSCO, Software Development and Operations (JLS), Transmission, and BPA Facilities are increasing their knowledge to apply best industry standards to manage their capital and O&M (and “one-offs”) projects to include the nexus they will have with including security systems assets. OSCO, in itself, has a very young NERC CIP 014 capital program (six years old) and it is launching the NERC CIP 006 “Refresh/Upgrade” capital program for electronic security system (ESS) assets as of FY22. The NERC CIP 006 capital program will be a continuous, annual program to ensure BPA’s initial capital investments in ESS remain viable and effective so they can continue protecting BPA’s operational assets and personnel. In addition, this program ensures that ESS assets remain compliant and ensures best security practices are incorporated with rapidly changing security technology (e.g. - hardware and software needs).

As BPA’s physical security assets, primarily ESS, continue to grow in number across the service area, there remains an overarching need to adequately maintain these assets through a healthy and sustainable expense budget. This is essential to protecting and maintaining the long-term value and reliability of the transmission system and is in direct alignment with the strategic plan goals 1 & 2 strengthening financial health and modernizing asset management/operations.

Understanding how existing standards, processes, and policy influence the cost of capital security systems and corresponding O&M security assets, lifecycle costs make visible the greatest opportunities for savings and a shift away from a reactionary approach to a business-driven planning, culture, and operational environment.

Specific, Measurable, Achievable, Relevant, Time-bound (SMART):

- Specific: OSCO and Software Development & Operations (JLS) will begin collecting and quantifying asset lifecycle costs for decision-making.
- Measurable:
 - OSCO and Software Development & Operations (JLS) will have an understanding of 100% of its assets and their corresponding lifecycle projected costs by EOFY 2025.
 - OSCO will work with internal business partners to determine how to deliver “One-Off” capital projects to incorporate security assets because of documented vulnerability and risk assessments by EOFY 2025.
 - OSCO will work with internal business partners to determine how to deliver small expense projects to incorporate security assets because of documented vulnerability and risk assessments by EOFY 2025.
- Achievable: OSCO will continue to determine where efficiencies can be gained with capital program integration. An example includes the decision to address NERC CIP 006 ESS lifecycle replacement with NERC CIP 014 projects as a holistic approach to integrate requirements by US DOE, NERC CIP, as well as BPA best security practices.
- Relevant: Creating a cost conscious culture that uses cost, performance and risk is described from the IAM anatomy to “help the organization on their asset management journey...adopt and improve on their asset management capabilities and deciding where to focus on systems/process etc.”
- Time bound: Due to the degree of complexity of “IT-security asset management systems”, data integration and financial mapping of an ESS asset lifecycle costs will allow the highest probability for success. In addition this effort would begin to socialize the changing of standards (both design and maintenance) to highlight which assets have the highest lifecycle costs relative to industry benchmarking or classical projections of uncapped reliability focus.

OBJECTIVE 2: IMPROVE PROGRAM STANDARDIZATIONS (Future)

As OSCO’s SAMP matures, a forecast of a possible objective has been identified and OSCO will reserve the development of this objective in time. As such, no SMART dialogue is to be developed for this possible objective.

As identified in the SWOT analysis, the US DOE, NERC, and BPA security standards will drive consistent decision making across stakeholders that integrate security systems within their design/build assets and through the O&M security system asset lifecycle. However, evolving and resistance to security system standards and requirements where best security practices are to be served will create an inability to fully influence security design/build culture.

- **Design & Construction Standards**
To positively affect Operations and Maintenance, thoughtful and forecasted security needs are determined by the decisions made during the design and construction. The more standardized the portfolio is, the more economies of scale can be leveraged in spare parts, technical training, specialized

tools, preventive and corrective maintenance tasks etc. This fact suggests a continual relationship between desired service levels and the decisions made during the design/construction phase.

- **Maintenance Standards**

Clear and objective service standards will drive the selection and implementation of industry best maintenance practices for the various assets/systems/components within the OSCO portfolio. Execution and documentation will not only result in better asset reliability, performance and lower lifecycle cost of ownership, but the historical data compiled will also inform improvements to design, service, and maintenance standards in the future.

- **Materials/Equipment Standards**

The existence of approved security systems, individual components, and software within the scope/design/build environment adds efficiencies to projects integrating security systems and removes unnecessary overhead and cost for spare parts, training, specialized tools, etc.

6.3 Current Strategies and Initiatives

OSCO and Software Development & Operations' O&M Initiatives:

OSCO funds and Software Development & Operations administers the service contract to a commercial security systems integrator for repair and maintenance support of the electronic security systems. The contract commercial security systems integrator is responsible for the maintenance and repair of electronic security systems and devices as well as providing 24/7 break-fix maintenance support. The vendor is not responsible for the maintenance or repair of the servers or network infrastructure supporting the system. Vendor support is separated in to two categories, Annual Plan of Activities (Preventive Maintenance) and Break-Fix Maintenance Support.

Software Development & Operations has “cradle to grave” responsibility for management of security devices, components, and systems that define the electronic security system, which is from the time of scoping to retirement into BPA’s Investment Recovery Center (IRC). All security devices, components and systems are acquired with a one (1) year standard manufacturer warranty and are tracked in accordance with BPA’s asset management policies.

The overall health of the electronic security system O&M program is directly dependent upon BPA’s commitment to properly fund the expense coffers as it pertains to current and future OSCO business case submittals. In conjunction, all Transmission and Facilities’ business cases of their respective capital projects must reflect the same commitment to security system expense funding allocations.

Although necessary maintenance expense funding is included in OSCO business cases, these maintenance funds do not flow from annotation of the business case into the actual OSCO expense budget. Resulting in more security systems being added, but no proper level of funding allocated to OSCO to maintain the additional security system assets.

If the lack of expense funding to support BPA’s security systems is not recognized and resolved, giving the onus of responsibility to BPA’s Finance and CAO offices, then a catastrophic degradation of critical security systems protecting BPA’s critical high voltage assets and non-energy delivery facilities will be inevitable.

*Integration of OSCO into Transmission SAMP Initiatives:***Transmission Asset Portfolio Management (TAPM)**

OSCO has fully integrated its capital security enhancement projects into the TAPM. Subsequently any Transmission funded, scope/design/built, and project-managed facility must go through the TAPM process from inception to energization. This integration has provided visibility into plan portfolio activities across all asset categories involving security systems to yield a more complete picture of emerging investments and better align resource management between OSCO, Software Development & Operations, Facilities, and Transmission.

Capital Investment Acquisition (CIA); Portfolio Management Team (PfMT); Criticality, Health & Risk (CHR)

OSCO has integrated into Transmission's Capital Investment Acquisition (CIA) and Portfolio Management Team (PfMT) processes for its capital security enhancement execution in regards to scope/design/build of security systems. OSCO's capital portfolio is included in all program and project (including financial) level tracking through the BPA Report Server. With the integration of OSCO's security needs into Transmission's processes and its criticality, health, and risks (CHR) system, OSCO can better understand the methodologies and analytical methods adopted to inform prioritization of maintenance and capital investments as it relates to security policy and systems. Transparent, objective CHR information and risk quantification will enable OSCO and its stakeholder decision makers to optimize the utilization of their respective financial streams to deliver best security practices and policies to their programs and projects.

Secondary Capacity Model (SCM)

OSCO is in discussion to adopt Secondary Capacity Model to augment the Primary Capacity Model in regards to executing projects to secure facilities that may fall into a "one-off" category due to critical security/safety needs. This approach is intended to offer flexibility as demand fluctuates and as other capacity models expand and contract. The Secondary Capacity Model is currently being used for initial projects, vendor/partner selection, and on boarding. The on-boarding process will include production of actual work products via selected pilot projects.

*Integration of Facilities SAMP Initiatives:***Program Management Information System (PgMIS)**

OSCO's security system asset projects to be funded, scoped/designed/built, and led by Facilities utilize the PgMIS called **Facilitate**. This Facilities' project management platform aids in target data tracking and report generation, earned value analysis and forecasting, improved budgeting and scheduling capabilities and generation of risk profiles at the asset and portfolio levels. The initiative is part of a larger effort to improve BPA Facilities informatics capabilities in the areas of data tracking, data standardization and increased reporting automation.

6.4 Resource Requirements

The SWOT analysis outlines various bullets for security system, resource requirements; and as such, security systems are dependent upon all-sourced BPA organizations for the overall security system health across the BPA region.

OSCO collaborates with Transmission, Facilities, and IT to accomplish all capital and expense related security projects and work to ensure full security compliance and best practices are adhered to in accordance with US DOE Orders, NERC CIP mandates, and BPA security standards and requirements. Such information and collaboration are expressed in the below bullets.

Knowledge Management:

- Through best industry security practice and security technology evolution via US DOE Security Departments and professional utility outreach and partnering, a continuous development and updating security-centered scoping and design efforts utilizing professionally engineered policies, estimates, standards, and specifications
- Electronic repository locations for security system architecture, estimates, standards/specifications, capital program and project portfolio, expense O&M portfolio

Staffing Limitations and Succession Planning:

- Federal and Contracted SME staff retention issues across project teams can negatively impact project continuity
- Majority of current Federal and Contracted security-SME workforce are within seven years of retirement and if not overlapped with new hires will leave a gap in knowledge transfer
- Human resource management for new hires and training must be planned for seamless knowledge and skillset transfer

Capital Funding Increase:

- Increase in the number of facilities being expanded and protected
- Increase in the complexity and size of these systems because of evolving security requirements
- Increase of BPA and Contracted design/build efforts, labor and material costs

Expense Funding Increase:

- Increase in capital builds leads to an increase in O&M costs
- Aging security devices/components
- Increased need to require added “one-off” security devices and associated project execution capacity
- Increase of BPA and Contracted design/build efforts, labor and material costs

7.0 ASSET CRITICALITY

7.1 Criteria

BPA’s Transmission and Facilities business lines each have criteria of asset criticality that can be found in their respective SAMP documentation. While their definitions/criteria do not align exactly for a variety of reasons, it is important to note that a security system is a sub-system of a facility’s operational aspects, similar to a fire suppression system, plumbing system, or lighting scheme.

As described in Section 3 of this SAMP, to ensure alignment with the agency strategy, OSCO ascribes, aligns and adapts its capital program business practices and their respective criticality criteria to their main collaborative leaders: Transmission and its established Transmission Business Model (TBM); Facilities’ business model; and IT’s business model.

As defined by the operational areas and in collaboration with the Transmission, Facilities, and IT portfolios, security system assets within BPA’s operational areas are grouped into five asset classifications relative to BPA’s defined asset criticality. “Criticality” in this sense pertains the asset’s importance in supporting or maintaining the bulk electric system:

- **Mission Critical:** Control centers and data centers having a direct impact on Bulk Electric System operations or outage in the event of failure.
- **Mission Essential:** Control houses, radio stations, associated facilities and backup power systems that provide for operation of substations.
- **Primary Support Facilities:** Facilities and structures that support day-to-day operations and maintenance of the Bulk Electric System.
- **Secondary Support Facilities:** Facilities and structures that support activities for routine operations and maintenance activities, training, research and infrastructure.
- **Other:** Facilities and structures mostly underutilized.

Regulatory Requirements

BPA facilities have specific requirements for physical security and will adopt a minimum security baseline for newly designed and pre-existing substations and facilities. These requirements are based on DOE’s Design Basis Threat (DOE O 473.3C), the Department of Homeland Security - Interagency Security Committee (ISC), North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards; BPA Policy 430-1, Safeguards and Security; BPA Policy 432-1, Physical Security Policy; the Department of Homeland Security Presidential Directive 12 (HSPD-12); Physical Security Requirements for NERC CIP Critical Asset Sites; and Physical Access Control and Monitoring System Design and Installation Requirements, among other sources. These mandates have been interpreted and consolidated into BPA Procedure 432-1-2, Critical Asset Security Plan, with which this policy is aligned. Physical security design details meeting the criteria of this policy reside within other standards referenced in this document.

The required security measures will align with the existing standards for sites with medium impact rated systems with external routable connectivity (ERC). By adopting this approach, BPA will focus on implementing best security practices and a consistent approach to security across the field and will allow BPA to avoid the cost of retrofitting buildings to add security measures.

Asset Categorization

Transmission Services is charged with determining if a site is considered a critical high voltage asset. The Bulk Electric System (BES) Cyber Systems Identification Process is owned and managed by BPA’s Transmission Technology organization, Security and Compliance Team (SCT). The process starts with the Transmission Customer Service organization applying the NERC BES definition to a site’s asset list and providing a pared down list to the SCT office. The SCT group then applies the applicability process from NERC standard CIP-002, resulting in a final list of High and Medium impact assets. BPA’s System Protection and Control (SPC) and Power System and Control (PSC) groups are responsible for identifying the BES systems for the Control Center (High) and field sites (Medium) for these assets. The generated lists are validated and then approved by the BPA CIP senior manager and the process is reviewed annually. See NERC standards CIP-002, CIP-005, CIP-006, and CIP-014 for more information on NERC asset categorization and how this applies to physical security. BPA process documentation is also located on the SCT/Transmission Technology group internal website.

Facility Criticality for OSCO

The Critical Asset Security Plan (CASP) (BPA Procedure 432-1-2) provides physical security performance requirements for facilities determined to be critical assets under DOE Order 470.3C, Design Basis Threat (DBT), and categorizes Department assets into levels or categories based on consequence of loss. Protection Levels (PLs) are defined for each category of assets. BPA assets are currently categorized as PL 6 through PL 8. The DBT, along with other regulatory requirements, influences how BPA protects its assets. OSCO develops and maintains security requirements for BPA facility assets using a graded approach. This approach takes into account the facility protection level rating as well as a site-specific assessment. Physical security requirements and associated security assets are intended to provide a layered approach with increasing security infrastructure, processes and procedures radiating concentrically inward from the outer perimeter to the innermost areas required to be protected.

The need for security assets (e.g. – electronic security systems, fences, barriers, etc.) at a particular site or facility is dependent on the criticality of the BPA asset being protected. The Security Protection Level and their general performance requirements are officially described in the CASP. The following is a brief description of the Protection Levels that are applied to BPA’s facilities and their subsequent criticality as it pertains to the assets importance in supporting or maintaining the bulk electric system:

- PL 6 High Impact – Control Centers only. (2)
- PL 6 Medium Impact – BPA’s most critical substations of such importance that their loss would immediately jeopardize the transmission system as well as vital substations with substantial importance for supporting the transmission system. (72)
- PL 6 or PL 7 Medium Impact – Other BPA facilities. Assessments and recommendations generally made based on site-specific needs. May be energy delivery facilities or Non-Energy Delivery Facilities such as maintenance headquarters. These sites represent varying importance to BPA operationally, and may be protected based on risk or other security assessments. (60+)
- PL 7 Impact Designated Facilities – These sites represent varying operational importance to BPA and include Low BES sites and below, and to include administrative facilities (owned or leased by BPA). (120+)
- PL 8 Personnel - PL 8 assets are personnel. PL 8 is used in conjunction with other PLs, not as in standalone PL.

7.2 Usage of Criticality Model

As annotated in above sections, OSCO is dependent upon the Transmission and Facilities criteria models for establishing security project criticality such as an energy delivery or non-energy delivery type of facility (e.g. substation, maintenance headquarters, and control centers).

From Transmission and Facilities respective criteria and criticality modeling, OSCO develops criteria, outlined below, which will best serve the capital investment. Detailed processes are restricted on need-to-basis but can be discussed and explained on a case-by-case basis.

Risk Management

OSCO implements the US DOE Design Basis Threat and the Interagency Security Committee – Risk Management Process (ISC-RMP) security assessment principles to identify and document risk, vulnerabilities, and threats associated with BPA personnel, facilities and critical assets. This includes the protection of BES Cyber Systems. Pertinent information will be provided to management to support a risk-informed decision for the implementation of protection strategy recommendations. OSCO implements the use of a variety of tools and methodologies related to vulnerability, threat and risk assessment.

Risk Assessments

OSCO conducts risk assessments and associated vulnerability assessments in accordance with various regulatory requirements and timelines. Examples include the *NERC CIP 014-2, Physical Security* standard and *DOE Order 470.3c Design Basis Threat*. OSCO's Physical Security team also completes an annual threat assessment, which helps feed the risk assessment process. The risk and vulnerability assessments conducted by OSCO help to inform the strategy for security projects which add new security assets for the protection of BPA's facilities, personnel, and assets.

Risk assessments are explained in more detail in Section 9 of this SAMP. These assessments evaluate whether there is a lack of security protections based on the criticality of the BPA asset evaluated and assess the condition and performance of existing security assets in place to protect the BPA asset.

8.0 CURRENT STATE

8.1 Historical Costs

OSCO's Capital Security Enhancement Program funds:

- Immediate Threat Mitigation capabilities to provide BPA the ability to respond immediately to newly discovered security gaps or threats requiring capital investments.
- NERC CIP 006 & 014 required protections at recommended levels for critical infrastructure protection to meet NERC CIP, US DOE Design Basis Threat, and best BPA security practices.

This program ensures timely funding allocations for the required security enhancements with minimal risk exposure especially as it relates to:

- Increased BPA and Contracted design/build efforts, labor and material costs
- Ongoing high maintenance and repair costs for systems that are not aligned to our current protection strategy,
- Risks posed by criminal activity and intrusion into the energized yards,
- BPA's site location and possible regional criticisms from local utilities and state government regarding the protection of the critical facilities, which are vital to the service area's critical infrastructure and economy.

The funding for the FY18 OSCO Capital Security Enhancement Program had a shortfall of \$1.2M, which negatively affected full contract execution in FY18. This shortfall was the result of pre-established CIR16 budgets that reduced the overall OSCO budget from \$8 million to \$6 million for FY18. The FY18 Agency Decision Framework (ADF) approval and budgetary increase corrected OSCO's capital portfolio covering all expenditures associated with the planned capital projects.

The funding for the FY20 OSCO Capital Security Enhancement Program had a shortfall of \$700,000, which negatively affected full contract execution in FY20. This shortfall was the result of an increased FY20 project workload associated with the scope, design, and construction costs and overall inflation rates higher than business case allocation. The FY20 Agency Decision Framework (ADF) approval and budgetary increase corrected OSCO’s capital portfolio covering all expenditures associated to the increased project workload; increased construction costs due to the breadth of Bell Substation/MHQ security enhancements; BPA safety watcher and contract inspectors; increase and long lead-time of fence line/security materials; and increased BPA design/construction standards and requirements.

Due to the FY20 COVID crisis and BPA’s work stoppage, the OSCO Capital Security Enhancement Program scope/design/build projects were moved to the right of the overall fiscal year calendar. As a result, the FY21 budget variance is positively affecting the full financial health of the OSCO capital program. This kept BPA Labor and Contract Labor stresses to a minimum, and helped keep full NERCCIP and BPA security compliances and best practices adhered to, and resulted in OSCO’s FY21 capital portfolio being underspent.

Table 8.1-1 Historical Spend

NERC CIP 006 & 014 Security Enhancement Program	Historical Spend (in thousands) With Current Rate Case					
	2017	2018	2019	2020	2021	2022
Capital Sustain						
CIR/IPR Allocation	\$8,000	\$6,000	\$8,000	\$7,000	\$7,000	\$8,000
ADF Budget Increase		\$1,200		\$700		
Adjusted Allocated Total	\$8,000	\$7,200	\$8,000	\$7,700	\$7,000	\$8,000
Total Spend Budget (Actual) (* Estimated)	\$7,805	\$6,727	\$8,081	\$7,088	\$2,039	\$7,300*
O&M Expense						
O&M SOY	\$748	\$600	\$600	\$650	\$650	\$580
O&M OY	\$542	\$600	\$635	\$650	\$650	\$580
Total Spend (Actuals) (* Estimated)	\$516	\$592	\$635	\$624	\$640	*687

In accordance with DOE Order 473.3, the objective of OSCO’s Security Performance Assurance Program (SPAP) is to identify essential security system elements, conduct regular system performance tests and maintenance, with corrective O&M occurring commensurate with the level of criticality and location of the system. This program

also identifies if a “one-off” security system upgrade project is warranted due to a new or previously unknown security vulnerability identified within an SPAP inspection.

Current security system asset O&M maintenance activities are broken out into two major categories:

- Preventative Maintenance
- Break Fix Maintenance

Note, the amounts identified in the chart above do not reflect the increased workload as new sites transition from warranty-covered O&M to internally covered O&M efforts.

Preventive Maintenance

A schedule of annual preventive maintenance activities is developed and coordinated between OSCO’s Physical Security Team, the Software Development & Operations Team, and the security vendor. BPA is required to complete preventive maintenance once within a 24-month cycle at facilities that are deemed critical under the NERC CIP standards.

Break-Fix Maintenance

The repair, reconfiguration and replacement (Break/Fix) of faulty or broken security systems or devices is managed and changes documented using BPA Service Tracking, and CRMs (work flow and change management), Asset Suite, Sunflower, and through work orders and invoices.

“One-off” Upgrade

The SPAP program can identify if a “one-off” security upgrade or modification is warranted due to an unknown security vulnerability identified within an SPAP inspection. An upgrade may consist of an additional security device to cover one or more physical and electronic needs. This need would use expense stream funding; however, there is currently no mechanism in place to fund or execute these types of project needs. The maturity of the OSCO expense budget and the program/project processes to include a contractual establishment that will support the “one-off” upgrade must be championed and established.

Disposal (Decommissioning) of Equipment

Security systems, devices, and/or components that are found to be faulty or excess are transferred to BPA’s Investment Recovery Center (IRC) for disposal. The transfer of equipment is processed using the Software Development & Operations internal Asset Management Process. Devices that contain sensitive information (Intelligent Controllers and Video Hard Drives) are transferred to BPA’s Data Center Services to secure until the items are destroyed locally under contract.

Work Priority

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

Prioritizing simply based on relative criticality of the site (protection level) may not be the best approach under all circumstances because security risk is influenced by several other factors including threat information and security system or mitigating strategies. For example, while a PL 6 High or PL 7 Medium site may have a greater

consequence resulting from malevolent acts, a PL 7 Impact site that is experiencing a high level of criminal activity may be at a greater “Risk” of loss thereby warranting an earlier or greater investment in security infrastructure.

When prioritizing O&M (Time & Materials and Firm Fixed), several factors are considered:

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

Table 8.1-2 O&M Work Priority Table

Priority Level	Description
Priority 1 24 Hours	Will be used in a case-by-case basis. Repair work identified for this priority will have to do with life safety or have a high operational impact as determined by Physical Security, the COR and/or the ISO.
Priority 2 3 Days	Will be used whenever a system or device used for monitoring or logging is malfunctioning at a BPA documented NERC CIP facility. Non-NERC facilities with these device types will be considered a Priority 3
Priority 3 5 Business Days	Will be used when a critical device failure can be mitigated through the use of other devices or systems
Priority 4 2 Weeks	Will be used for non-critical system or device failures
Priority 5	Will be used by the Software Development & Operations Team for projects, directed work, administrative tasks, or operational needs associated with asset management
Priority 6	Preventative Maintenance (Routine) Bi-Annual Requirement
Priority 7	Deferred Work (this work is non-critical and deferred due to project size, scope of work, cost savings, or fund limitations) <ul style="list-style-type: none"> • P7.1 – Deferred awaiting next site visit by vendor • P7.2 – Deferred awaiting a technical evaluation, proposal and funding decision (small project) • P7.3 – Deferred, this work falls outside the scope of break-fix maintenance (“one-off upgrades/additions)

Spending Priorities

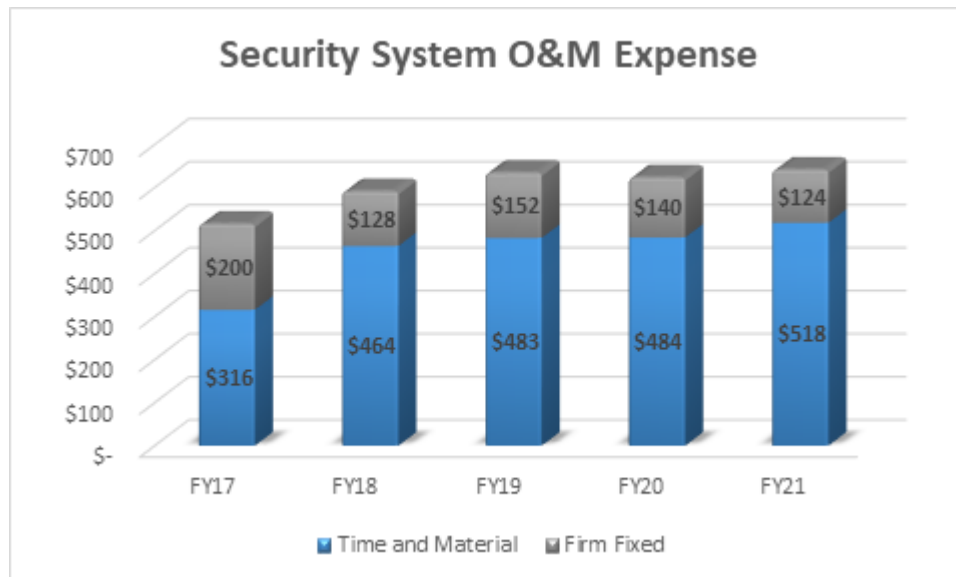
OSCO and Software Development & Operations continually collaborate to balance planned improvements within the respective OSCO capital portfolio as well as provide SME knowledge to the Transmission and Facilities capital portfolios in regards to scope/design/build of security systems. Regarding capital work, the OSCO security enhancement program executes on average two projects in scoping, two projects in design, and two projects in build every year. Accordingly, annual historical data at the program and project levels will provide a snapshot of several major projects under development.

Security best practices and compliance are weighed against the relative return on investment as capital build/replacement and major expense upgrades with more tactical/urgent O&M actions are planned and in return, required to maintain site security operability.

For security system O&M, there continues to be increasing challenges with balancing planned, long term maintenance activities with more immediate break-fix actions under the current limited annual allocation of expense funds. As security systems continue to age, urgent O&M (Time & Materials, Firm Fixed) makes up the majority of the OSCO security expense program leaving little opportunity for expense upgrades, resulting in the need for BPA to establish a more robust sustainment expense program.

In reference to figure 8.1-2, O&M trends are showing that break fix costs are increasing as the firm fixed costs have been decreasing. Increases in break fix costs are due to the aging of the systems and the infrastructure that supports these systems. In the last year we have been seeing an increase in failures associated with the infrastructure, specifically fiber runs in energized facilities. These costs have been increasing over time and is becoming very difficult to absorb under current maintenance dollars. The decrease in the firm fix costs are due to efficiencies that have been put in place over the years. However, Firm Fix costs will increase over time as the number of sites and the number of devices at sites continues to increase.

Figure 8.1-2 Historical Expenditures



8.2 Asset Condition and Trends

Section 10.5 below reflect Asset Conditions and Trends of security system assets as it pertains to the lifecycle management including O&M. As security industry trends indicate, electronic security systems average lifespan is five years.

NERC CIP 006 Portfolio:

The age of OSCO's NERC CIP 006 portfolio is approximately 12 years old and in need of increased funding resources towards maintenance and replacement. OSCO's maintenance budget of approximately \$500,000 - 650,000 per year supports device repair or replacement upon failure and bi-annual preventive maintenance visits. However, OSCO expects to see an increase in these costs due to the following: 1) aging security devices/components 2) increased need to require added "one-off" security devices 3) increase in the number of facilities requiring protection and 4) an increase in the complexity and size of these systems because of evolving security requirements.

Currently, OSCO's O&M budget adequately covers Break Fix and Preventive Maintenance costs. Moving forward, however, projected expense budget forecast indicate overall increasing infrastructure needs and rising national inflation will commensurately increase pressure on OSCO's capital and O&M budgets. OSCO anticipates that the overall health of BPA's security systems will continue to deteriorate for the next two to five years, requiring a significant investment in O&M capital and expense funding.

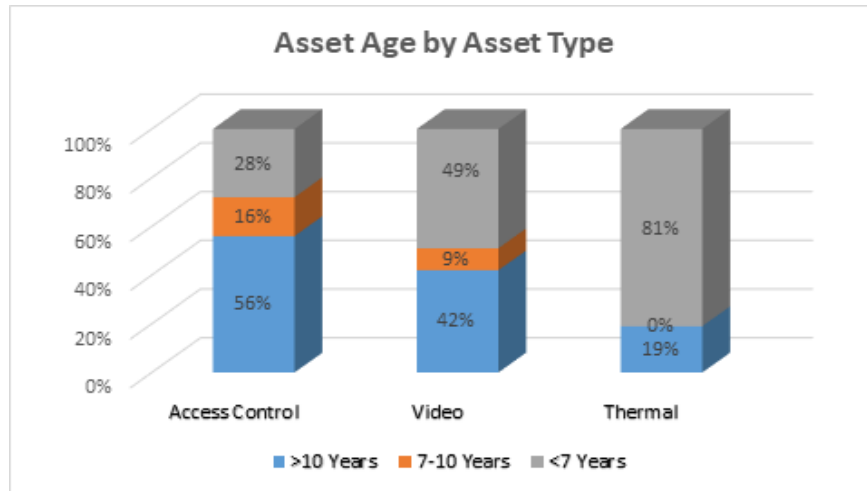
NERC CIP 014 Portfolio:

The age of OSCO's NERC CIP 014 portfolio is six years old. Not enough data to create a long-term, trend analysis has been collected in regards to the security system asset condition. However, given the average lifespan of a security system is approximately 5 years (as indicated by security industry data), the electronics and IT systems for the oldest CIP 014 sites may experience degradation in effectiveness and efficiency in the near term.

The data in figure 8.2-1 represents the age of electronic security devices broken down by asset type. The data suggests that access control devices are quite reliable but life expectancy of video devices such as cameras are negatively impacted by extreme environmental conditions in parts of BPA's service territory. It is hard to tell if this trend will continue as many of these devices are at end of life and replaced upon failure so we should expect to see the overall age of these devices decrease over time. Note that the bar representing thermal devices on the graph in figure 8.2-1 shows that we do not have any thermal devices in the 7-10 years age range.

These devices were first introduced at Raver and Custer substations in 2016 as a proof of concept, and were later incorporated as part of the design criteria for CIP 014 security installations in approximately 2017. These devices have been reliable and require little preventive maintenance, which reduces firm fixed costs. Note that these savings are offset somewhat as these are more expensive when compared to costs to repair or replace other security devices on the system. Another impact due to age that is not shown in the below graph is the aging infrastructure used to support security systems in energized yards, specifically fiber. These types of repairs can be extremely costly as compared with other break fix type work and we are seeing these type of repairs having a greater impact on the O&M budget over time.

Figure 8.2-1, Current Asset Age by Asset Type



8.3 Asset Performance

Security system asset health performance information does exist for some assets but the level of detail varies by asset type. The electronic security system has the most granular level of performance data and is tracked by Software Development & Operations organization. However, other security system asset information, such as for perimeter security fencing and gates, exists within Transmission and Facilities but is not reliable, given that these organizations have not historically tracked this type of data for an asset that does not change for decades.

OSCO and its partners are working towards best practices for the management of security system asset information. By improving security asset information governance, stewardship, and system architecture, along with the initial operating capability for Criticality Health, and Risk, BPA will be able to make better-informed decisions for asset management.

The following questions and answers describe OSCO’s asset performance relative to expectations:

- What has performance been in relation to expectations? Performance of an electronic security system in relation to expectations is relative to the age of the system, usage, and the environment for which it serves in. Almost the full complement of the BPA’s security systems are beyond their life expectancy. However, systems and components are performing generally as expected, given weather conditions, electrical/magnetic frequency interferences, etc.
 - Energy Delivery sites (substations) are impacted induced with extreme weather conditions, electrical magnetic/frequency interferences, BUD Network and bandwidth reliability variances
 - Non-energy Delivery sites (MHQs, HQ, Ross Complex, Control Centers) may have extreme weather conditions, minimal to no electrical magnetic/frequency interferences, more reliable and applicable BUD Network and bandwidth applications
- What have been the most significant or important asset performance challenges?

- Geographic location of a site and the associated weather/atmospheric impacts
- BPA capital expansion far exceeding the O&M expense funding needs to support the expansion
- BUD network/bandwidth “pipelines” not supporting the transport of security information
- Changing PHYSEC requirements dependent upon the facility’s criticality
- Changing and evolving security system/device hardware and software technology

Given the large geographic footprint and distributed responsibility of managing BPA’s overall security system assets, there are some challenges instituting consistent performance metrics. These challenges do not prohibit formation of performance metrics but they will influence the scope and implementation:

- Resources: In order to develop and maintain security standards and effectively monitor the performance of security system assets, cross-functional expertise and cross-organizational resources need to be committed to the continual review of the full security portfolio. While the existing staff is equipped to track asset performance, there are no additional financial increases to perform the work needed to integrate complete O&M standards.
- Location: Security system asset performance needs to be evaluated relative to the conditions under which the systems operate. The climate and operational requirements (ex. IT BUD Network Bandwidth) play an important part in determining the useful life of the asset. For example, certain system components of the same specification will have different lifespans based on where they are installed, indoor vs outdoor. This is true for a wide range of building systems.
- Access to Data: Access to security system information (knowledge management within ProjectWise, Procore, and RAM-T drive) is stable and more prevalent in respect to which security system is being inquired about. This includes security system software and hardware; prints/drawings development, storage, and access; published standards and requirements and their updating capability.
- Consistency: Capital security system asset (ex. perimeter fence, electronic security) standards for funding/scope/design/build efforts must be applied consistently by all stakeholders, and must not be deviated from without proper justification and approval.
 - Security system O&M is a distributed responsibility between OSCO and Software & Development Operations and a uniform method for evaluating performance metrics has been agreed upon and adopted. OSCO continues to assess the security system O&M program as part of BPA’s best security practices and Federal government security compliance requirements.

OSCO and Software Development & Operations do not have data supporting a Historical Asset Performance Summary in a format that is in line with strategic goal #2: *Modernize Assets*. These organizations have implemented metrics associated with the performance of electronic security systems starting in FY22 that now include: relative asset health, asset reliability per sub-set of the overall asset (e.g. PACS, VASS), asset turnover ratio, and percentage of asset life remaining as key measures for understanding asset performance from an individual asset to a system of networked assets.

Historical Asset Performance Summary, Table 8.3-1. This data is not currently available and will be updated during the next schedule SAMP update.

Table 8.3-1 Historical Asset Performance Summary

Strategic Goal	Objective	Measure	Assets	2017	2018	2019	2020	2021
Modernize assets	Reliability: Security Compliance and Best Practices	NA	#	NA	NA	NA	NA	NA

Note that assets not currently in Sunflower do not have a health score, precluding OSCO and Software Development & Operations to calculate a reliability coefficient. Some security system components (ex. Intrusion Detection Systems- IDS, which are just a small part of a full security system) are not currently managed “assets” due to the vast number and low cost of such components. Electronic security system asset health maturity is still evolving and OSCO and Software Development & Operations are working to connect the observed/measured field data to gain higher confidence levels in understanding full asset health. Today there are limited security system assets (ex. Video Assessment Systems) that have a level of robust trending data that would allow us to quantify health/probability of failure.

OSCO and Software Development & Operations both maintain updated financial and project portfolios. These organizations also track security incidents and/or system performance standards and report trends through formal meetings and dashboards distributed to personnel, to include BPA’s Finance organization and executive leadership. OSCO and Software Development & Operations currently track security incidents and outage metrics that can be found in such reports.

8.4 Performance and Practices Benchmarking

In accordance with NERC CIP 006 & 014 program compliance requirements, system performance and trending must be “benchmarked” and “audited” by same industry 3rd party associates such as Western Electricity Coordinating Council (WECC) or Western Area Power Administration (WAPA). The intent is to assess the effectiveness of BPA’s security program against that of a large electric utility. Software Development & Operations benchmarks and is benchmarked by organizations that scope/design/build/O&M IT software and hardware aspects of an electronic security systems down to the component level.

BPA’s OSCO currently participates in the Physical Security Working Group, an organization that includes physical security SMEs from peer electrical or other public utilities located from the Rocky Mountains USA, SW USA, the West Coast, and Pacific Northwest to engage and discusses all aspects (to include benchmarking) of security programs and projects, expenses, processes, and compliance standards for securing energized an non-electrical assets and facilities.

Security system (physical type such as fences/gates; electronic/IT type such as PACS, IDS, VASS) standards, requirements, and specifications are researched and accepted by BPA’s various engineering and IT organizations before implementation and energization. BPA documents adhere to and reference US DOE, USACE, US DoD, NERC, ASTM, IEEE codes, and all US architecture and building industry codes.

Industry peer data for security systems is in its infancy but growing rapidly with the need to protect utility assets Safety, Security, Grid Reliability, and Consumer and Industry Confidence. Participating in a more in-depth benchmarking study with other peer utilities could yield identification of new performance metrics, investigation and comparison into work volume, drivers of work – emerging and innovative practices and provide comparative data with peer utilities that OSCO and its stakeholders do not have at this time.

9.0 RISK ASSESSMENT

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 threats like general criminal activity and vandalism. In addition, certain types of security systems will be more effective for reducing risk from specific threats, while having practically no impact on others.

A security system asset, within a facility or designated area serves as a deterrent to current and future nefarious activity and must provide the capabilities of detecting, delaying, assessment, communication and response. Security system assets provide:

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

Security system asset risk management involves anticipating and avoiding events that have the potential to adversely affect OSCO program goals and strategic objectives. BPA’s five categories of risk are identified and are evaluated (through business cases, Agency Decision Frameworks, or Change Requests) in the OSCO security capital and O&M programs and projects that have been modified for OSCO’s SAMP. Risk mitigation strategies are identified in Table 9.0-3.

OSCO provides an enabling function to internal customers, allowing them to execute their missions. The consequences of the failure of security assets or services are directly related to the functions that OSCO enables. In other words, the consequence of a fence failing to secure a parking lot would be much less than a fence failing to secure a control center; therefore, OSCO will derive the criticality of security assets from the criticality of the assets it secures.

OSCO risk heat maps will be developed for each risk category, and will heavily rely on the input from the asset categories that depend on security from OSCO (Facilities, Transmission, and IT). Development of the OSCO risk matrices is underway, and the next version of the SAMP will seek to report the risk heat maps for each risk category in more detail.

Electronic security systems are a sub-system of a building. OSCO refers to the risk matrices of Transmission and Facilities for their respective buildings/assets as defined by their SAMPs, and the IT SAMP for the same need. An electronic security system is dependent upon the overall IT and building health and reliability for its protection.

Physical security systems (fences and gates) will follow the same processes to derive criticality. Risk assessments in the Transmission and Facilities’ SAMP for fences and gate systems are owned and maintained by those organizations.

Table 9.0-1 Responsibilities of OSCO and Other Business Lines

<i>Asset Type</i>	<i>Capital</i>	<i>O&M</i>
<i>Fences and Gates</i>	<i>OSCO/Transmission/Facilities</i>	<i>Transmission/Facilities</i>
<i>Electronic Security Systems</i>	<i>OSCO/Transmission/Facilities</i>	<i>OSCO*</i>

**JLS executes the O&M of ESS, but OSCO is the funding Organization*

Risks are defined in accordance with the current Agency risk assessment categories to quantify earthquakes, accidents, theft, vandalism, terrorism, compliance with life safety codes, OSHA requirements, and building codes.

Table 9.0-2 Risk Assessment, Reliability

Reliability Risk Map						
Probability	Almost Certain This event could occur within the next 2 years.					
	Likely This event could occur within the next 5 years.			Gates and Fences, Electronic Security Systems		
	Possible This event could occur within the next 10 years.					
	Unlikely This event could occur within the next 50 years.					
	Rare This event could occur within the next 100 years.					
		Insignificant	Minor	Moderate	Major	Extreme
		Consequence				

Table 9.0-3 Risk Assessment, Financial

Financial Risk Map						
Probability	Almost Certain This event could occur within the next 2 years.		Gates and Fences, Electronic Security Systems			
	Likely This event could occur within the next 5 years.					
	Possible This event could occur within the next 13 years.					
	Unlikely This event could occur within the next 50 years.					
	Rare This event could occur within the next 100 years.					
		Insignificant	Minor	Moderate	Major	Extreme
		Consequence				

Table 9.0-4 Risk Assessment, Environmental

Environmental Risk Map						
Probability	Almost Certain This event could occur within the next 2 years.	Gates and Fences, Electronic Security Systems				
	Likely This event could occur within the next 5 years.					
	Possible This event could occur within the next 13 years.					
	Unlikely This event could occur within the next 50 years.					
	Rare This event could occur within the next 100 years.					
		Insignificant	Minor	Moderate	Major	Extreme
		Consequence				

Table 9.0-5 Risk Assessment, Compliance

Compliance Risk Map						
Probability	Almost Certain This event could occur within the next 2 years.		Gates and Fences, Electronic Security Systems			
	Likely This event could occur within the next 5 years.					
	Possible This event could occur within the next 10 years.					
	Unlikely This event could occur within the next 50 years.					
	Rare This event could occur within the next 100 years.					
		Insignificant	Minor	Moderate	Major	Extreme
		Consequence				

Table 9.0-5 Risk Assessment, Safety

Safety Risk Map						
Probability	Almost Certain This event could occur within the next 2 years.		Gates and Fences, Electronic Security Systems			
	Likely This event could occur within the next 5 years.					
	Possible This event could occur within the next 13 years.					
	Unlikely This event could occur within the next 50 years.					
	Rare This event could occur within the next 100 years.					
		Insignificant	Minor	Moderate	Major	Extreme
		Consequence				

10.0 STRATEGY AND FUTURE STATE

OSCO seeks to balance both Federal security compliance requirements and best security protection initiatives in order to provide BPA with the most risk appropriate security system assets while applying sound asset management principles and efficiency studies to manage costs and maximize the use of rate payer dollars. Effective implementation of the NERCCIP 006 and 014 planning efforts and its overall standards remain the focus of BPA’s approach and will set the direction for the next decade and beyond.

OSCO assumes future capital and expense funding will grow in-line with ever-increasing scope/design/build/O&M levels and has embarked on a number of initiatives to achieve incremental improvement in cost management and execution capabilities. The initiatives described in Section 6 will assist OSCO to continue to manage the condition and performance of the security system asset base and prevent further deterioration of security’s most important needs, compliance, and practices within its facilities. Under present funding levels, however, there are not sufficient resources to address all assets equally.

10.1 Future State Asset Performance

OSCO’s and Software Development & Operations’ future asset performance is dependent upon various factors some of which are outside OSCO’s control:

- Telecom/IT BUD Network and bandwidth capabilities across BPA’s regions
 - This should follow the Transmission and IT SAMP
- Future BPA capital facility expansion conducted by Transmission and Facilities
 - This should follow the Transmission and Facilities SAMP
- Current Transmission’s Bulk Electric System (BES) substation modeling
 - This should follow the NERC and Transmission BES processes
- Capital and expense (O&M) funding levels
- Technology changes to software and hardware associated electronic security systems and needs
 - This follows BPA’s IT protocols

Future Asset Performance Objectives, Table 10.1-1. Data on Future Asset Performance Objectives is not currently available. OSCO and Software Development & Operations are exploring ways to measure electronic security asset performance and will include this information in future SAMPs

Table 10.1-1 Future Asset Performance Objectives

Objective	This Year	Year +1	+2	+3	+4	+5	+6	+7	+8	+9	+10
Reliability: Security Compliance and Best Practices	NA	NA	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD

10.2 Strategy

10.2.1 Sustainment Strategy

OSCO and Software Development & Operations are focusing on growing awareness of the need for sustaining and growing capital and O&M funding to meet the growing number of facilities and the increasing age of our assets. O&M funding, historically, has not been a consideration, and has not been increased or a factor, when capital funding is requested for scoping/design/build of new facilities. This is a significant gap, and O&M funding for security system lifecycle management should be a part of any requests/reviews/approvals of new capital projects.

Long-term security system, asset strategies and plans for capital replacements and maintenance have been developed for the following types of facilities listed below. However, the positive caveat to all the types of facilities listed is the security system assets at these facilities are largely very similar, with some variations based on scale or complexity at each site.

- NERCCIP 006 energized sites
- NERCCIP 014 energized sites
- Control Centers
- Complexes (ex. Ross, Celilo)
- Radio Communication sites
- Administrative Buildings (ex. HQ, Van Mall, MHQs)

In 2015, OSCO began a 15-20 year program focused on CIP 014 security enhancements. This capital program maintains two projects in scoping, two projects in design, and two projects in build every fiscal year, year over year. Beginning in FY22, OSCO will add two additional sites per year to this program, focused on CIP 006, resulting in four projects in scope, four projects in design, and four projects in build every fiscal year. Success of this program is dependent upon CIR/IPR increased financial support, alignment with Transmission and Facilities capital programs, and the availability of BPA and contracted SME design/build support.

Security system sustainment planning is driven by the larger asset planning of the Transmission and Facilities organizations, and takes into account the overall complexity of an energized or non-electric facility as it pertains to the direct bulk electric system, the support of the personnel building/maintaining the bulk electric system and the demands placed on each of them.

OSCO's capital program strategy focuses on asset health and risk of failure to the security system, along with a strategy for mitigating any associated risks. As security system asset management matures and criticality/health/risk, financial needs (capital and O&M), and decision maturity increases, the various BPA capital programs' methodologies for assessing their overall asset health and risk will follow the same decision-architecture so that assets and programs can be discussed comparatively through a systematic approach using industry best practices.

Operations & Maintenance Strategy

OSCO and Software Development & Operations continues to align its replacement and maintenance work streams by utilizing processes and analytics to align CHR aspects, Federal compliance, and best security practice values at all levels of the organization. See Table 8.1-2 O&M Work Priority Table.

Expense funding constraints delay some O&M or "one-off" activities that would mitigate vulnerabilities and reduce risk, and realize significant value for the security program. Often, OSCO has to decide what work to postpone or cancel in order to address high priority, unexpected break-fix work, or to implement a "one off" unplanned project to mitigate an emerging threat. Sometimes this is a result of it being an unanticipated expenditure or the available budget has already been consumed and/or committed.

It is important to ensure financial mechanisms such as IPR align to business strategies that incorporate cost, performance, and risk for all active and planned security system assets. OSCO's strategy moving forward is to continue working on asset segmentation/criticality/survival analysis with the intent of creating bands of asset classes with different maintenance intervals, based on trending data for each asset type. Current state is limited to interval-based maintenance; with corrective actions initiated by internal standards and guides to drive a maintenance action.

10.2.2 Growth (Expand) Strategy

OSCO's capital security system program, itself, does not participate in Growth (Expand) Strategy. However, it supports Transmission and Facilities respective Growth (Expand) Strategy as outlined within their respective SAMPs. A security system is an asset consisting of a number of sub-system assets. However, a security system asset planned for a facility becomes a sub-system of that facility and is no different from a lighting system, fire suppression system, or plumbing system. Security systems are required components for any growth (expand) strategy/asset, through Federal orders (NERC and US DOE), BPA policies, building industry codes/standards/requirements, and best security industry practices.

An expand project facing BPA's Transmission and Facilities' organization includes the acquisition of three energized yards and associated facilities at Grand Coulee Dam. This large project will need to incorporate physical and electronic security measures applicable to US DOE Design Basis Threat, NERCCIP 006 and 014, and BPA security standards. All though this project will be led by Transmission, OSCO will reflect capital IPR FY24/25 budgetary estimates specifically for the Grand Coulee Transmission program and project. OSCO will reflect associated expense forecasting needed to incorporate Grand Coulee security O&M needs beginning FY26. This is intended to provide transparency for estimated security costs for this large-scale project.

As per **Section 3.2 Scope** of the OSCO SAMP, OSCO's strategic goals of security and compliance will be achieved by meeting the following objectives:

- Transmission and Facilities upgrade projects and new construction projects incorporate Agency, DOE, and national level standards.
- Upgrade projects and new construction by Transmission and Facilities incorporate required security measures and related costs into individual projects. All resulting security systems included in future asset lifecycle management planning as well as a sustainable maintenance program.

Transmission and Facilities shall follow all established BPA policies and standards associated with the execution of the Physical Security Policy STD-D-000032 - Section 4.1 Regulatory Requirements.

Adherence to this strategy is the overall responsibility of the OSCO organization, but responsibility for compliance and execution of strategic goals is shared with partner organizations performing overlapping asset life cycle functions. Examples include the acquiring of, retrofitting of, and/or construction of high voltage sites or maintenance headquarters or O&M of current security assets.

This SAMP affects any organization that utilizes physical and electronic security system assets. This is the responsibility to fund capital expenditures for the scope/design/build of such security assets and the documentation and responsibility to ensure funding of expense (O&M) flows to OSCO and Software Development & Operation for reliable maintenance and care of electronic security systems.

10.2.3 Strategy for Managing Technological Change and Resiliency

Technological Obsolescence

OSCO, Software Development & Operations, Transmission, and Facilities are faced with the challenge of changing Federal requirements, evolving best security practices, and ever changing security system technology and engineering in several different disciplines: IT security software, electronic security system hardware, and advanced professional engineering standards.

Maintaining security system and equipment operability with multiple older vintages of equipment increases the necessary inventory of spare parts and creates additional instances of equipment and system failures. In turn, the future costs of O&M is expected to increase substantially as, while some equipment may still be in fair or good condition, the lack of vendor support and replacement parts makes repairs expensive and increases the potential for outages of unacceptable duration.

Many new technologies exist that can provide security systems assets with flexibility to perform O&M or replacement activities without requiring possible security system outages that must be planned throughout

the regions of BPA. OSCO and Software Development & Operations are continuously researching new design concepts to identify and implement new security technologies that would reduce the number and the duration time of planned outages for maintenance, repair and replacement. In addition, these new design concepts reduce human performance errors for system users.

Resiliency Resiliency is defined by NERC/FERC (Docket AD18-7-000) as “infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.” This puts a time based function on reliability where maintaining existing security systems assets’ performance levels has been the traditional thought, that a designed level of response time to a security event is adding resiliency to the security system and the Federal orders, policies, standards it serves. This would be intended to be a designed program that grows as it matures and definitions are codified by NERC, US DOE, and BPA regulatory orders, standards with guidance on reasonable levels of reliability/resiliency.

Resiliency in regards to security fence/gate systems, security poles, and associated infrastructure are solely dedicated to the area it is designed to protect. Any expansions to those areas is covered under the Transmission and Facilities’ SAMPs as well as the funding/scope/design/build of the security perimeter needs. Capital and/or O&M program management responsibility associated with fences and gates consist of:

- OSCO - Energy delivery sites’ perimeter fencing capital upgrade (NERC CIP 014 sites)
- Transmission – Energy delivery sites’ perimeter fencing/gates new build, lifecycle replacement, maintenance (requires bonding/grounding)
- Transmission - Energy delivery sites’ interior fencing/gates new build, lifecycle replacement, maintenance (requires bonding/grounding)
- Facilities - Non-energy delivery facility/site fencing new build, lifecycle replacement, maintenance lifecycle replacement (no bonding/grounding)

Resiliency in regards to electronic security systems (ESS) consist of four sub-systems:

- Intrusion Detection (ex. motion sensors)
- Physical Access Control (ex. card readers)
- Video Assessment and Surveillance (ex. cameras)
- Security Software

The NERCCIP 006 electronic security systems (ESS) started being integrated into BPA sites as early as 2009, and with seven year life span, a large numbers of security systems (either sub-system or as a whole) are projected to fail completely in due to exceeding manufacturer recommended Mean Time to Failure (MTTF). This will negatively affect NERCCIP and US DOE DBT compliance, security system effectiveness if replacement or repairs cannot be affected in a timely manner. It will also cause a tremendous increase in maintenance fees and drain limited BPA and contracted resources.

To manage this, OSCO is launching the NERC CIP 006 “Refresh/Upgrade” capital program beginning in FY22. This program will work to remove obsolete and failing security systems and replace them (through scope/design efforts) with improved technology across the whole security spectrum. The NERCCIP 006 capital program will be an on-going/rolling program to ensure compliances and best security practices are kept up-to-date and in-line with current security hardware and software needs.

OSCO has a very young NERCCIP 014 capital program (six years old) however, (as the NERCCIP 006) the NERC CIP 014 technology must be properly maintained through planned O&M activities to maximize its MTTF as well as evolve into a NERCCIP 014 “Refresh/Upgrade” program. As the NERCCIP 006 and 014 programs mature, a nexus and trend will occur at sites that have both programs integrated into an O&M and “Refresh/Upgrade” cycle.

Resiliency of ESS for both OSCO capital programs (CIP 014 and CIP 006) (along with IT, Transmission, and Facilities SAMPS/capital programs) are dependent upon an overarching need to maintain the ever-growing security systems is through a healthy, evolving, and sustainable expense budget.

Resiliency to across the full security system spectrum (perimeter fence/gates, security poles, civil/structural/electrical/Telecom, ESS) also plays into supports a healthy and funded research and development (R&D) program/projects. The expenses stream needed is to must be funded by the organization requesting the research.

The R&D team includes security system technical experts that continue to look for innovative and cost saving solutions in meeting BPA’s ever changing and growing security compliance and best practices obligations. This program would provide the capability to research new security technologies in order to drive future system costs down, provide solutions more closely tailored to the needs of BPA, and to ensure electronic security systems running on BPA’s network meet regulatory requirements. Funding for this program is not currently covered by OSCO’s annual maintenance budget.

An example of an R&D project is to develop a new security system design focusing on meeting the following criteria:

- Increase system reliability: Keep it simple by limiting the number of system devices; reduces number of device failures; reduces programming time; reduces installation cost and time.
- Lessen the impact on users: New design does not require local arming/disarming of the system, the system is always on; eliminates the occurrence of violations for not arming a site. The result is a significant decrease in human performance errors.
- Meet NERC CIP requirements: This was accomplished by adding a new device that monitors access points.

The new security design was installed at the Santiam Substation as a security system refresh proof of concept and was completed in March 2018. Data was pulled for March 2017 prior to the system upgrade and data was pulled for March 2018 after the installation was completed. Software Development & Operations specifically researched if there was a reduction in alarms and a reduction in device relay usage. The data shows a 100% reduction in site alarms and a 78% reduction in relay usage. The reduction in relay usage equates to a reduction in device failure and longer life expectancy.

As per this R&D effort and continued success, all BPA energy and non-energy delivery facilities are scope/design/build to this new electronic security system.

10.3 Planned Future Investments/Spend Levels

Table 10.3-1 is a summary of OSCO’s expressed capital budgets currently allocated, as well as Software Development & Operations’ forecasted expense needs within the NERCCIP 006 & 014 security asset

management program. The costs listed in table 10.3-1 are estimates that will be finalized during IPR, and updated in the next iteration of the SAMP.

O&M security system expense costs have not been developed and finalized prior to the completion of this SAMP. Tentatively, expense costs are expected to increase, but the amount of increase is unknown as it relates to inflation.

Table 10.3-1 Future Expenditures (in thousands)

Program	Rate Case FYs		Future Fiscal Years									
	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033
Capital Sustain												
CIR/IPR Allocation (* Forecasted)	\$8,000	\$8,200	*\$14,000	*\$15,000	*\$15,375	*\$15,760	*\$16,153	*\$16,556	*\$17,000	*\$17,425	*\$17,860	*\$18,307
GCOU Security Enhancements (** Forecasted)			**\$4,300 (NERC CIP 006, Enclosure Fencing)	**\$6,000 (NERC CIP 014)								
O&M Expense												
Corporate Expense Budget (***) Forecasted)	\$580 ***\$750	\$675 ***\$800	\$691 ***\$850	\$708 ***\$1,000	\$1,030 ***\$1,030	\$1,055 ***\$1,055	\$1,081 ***\$1,081	\$1,108 ***\$1,108	\$1,136 ***\$1,136	\$1,165 ***\$1,165	\$1,195 ***\$1,195	\$1,225 ***\$1,225
Expense Costs Associated with Grand Coulee Security Operations (****Forecasted)			\$1,086	\$1,140	\$1,197	\$1,256	\$1,318	\$1,383	\$1,452	\$1,524	\$1,600	\$1,680

* As per BPA Finance direction – OSCO, in FY21, completed FY22 capital forecasting for FY22 CIR/IPR allocation along with a general forecast of out-year capital funding needs, this is depicted in Table 10.3-1. However, as FY22 has commenced BPA has seen a dramatic increase of contractor material and labor inflation via capital bid processing for scope/design/build efforts. OSCO’s capital needs for future fiscal years has dramatically changed due to national and regional inflation of labor and materials to near two times the afore-mentioned forecasted outlook. For OSCO (along with Transmission and Facilities) to maintain positive health for best security practices and its respective capital security program; new estimates, based on the increase inflation rates, must be developed and analyzed for CIR/IPR purposes. **Initial trends reveal the need of an approximate and immediate increase of capital funding allocations to total \$14M to \$17M per fiscal year.**

** As per direction from the Grand Coulee Acquisition Project Team (with Transmisison) - This is intended to provide transparency for estimated capital security costs for the acquisition, scope, design, and build of the security enhancements needed for the Grand Coulee project.

- NERCCIP 006 - Electronic Security System Install 115kV Switchyard (Control House)
- NERCCIP 006 - Electronic Security System Install 230kV Switchyard (1 Control House, 1 Relay House, 1 Admin/Shop, 1 Motorized Gate)
- NERCCIP 006 - Electronic Security System Install 500kV Switchyard (1 Control House/Admin-Shop, 1 Motorized Gate)
- NERCCIP 014 - Medium Perimeter Security Fence and Video Assessment & Surveillance System (500kV Switchyard)
- New Switchyard Enclosure Fencing (115kV, 230kV, 500kV); to segregate high voltage yard from parking areas

*** Due to the way that O&M for security projects are funded, expense budgets are not known in the current Rate Case year or out-years. Increase for new contract rate increases, parts inflation, and increased support of new/upgraded systems coming off warranty. Along the same trajectory of increased capital funding due to inflation the O&M funding will need to be addressed and increased as stated. **If the inflation trends continue, the approximate increase of expense security funding requested will be near or above \$1M per fiscal year beginning FY25.** The forecasted expense numbers would absorb the annual expense costs needed to conduct maintenance as well as address break/fix needs associated with Grand Coulee electronic security systems.

OSCO develops business cases to annotate the out-year O&M needs for a project at the particular site of design/build. Yet, it is unknown how those projected O&M costs filter down from Financial management to the Corporate management to initiate the expense funding needed for the security O&M needs.

Transmission and Facilities capital projects, through their respective SAMPS and business cases, filters security system O&M expense streams to the Corporate levels so that OSCO and Software Development & Operations can act upon repairs, outages, or “one-off” needs.

In either case noted above, OSCO does not receive (from any of the three program streams of Transmission, Facilities, or OSCO) the O&M funding projected to maintain the new security assets being delivered to BPA.

OSCO and Software Development & Operations future asset expenditures will be dependent upon various factors:

- Steady-state/increase of capital and expense (O&M) funding
 - This is determined by the amount of capital projects approved within the Transmission and Facilities SAMPS and the current amount of OSCO’s capital program for NERC CIP 006 and 014 security enhancements
- Telecom/IT BUD Network and bandwidth capabilities across BPA’s regions
 - This should follow the Transmission and IT SAMP
- Future BPA capital facility expansion conducted by Transmission and Facilities
 - This should follow the Transmission and Facilities SAMP
- Current Transmission’s Bulk Electric System (BES) substation modeling
 - This should follow the NERC and Transmission BES processes
- Technology changes to software and hardware associated electronic security systems and needs
 - This follows BPA’s IT protocols

**** This outlines the annual, estimated expense costs that BPA will need to pay for Bureau of Reclamation (BOR) for continuing security operations for the Grand Coulee facilities. BPA expects BOR to continue with site security monitoring, patrols, and response under a memorandum of agreement as BPA takes possession of these facilities. Currently, BPA subsidizes BOR approximately \$9M annually for associated Grand Coulee management. It is anticipated that this subsidy would continue, but possibly be reduced, as BPA takes ownership and control of Grand Coulee transmission assets. However, security funding for operational support will be a long-term effort as security patrol and response will continue to be necessary from BOR’s response force.

10.4 Implementation Risks

More information on Risk and Risk Assessment as it pertains to the security system asset can be reviewed in Section 9 Risk Assessment. Security system assets and what they provide are the responsibility of BPA as a whole, this pertains to its policies and standards that lead to funding/scope/design/build/O&M and all risks associated with the implementation of new BPA capital facilities into include OSCO’s capital program strategy. These are outlined through the implementation risk categories defined below.

Table 10.4-1, Implementation Risks

Risk	Impact	Mitigation Plan
BPA cultural resistance to security paradigm shift	“Pocket veto” can delay or halt security maturity growth	Top down support and communication plan that demonstrates “what’s in it for me” and executive commitment to enforce change to deliver better value to Security as Safety is to BPA
Constrained execution of resources	Delayed and/or deferred projects degrade security reliability, effectiveness, and compliance	Organizational changes and redeployment and in some cases re-training employees is a long term proposition, in addition to an increase in managed services contracts such as procure/design/build. Secondary capacity initiative and re-engineering work and processes is another alternative but the Agency would need to direct employees to accept more calculated risk in processes and methods
Premature redirection (aka chasing the next shiny object)	Redeployment of resources prior to reaching project or program maturity, steady state business implementation of improvement initiatives prevents realization of potential value and discourages employees	Executives and Managers must continually educate/communicate with the workforce to direct the level of effort and resources required, and stay the course to successful completion to realize dividends in years to come. Repeated demonstration of this level of commitment is required before BPA’s minor regard for security culture can change. Executive-led, enterprise wide communication strategy should include projected and realized efficiencies, repeated often with transparent expectations of staying the course
Delay in Performance Standards development	Challenges with consistent deliverables and slower execution during the design process	Develop standardize owner project requirements and performance specs for the most frequent types of work

Accurate Staffing Forecasting	Frequent changes to staffing forecast prevents a strategic and cost minded approach to managing IT and engineering disciplines	Develop flexible strategies with alternate scenario contingencies. Continue working with CAO and Transmission business line to maintain accurate staffing of technical positions
Adoption of alternative project delivery methods	Continued challenges to solicit competitive bids and limited ability to anticipate execution costs and schedule	Continued research in Primary and Secondary Capacity Model usage. Continual contract language evolution for solid procurement of scope/design/build services and phase

10.5 Asset Conditions and Trends

Due to the vast number of security systems across BPA and limited resources and funding it is anticipated the overall condition of the overall security system health will continue to deteriorate for the next two to five years until a significant investment in O&M expense funding is allocated.

Software Development & Operations’ limited trend analysis indicates Mean Time to Failure (MTTF) for its electronic security systems (either singularly or as a whole) are projected to fail in the coming years due to exceeding manufacturer recommended MTTF. Currently, JLS does not have complete estimates of MTTF for its electronic security systems. If not managed, this will negatively affect NERC CIP and US DOE DBT compliance, security system effectiveness, and cause a tremendous increase in maintenance fees and drain limited BPA and contracted resources.

OSCO, through its capital NERC CIP 006 and 014 program, will leverage new security system technology that can be sustained for longer durations. The benefits to this approach are:

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

As each project completes, lessons learned and key achievements establish new project delivery methods, consistent project requirements, quality assurance methods, and performance standards for use across all BPA capital projects and OSCO’s capital portfolio. These improvements allow for efficient resourcing and consistent estimating throughout the strategy window. Specific trends of this strategy include the following:

Time Frame	Objective	Trend	Primary Driver
1-2 years	Security system reliability	Significant deterioration	Aging/obsolete software and hardware technology
	Asset Condition	Significant deterioration	Failing electronics security systems
	Cost Management	Slow deterioration	Planning for increased security system footprint

3-5 years	Security system reliability	Slow/Moderate deterioration	Sustain system replacements
	Asset Condition	Slow/Moderate deterioration	New projects/facilities completing
	Cost Management	Steady State	Capital investment starting to peak
5-10 years	Security system reliability	50% Steady State, 50% moderate deterioration	Up-to-date technology
	Asset Condition	50% Steady State, 50% moderate deterioration	Established security system
	Cost Management	Significant improvement	Capital investment steady

Figure 10.5-1 Future Asset Age by Asset Type

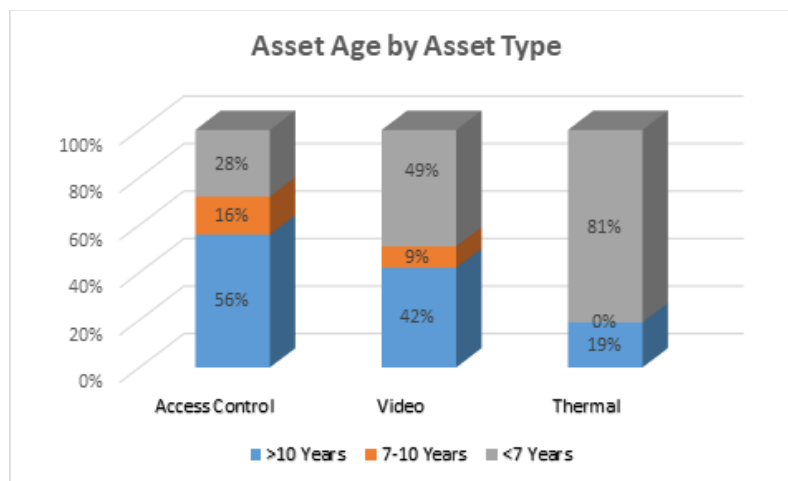


Figure 10.5-1 describes the age of security devices by asset type and does not take into consideration other infrastructure that may be used to support these systems. Examples would include the network and the fiber used to support our systems. The trends that we are seeing from a maintenance perspective is that the Access Control system is very reliable and this is the system that is used to maintain BPA’s NERC CIP compliance. A majority of the systems are original dating back to 2009.

The thermal camera systems are used to provide perimeter security. These are one of the most expensive devices in our inventory to repair or replace, however, they have a much better ability to withstand the harsh weather environments and we are not seeing the failure rates that we see in other cameras under similar conditions.

The two areas of greatest concern are the video systems and the fiber used to support these systems. The video system cameras are in very harsh environments and we are seeing an increase in mean time to failure as a result. We are seeing an increase in the degradation of these devices over time, however, due to budget constraints

many of these devices are still in service. The other area of concern is that we have seen an increase in fiber failures over the past two years (2020-2021). It is too early to see a pattern; however, these failures have a big impact on the maintenance budget and can cause extended outages. These outages have a major impact on the ability of security to effectively monitor impacted sites and adequately protect BPA personnel and assets.

Deferred capital projects of the NERC CIP 014 program would be a detriment to NERC CIP and US DOE compliance and best security practices to BPA's most critical BES high-voltage assets. Such deferred work would negatively disrupt the allocated capital budget set within the IPR cycle as a financial consideration as well as degrade security posture and not serve security needs due to increased criminal activity within the BPA service area.

Deferred ESS maintenance is not healthy for compliance and best security practices across the whole ESS spectrum based on criticality of BPA's influence to the national grid system. If maintenance is deferred to the right, then risk must be accepted and re-evaluated during a future site visit if the maintenance is deemed necessary.

- Deferred Work (this work is non-critical and deferred due to project size, scope of work, cost savings, or fund limitations)
 - Deferred awaiting next site visit by vendor
 - Deferred awaiting a technical evaluation, proposal and funding decision (small project)
 - Deferred, this work falls outside the scope of break-fix maintenance (major project or system additions)

10.6 Performance and Risk Impact

OSCO's approach to risk management has been established through Physical Security's risk and vulnerability assessments. However, as US DOE's Design Basis Threat matures so will the maturity of asset information that is able to be tracked and trended. Subsequently, Software Development & Operations' software and electronic security hardware risk and forecast management has been established and like OSCO, asset information will mature as trends ebb and flow with ever changing IT technology applications and requirements.

A deliberate risk mitigation strategy for asset criticality levels (such as NERC compliance) will minimize security system downtime impacts as it is very likely that asset conditions will markedly change as technology changes and unforeseen security system failures as age and usage occurs. Additionally, these assessments provide a framework for the prioritization of key actions in the proactive management of the security asset portfolio.

Table 10.6-0 Strategic Initiatives and Risks Addressed

Drivers	Initiatives	Risks of Foregoing Implementation
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Security Enhancements (DOE/NERC CIP 006 & 014)</p>	<p><i>NERC CIP 006 and 014 more closely links security and compliance resulting in a single total</i></p> <p>Compliance (NERC CIP 006 & 014): Ensure compliance with security regulation by applying mandatory security enhancements as required by NERC, DHS, DOE, and CASP etc.</p> <p>Critical Infrastructure Protection: Installation of security systems designed to provide the appropriate level of protection for critical infrastructure designated PL6 and PL7</p>	<p>Financial and Reputational Risk Due to Regulatory Non-Compliance: Findings by regulatory entities within one year leading to; a) possible cost incurred due to physical security audit findings, b) mandated policy changes and, c) public criticism.</p> <p>Financial and Operational Risk Due to Terrorist/Criminal Activity: Continual exposure to the “medium risk” of terrorist attack or collateral damage from criminal activity which could result in the loss of critical transmission facilities with:</p> <ul style="list-style-type: none"> • an extreme consequence to the bulk electric system • major economic impact to regional customers and economy and • severe observable impact and orders for substantial corrective action, including some mandatory changes in BPA operation or administration <p>This includes OSCO, Transmission, and Facilities capital projects currently scheduled</p>
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Immediate Threat Mitigation</p>	<p>Immediate Threat Mitigation: Provides agility to respond to emerging threat vectors or respond in a timely and expeditious manner to previously unknown security gaps at BPA facilities, with appropriate capital or expense investments.</p>	<p>Strategy: This strategy allows BPA to confront the unpredictable nature of threats and resulting security conditions. Not programming funds towards this end removes the flexibility to maneuver in an environment where security conditions can change with little advanced warning. This ensures adequate baseline level of security commensurate with criticality to include avoidance of financial, reputational, and/or operational risks to non-compliance, terrorist, or criminal activities.</p>
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Preventative O&M Program</p>	<p>Replacement & Renewal Program: Timely replacement of failed components commensurate with criticality of system to maintain compliance and provide security protection. Strategic phase-out of components that are no longer technologically viable.</p>	<p>Operational and Reputational Risk Due to Inadequate Maintenance: Failing or faulty security systems and equipment leading to:</p> <ul style="list-style-type: none"> • compromised protection of critical infrastructure • strain on limited resources to support O&M activity • criticism by Federal regulatory entities due to unplanned outages of critical security systems; or worse, damage to critical energy delivery infrastructure from a physical attack.

OSCO’s portfolio risks and the associated strategies for risk mitigation in the near, mid and long-term are as follows:

10.6.1 Safety Risk

The safety and security of our BPA workforce is a core value at the BPA. Given the number of aged security assets on BPA’s system, current OSCO strategy is focused on prioritizing maintenance, lifecycle replacement of NERCCIP 006 and 014 security assets, and initial installation of CIP 014 security protections. Sites that fall into this category are typically energized (substations), but non-energized (MHQ) field sites are also included in maintenance and lifecycle activities. Larger sites and complexes are assessed through DHSISC – RMP and US

DOE DBT assessments and Facilities’ Strategic Framework Guide to establish site-specific development strategies in collaboration with safety and security design principles.

These assessments and guides structure capital replacement programs to retire and replace electronic and physical security systems with updated systems/components that meet compliance and other standards. Through this path, OSCO will gradually reduce the number of systems that fall into the severe range of the risk heat map, however with the sheer number of deficient security systems, a focused effort of replacement through the expense program will be needed to improve asset conditions. When data, trends, or failure indicate a critical security building systems is in need of replacement, this information informs the prioritized investment strategy in the short term. With an average replacement rate of <5 NERC CIP 006 security systems a year and current work capacity, system replacements will not be completed in sufficient quantities in order to markedly improve conditions or match increasing numbers of premature failures. Longer-term tracking of system condition data is needed to assess and then reduce risk in this category with any level of certainty.

Table 10.6-1, Strategy, Risk Assessment Safety

Risk Category	Safety
Asset Risk	Non-compliance with security orders/policies/standards/requirements, OSHA requirements, life safety codes, and modern seismic design standards within facilities are a liability to BPA and present safety and security risks for staff and resiliency risks for operations and critical assets.
Owner/Control	Safety, Transmission, Facilities
Risk Mitigation	<p>Strategy:</p> <ul style="list-style-type: none"> • Immediate – Consistently execute capital NERC CIP 006 and 014 programs to design/build at new sites and replace aging security system assets at existing sites to ensure compliance • Immediate – Prioritize security system replacements at critical assets with available expense funding • 2 year – Refresh the security system asset registry to gain better trending information of system level improvements • 2-5 years – Extend or re-compete vendor contract to all BPA facilities that can replace systems versus using internal resources • 5-10 years – Realize improvement in the condition of security systems (reduction of 50% of security systems in severe risk of failure)

10.6.2 Reliability Risk

The reliability of security system assets will generally increase over time as older systems are fully replaced with the latest technology as well as new facilities being built with the same (updated) technology. However, if BPA’s overall Administrative Network is not upgraded for increased efficiency and effectiveness, all new technology will be degraded due to poor network bandwidth. As per O&M trends, if expense funding is not increased as security system assets are implemented in new or retro-fit design/build then reliability risk to all security systems will increase as expense funding to repair or maintain the assets will not keep pace with ever expanding security infrastructure. The benefits of properly funding and successfully executing O&M activities in support of security system assets include:

- Alignment with BPA’s strategic objective of modernizing assets which would increase system reliability due to a decrease in component/system failure risks
- Alignment with BPA’s strategic objective of strengthening our financial health by reducing break-fix costs over time
- Reduced risk of non-compliance with standards and requirements
- Reduces risk of component or system failure and unplanned outages,

Three main drivers in support of this strategy:

- Compliance – Electronic security system assets and lifecycle activities are mandated to be compliant with security, regulatory requirements, governance and agency policies specific to physical access control, intrusion detection, and video assessment of selected BPA facilities
- Security System Reliability – Well maintained systems provide consistent protection. When installed security systems are assessed and maintained on a regular basis one can mitigate the risk of unplanned security system outages or failures that could result in compromised protection
- Cost Management – Requested funding for system maintenance activities are economical and sustainable with risk informed forecasting and work prioritization to ensure reliable system performance

Table 10.6-2, Strategy, Risk Assessment Reliability

Risk Category	Reliability
Asset Risk	Personnel Security Insufficient expense funding NERC, US DOE, and HSPD-12 compliance Security system failures
Owner/Control	OSCO, Software Development & Operations
Risk Mitigation	<p>Strategy:</p> <ul style="list-style-type: none"> • Immediate: <ul style="list-style-type: none"> – Coordinate with Software Development & Operations to track the replacement of critically level assets (ex IC panels, NVRs) and review the impact to system conditions – Prioritize system replacements at critical assets with available expense funding • 2 years – refresh the asset registry to gain trending data • 2-5 years: <ul style="list-style-type: none"> – Replacement of complete security systems – Extend or re-compete vendor contract to all BPA facilities that can replace systems versus using internal resources • 5-10 years – Realize improvement in the condition of security systems (reduction of 50% of security systems in severe condition or severe failure risk)

10.6.3 Financial Risk

For the substation environments, costs for design and construction services and materials are increasing, and the labor market is very tight, resulting in capacity challenges for BPA and vendors in respects to the needs of BPA’s Transmission and Facilities capital forecasts. This is leading to higher design and construction prices on all new security system installation, “one-off” projects, and other full capital projects. This upwards price pressure creates a financial risk due to the limit it applies to the amount of work that can be performed within a fixed budget and, as time goes by, inflation compounds this problem.

OSCO’s security system O&M program can be funded properly through the new NERC CIP 006 refresh/upgrade program for energy delivery sites. By focusing BPA resources to better utilize available capital funding, this shifts focus from reactive break-fix and O&M replacements (expense) to full security system asset replacements (capital).

This would lead to the ability for the simultaneous execution of two major capital projects if program delivery may be improved through a consolidation of O&M service contract actions. Additionally, alternative project delivery methods, such as progressive design/build, may be used to transfer the execution resource burden from internal resources to contracted external vendors. Secondary benefits of a shift to alternative delivery methods would include improved certainty of project schedules and costs, which are needed to balance the spend levels at the limit of available program funding.

Table 10.6-3, Strategy, Risk Assessment Financial

Risk Category	Financial
Asset Risk	Inability to consistently track project expenditures over the project lifespan Market conditions driving costs higher than planned Capital and Expense funding held flat, not pacing construction inflation
Owner/Control	OSCO, Software Development & Operations, Transmission, Facilities
Risk Mitigation	<p>Strategy:</p> <ul style="list-style-type: none"> • Immediate: <ul style="list-style-type: none"> – Establish an execution plan with simultaneous capital replacement projects in design while another proceeding plan is under construction – Develop automated estimating tools that are security system related for owner project requirements and efforts • 2 years: <ul style="list-style-type: none"> – refresh the asset registry to gain trending data – Implement alternative project delivery methods (ex. IFM contract, Secondary Capacity Model) • 2-5 years – Extend or re-compete vendor contract to all BPA facilities that can replace systems versus using internal resources • 5-10 years – Realize improvement in the condition of security systems (reduction of 50% of security systems in severe condition or severe risk of failure)

10.6.4 Environment/Trustworthy/Stewardship Risk

Key activities that support Environment/Trustworthy Stewardship for OSCO security system projects include failure to properly complete and incorporate environmental reviews of perimeter fence locations, failure to conduct proper vegetation management, or failure to comply with pollution abatement processes. In these examples, the loss of trust and best security practices and stewardship due to such inaction could result in program shutdown and restructuring.

OSCO’s essential physical security mission is to properly protect and continue its strong stewardship of rate payer backing and assets funded by rate case financial endeavors. Stewardship of these critical assets means properly protecting them, ensuring they are available, safe, and reliable from a security perspective, and cannot be compromised by an adversary.

*Figure 10.6-4, Strategy, Risk Assessment
Environment/Trustworthy/Stewardship*

Risk Category	Environment/Trustworthy/Stewardship
Asset Risk	Inability to meet Agency environmental, vegetation, and pollution abatement schemes Failure to properly secure and protect energy delivery and non-energy delivery assets
Owner/Control	OSCO, Software Development & Operations, Transmission, Facilities
Risk Mitigation	Strategy: <ul style="list-style-type: none"> • Immediate and Forecasted Future – BPA’s design/build capital and O&M programs will create new security system needs and as such will require oversight for proper application

10.6.5 Compliance Risk

The risk of not complying with all applicable orders, policy, standards, requirements and specifications (as addressed within this SAMP) is both punitive through possible cost incurred due to physical security audits. Given the average age of BPA facilities and the number of deficient security systems, it is impractical to address all field sites compliance issues in a short period. Therefore, OSCO intends to correct all identified compliance concerns when completing planned NERC CIP 006 and 014 projects. Individual security systems not in compliance with regulations or codes will continue to be addressed through the O&M expense program on a prioritized basis that balances program goals. Audits of the existing facilities and sites to gain a better understanding of the current state of compliance will quantify this risk to the Agency through the update to the asset registry.

Table 10.6-5, Strategy Risk Assessment Compliance

Risk Category	Compliance
Asset Risk	<p>Cost incurred due to physical security audits due to noncompliance with regulations, guidelines, and standards</p> <p>Negative public perception of BPA due to noncompliance</p>
Owner/Control	OSCO, Software Development & Operations, Transmission, Facilities
Risk Mitigation	<p>Strategy:</p> <ul style="list-style-type: none"> • Immediate <ul style="list-style-type: none"> – On-going review and approval of all applicable orders, policy, standards, requirements and specifications as needed to support capital and O&M operations – Expand Capital acquisition program, Sustain Capital repair/renovation program, and security O&M expense program will comply with all applicable orders, policy, standards, requirements and specifications • 2 years – Refresh the asset registry to identify outstanding compliance issues • 5-10 years – Reduce the number of deficient systems by 50% of the existing total

11.0 ADDRESSING BARRIERS TO ACHIEVING OPTIMAL PERFORMANCE

With the collective increase of BPA’s NERCIP energized and non-energized facilities and the increasing age and number of security system deficiencies affecting BPA security assets, there are a number of barriers that are preventing our program from reaching the optimal asset management performance. Some of these challenges are inherent with the funding and resource constraints that the Agency is experiencing and will be difficult to address, while others can be more easily resolved through possible use of Secondary Capacity Model (SCM), increase in BPA Federal and Contract staff, and reallocation of existing resources and responsibilities. The following list identifies the most significant gaps to optimal performance and proposes the actions that can be taken to address these challenges

Table 11.0-1 Barrier to Optimal Performance

Barrier to Optimal Performance	Responsible Org.	Mitigation (short term)	Mitigation (long term)
Shared ownership of capital assets	OSCO/ Software Development & Operations /Facilities/Transmission	<ul style="list-style-type: none"> Coordinate with main Stakeholders on planned investments 	<ul style="list-style-type: none"> Establish partnership agreements with main Stakeholders (Primary and Secondary Capacity Model options)
Unified O&M program	OSCO/ Software Development & Operations /Facilities	<ul style="list-style-type: none"> Facilities implement IFM contract 	<ul style="list-style-type: none"> Establish partnership with IFM contract and current security vender for O&M portfolio management within OSCO/ Software Development & Operations
Limited Expense Funding	OSCO/ Software Development & Operations	<ul style="list-style-type: none"> Implement alternative project delivery methods Shift focus to Capital Renewal and Replacement 	<ul style="list-style-type: none"> Extend IFM contract to field sites Lobby for increased expense funding to coincide with capital investment forecasting
Limited Resources	OSCO/ Software Development & Operations/Facilities /Transmission	<ul style="list-style-type: none"> Leverage vendor services Contract SME support for IT and engineering disciplines 	<ul style="list-style-type: none"> Integrate Facilities planning, design, and execution into one group within Transmission
Staff Training	OSCO/ Software Development & Operations /Facilities/Transmission	<ul style="list-style-type: none"> Structure training program around strategic objectives 	<ul style="list-style-type: none"> Coordinate training across all project execution partners

12.0 DEFINITIONS

Office of Security & Continuity Office:

- **Alarm Monitoring Station (AMS):** The Alarm Monitoring Station monitors and assesses all BPA Security alarm enunciations for facilities equipped with electronic security systems.
- **Alarm Response and Assessment Performance Test (ARAPT):** The process of determining an alarm condition stimulus, the legitimacy of an alarm and identifying and executing the correct response based on standard operating procedures.
- **Bulk Electric System (BES):** Transmission elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electrical energy.
- **Clear Zones:** Areas established around the fence to provide an unobstructed view to enhance detection and assessment around fences.
- **Deficiency:** Conditions that materially degrade the actual protective effectiveness of security systems causing an unacceptable exposure to security risk or non-compliance.
- **Design Basis Threat (DBT):** The DOE DBT Order (470.3C) supersedes the Graded Security Protection policy. It establishes a risk management process based on a site's Protection Level for implementation of countermeasures designed to mitigate the Design Basis Threat.
- **Electronic Access Controls and Monitoring Systems (EACMS):** Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Electronic Security System (ESS):** Applies to a security system comprised of the following sub-systems: physical access control, intrusion detection, video assessment and surveillance, control cabinet, and associated power and fiber cabling needs.
- **Energy Delivery Facility:** A specific grouping of facilities that support the BPA transmission system. This includes an existing or planned location or site, encompassing all real property and appurtenances, at which a BPA substation, switching station, or radio station is located. Buildings located outside of or that are not a part of a station perimeter fence (if one is present) are excluded.
- **Federal Information Processing Standards (FIPS 201):** A US Federal government standard that specifies Personal Identity Verification (PIV) requirements for federal employees and contract workers.
- **Immediate:** Based on the priority of the need, taking action to accomplish without delay.
- **Inoperable Window (Fixed Window):** A fixed window cannot be unlocked, unlatched, or otherwise physically manipulated to create an "opening" as defined below. A solid pane, or panes, of glass associated with an inoperable window are considered a barrier of entry. Although having a vulnerability of minimal delay time from penetration into a PSP, it must be broken to create an "opening" that would allow physical access. The breaking of the window provides detection, upon discovery, that a potential malicious event, act or unauthorized physical access has occurred.
- **Interagency Security Committee - Risk Management Process (ISC-RMP):** A standardized methodology developed by Department of Homeland Security for conducting security risk assessments on Federal, non-military facilities and buildings. The BPA will utilize this methodology for conducting security risk assessments on PL-7 (non-energized) assets.
- **Intrusion Detection System (IDS):** Is designed to alert security personnel when unauthorized access is attempted and consist of electronic sensors such as motion sensors, contact sensors, and glass break detectors.
- **Limited Scope Performance Test (LSPT):** A performance test that evaluates specific skills, equipment, operations, or procedures. The events of the test may be interrupted to facilitate data collection and may be purposely directed by evaluators to achieve certain evaluation goals.

- **Network Video Recorder (NVR):** Network Recorders are used to store digital video footage captured by surveillance cameras.
- **Opening:** A hole or air gap that someone can physically pass through a part or whole of their body. Ninety-Six (96) square inches is the measurement for each maximum acceptable opening without physical protective measures in place. An allowable, unprotected opening may be greater than 96 square inches provided the narrowest portion of the window is not greater than six (6) inches and the opening does not provide the ability for the whole of a body to pass through or a part of the body to assist in gaining unauthorized access per DOE Order 473.1A, Physical Protection Program. (Example: an opening with the dimensions of 6" by 100" may not require protective measures.)
- **Non-Energy Delivery Facility:** All facilities not covered by the energy delivery facility definition, such as maintenance headquarters office buildings. This includes all real property and appurtenances associated with it.
- **Operable Window:** A window that can be unlocked, unlatched, or otherwise physically manipulated to create an opening as defined by "opening".
- **Physical Access Point:** A point of entry or an opening that creates a means of physical access. Examples include doors, operable windows, or hatches that can be manipulated to create an opening greater than 96 inches.
- **Physical Security Perimeter (PSP):** A perimeter protection acting as the first line of defense in providing physical security for a facility in which BES Cyber Asset (BES CAs), BES Cyber Systems or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
- **Physical Security Performance Assurance Program (SPAP) Tracking:** A process to manage and track testing results, corrective actions and maintenance requests associated with System Performance Testing.
- **Protective Cyber Asset (PCA):** Applies to each asset associated with a high impact BES Cyber System or medium impact BES Cyber System.
- **Protection Level (PL):** The DBT order categorizes Department assets into levels or categories based on consequence of loss. PL's are defined for each category of assets. BPA assets are currently categorized as PL 6-PL 8.
- **Risk:** The probability of loss resulting from a threat, security incident or event.
- **Risk Assessment:** The process of assessing security related risks from internal and external threats to an entity, its assets or personnel. It is typically expressed as: $\text{Threat} \times \text{Consequence} \times \text{Vulnerability} = \text{Risk}$
- **Risk Assessment Methodology for Transmission (RAM-T):** A robust, highly detailed, nationally accepted risk assessment methodology developed specifically for the energy sector (transmission).
- **Risk Management:** The identification, assessment and prioritization of risks followed by coordinated application of resources to minimize, monitor, and control the probability and/or impact of undesired security events. Risk management includes identifying critical assets and key sources.
- **Safeguards and Security (S&S):** Measures and controls implemented for protecting information, assets and personnel.
- **Security Area:** A room or facility that does not contain BES Cyber Assets, which is established to protect employees and sensitive equipment important to BPA's primary mission, by which Physical Access Control Systems are used to control, monitor and limit physical access.
- **Security Condition:** DOE's Security Condition (SECON) levels reflect a multitude of condition that may adversely affect departmental and/or facility and site security. SECON may include terrorist activity, continuity conditions, and environmental, and/or severe weather conditions. DOE has five SECON levels with SECON 5 being the lowest level of readiness and SECON 1 the highest readiness.
- **Security Fence:** A physical security barrier system that provides one or more of the following:
 - Gives notice of legal and safety boundary.
 - Assists in controlling and screening authorized entries.
 - Supports surveillance, detection, assessment, and other security functions by providing a platform for installing intrusion detection equipment.

- Deters intruders from penetrating a protected area by presenting a barrier that requires an overt action to enter.
- Causes a delay in obtaining access to a facility, thereby increasing the probability of detection.
- Security fencing can be constructed with fence fabrics rated at varying penetration resistance (security) levels, as determined by ASTM standards.
- **Security Survey:** A general inspection of the conditions of security systems, or security related assets located at a site. The survey can include items that serve a dual purpose such as fencing (safety and security), lighting, and brush control around the site and other items not considered “security” items but could influence the general condition of the site.
- **Streamlined Security Risk Assessment (SSRA):** The SSRA is a streamlined risk an assessment process designed to apply essential elements of the RAM-T process and reduce the staff hours needed to complete a formal RAM-T assessment. The SSRA leverages the robust aspects found in the RAM-T for threat, consequence and security system effectiveness (vulnerability) analysis.
- **Security System Performance Assurance and Testing Procedure (SPAP) Testing:** The process of testing site security systems such as access controls, intrusion detection systems, VASS systems, lights and other elements directly related to security and regulatory compliance.
- **Threat:** An adversary, undesired event (natural or manmade), person, group or organization that is capable of accomplishing a malevolent act or other undesired event that, if successful, would prevent or impede a mission, task or objective.
- **Video Assessment and Surveillance System (VASS):** System used to assess and identify the behaviors, activities, or other changing information to determine necessary actions (responses) needed to mitigate situations that pose a challenge to physical security by detection. These systems use a collection of cameras, recorders, switches, and monitors, enabling video images or extracted information of security events to be compressed, stored or transmitted over communication networks or digital data links.
- **Visitor:** Anyone who does not have authorized unescorted access or movement within a BPA facility, critical asset site or PSP.
- **Window:** A section of wall, door, etc. that contains a sheet, sheets or blocks of glass in place of a wall.

Investment Classifications:

- **Compliance:** Must be an executive order/directive requiring the specific investment must be made and that the project as proposed includes only the minimum required to comply with the directive. For example Cyber Security, Highway Relocations, biological opinion.
- **Replacements:** In-kind replacement of equipment and components. For example, wood poles, transformers, batteries, existing buildings, breakers, reactors, and conductor.
- **Upgrades/Additions:** Replacement of existing assets that provide addition capacity and/or capability. Examples include breakers, transformers, lines, etc. that after replacement have higher ratings to transfer power. Replacement of applications that provide new capability
- **Expansion:** Adding new assets to the system that did not exist before providing new capability. Examples include new IT applications, new buildings, and new units at existing power generation sites, new line and substations.