STRATEGIC ASSET MANAGEMENT PLAN – 10 YEAR OUTLOOK

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

The Office of Security & Continuity of Operations (OSCO) Strategic Asset Management Plan (SAMP) documents the current state of Bonneville Power Administration (BPA) physical security assets and describes planned asset management improvements, maturity and competencies needed to manage the entire lifecycle of BPA security system assets effectively and efficiently. The SAMP, covering 2024 – 2028, 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 is accountable for supporting BPA mission and stakeholder interests by protecting its personnel, facilities, critical systems, and information. The scope of the Physical Security Program includes a multi-state service territory with more than 450 facilities, 15,000+ miles of high voltage transmission lines, over 5,000 employees and contractors, and thousands of visitors each year. OSCO implements physical security requirements as well as security system designs and standards. BPA strives to remain compliant with regulatory requirements, guidelines, provisions and principles prescribed by the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, the 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 470.3C), and DOE's Physical Protection Program (DOE O 473.1A). 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, CIP 014, and DOE Protection Level (PL) 6 critical 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 addresses the risks while remaining cognizant of staffing limitations, inflation related cost escalations resulting in a need for increased capital funding, and O&M expense funding limitations. In the simplest terms, the older the security system asset, the more costly it is to maintain. Older security assets have longer and more frequent outages, resulting in increased risk to staff and facilities and more costly repairs.

At current staffing, funding (Sustain-Capital, O&M-Expense), and BPA Transmission project capacity levels, OSCO will primarily focus on "break-fix" as our strategy for maintaining our electronic security systems while we continue to implement a limited-scope capital replacement program, with a priority on NERC CIP 006 sites. This document will lay out, in detail, the current cost and trajectory as well as a path forward to address lifecycle management.

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 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 years 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

Digitally signed by ROBIN FURRER
Date: 2025.03.10 12:37:12 -07'00'

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 to reach future-state goals and establish the necessary data to inform, maintain and improve the health of the capital portfolio. The managers of each contributing stakeholder group reviewed and supported the conclusions and recommendations contained in this document.

2.2 Strategy Development Approach

To provide the necessary security asset lifecycle planning, projects and services, this document was developed closely with a multitude of stakeholders, partnering organizations, and subject matter experts (SMEs) to ensure the strategic approach is well 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. The process to refresh this document focuses on the integration of contributor 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 incorporates lessons learned gained by reviewing the impacts of the last strategy.

2.2.1 Key Contributors

All roles and responsibilities for key contributors and execution partners may be found in the BPA Procedure 432-1-2 Critical Asset Security Plan (CASP) Section 1.6.

Strategic Oversight and Strategy Guidance

- Chief Administrative Officer:
  - Approves the OSCO Strategic Asset Management Plan and Asset Plan, is the final signing authority on capital business cases and O&M funding approvals, and oversees delivery of Key Performance Indicators
  - Ensures all security policies and procedures are adhered to by the workforce
- Manager, Office of Security & Continuity of Operations
  - Provides strategic direction and mission objectives
  - Implements all physical security policies and procedures intended to meet regulatory compliance requirements for Physical Security
  - Serves as the final authority for approving physical security systems intended to meet regulatory compliance requirements and other physical security protection strategies
  - Ensures new security systems are validated to function as designed form an operational perspective and documentation of acceptance of the projects as completed

Execution Partners of the Asset Plan

- Supervisor, Physical Security
  - Defines budget allocations and performance targets for security capital and expense asset investments
  - Ensures security system acceptance and performance assurance testing are executed

  - Ensures security designs are reviewed and approved to meet security related regulatory compliance requirements and other protection strategies
  - Provides subject matter expertise for NERC CIP physical security standards
- Manager and Supervisor, Software Development and Operations
  - Responsible for the overall procurement, development, integration, modification, and operation and maintenance of the IT-supported security systems
  - Develops and approves installation and design standard for the IT physical security systems
  - Identifies, assesses, and approves software and hardware for IT-supported physical security systems
  - Provides engineering support for the installation and operation of IT supported physical security systems
  - Validates IT-supported physical security systems are installed according to design and coordinates with NNT to ensure the system or build is operational
  - Validates those devices installed during security projects are installed as designed and function correctly
- Manager and Supervisor(s), Transmission Project Management
  - Project Management Office provides Project Management for security projects assigned (continuous monitoring and reporting on scope, schedule, budget, variance, and mitigation)
- Manager and Supervisor(s), Substation Engineering (Electrical, Civil/Structural, Telecom)
  - Substation Engineering, Facilities Engineering, and Transmission Civil Works Engineering provides physical and electronic security consulting, scoping, engineering, design contract support, and construction support
- Manager and Supervisor(s), Transmission Field
  - Manages physical field operations
  - Provides site condition consulting and participates in the physical and electronic security scoping, design, and construction support
- Manager and Supervisor(s), Facilities Planning and Projects
  - Collaborates with OSCO to provide and receive ISC-RMP requirements for non-energized buildings where security system assets are installed. Provides input to the Asset Plan and coordination of joint project schedules. Leads the effort for funding, scope, design, and construction of physical and electronic security systems within their asset plan
- Manager and Supervisor(s), Transmission Strategy, Asset and Program Management
  - Collaborates with OSCO to provide and receive requirements for energized buildings where security system assets are installed. Leads the effort for funding, scope, design, and construction of physical and electronic security systems within their asset plan
  - Provides input to the Asset Plan and coordination of joint project schedules
  - Creates project estimates and supports OSCO's portfolio and program execution
- Program Managers (Transmission, Facilities, Software Development and Operations)
  - Informs and coordinates with the OSCO regarding any project affecting a physical security perimeter (PSP) to ensure PSP integrity is maintained during all stages of a project. Ensure Physical Security requirements and standards are integrated into project planning

  - Ensures such projects are funded to meet or maintain compliance requirements and BPA standards. Ensure project scope and funding changes are addressed as appropriate
  - Ensures OSCO reviews and approves project designs to ensure physical security protection strategies and compliance requirements are met
  - Ensures all security perimeters, devices, and systems are installed and functioning at project completion
  - Coordinates with OSCO to validate PSP changes and test security systems prior to project completion. Notify OSCO of any potential or discovered alterations to the PSP
- Finance
  - Provides budget operations (expense) services and capital investment management services
  - Operates and maintains the security asset management accounting system; develops and issues capitalization policies and procedures; and provides guidance regarding work order set-up and completion, asset retirements, and capitalization/expense determination
- Portfolio Management Team (PfMT)
  - Voting members from Strategy, Asset & Program Management, Asset Management Business, Delivery, & Performance, Transmission Project Management, and Construction and Maintenance Services, approves capital security projects for OSCO as they are submitted, and maintains the capital investment acquisition process throughout the project lifecycle

2.2.2 Key Activities

OSCO aligns and adapts its capital and expense program business practices to their main collaborative partners: Transmission and its established Transmission business model; Facilities' business model; and IT's business model. OSCO executes this SAMP through the following steps:

- Identify and plan electronic security systems assets
- Review and document the current health of security assets
- Identify security risks and execute risk-based decision-making process
- Develop strategies to get from current state performance levels to future state performance targets
- Identify challenges and gaps
- Work with Finance to align SAMP future spend to the OY, Rate Case, and IPR budget
- Align with Facilities for work related to all non-energized facilities
- Align with Transmission for work related to all energized facilities
- Review of BPA's 2024-2028 Strategic Plan and OSCO's SAMP to evaluate for alignment
- Identify and engage with partner organizations to review priorities, work planning, timelines, resources, and budget/funding levels for strategic alignment
- Vet FY24 SAMP with partner organizations and stakeholders
- Engage with CAO asset categories to align SAMPS with future year OY and IPR cycles

3.0 STRATEGIC BUSINESS CONTEXT

3.1 Alignment of SAMP with Agency Strategic Plan

The SAMP covering 2024 – 2028, 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, existing but aged 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 financial investments and protection strategies with the six Agency strategic goals that encompasses best security practices:

1) Invest in people to strengthen financial health
2) Enhance the value of products and services by modernizing assets and system operations
3) Sustain financial strength by providing effective, repeatable, and sustainable security systems and services
4) Mature asset management by providing effective, repeatable, and sustainable security systems and services
5) Preserve safe, reliable system operations while 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
6) Modernize business systems and processes including physical security system operations

The guidance defined in the SAMP informs the OSCO capital and O&M programs 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 with their main collaborative leaders: Transmission, Facilities, and Information Technology (IT). These organizations have developed value propositions and focus areas with corresponding outcomes to facilitate the delivery of the OSCO SAMP (Figure 3.1-1). Each of the organization's focus areas and outcomes are tied to one or more of the agency's six strategic plan goals 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**	Develop asset strategies and plans that are informed by asset condition, criticality, and risk: *Continuous effort* 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:	**Goal**: Sustain financial strength • Maintain cost-management discipline and execute capital plans **Goal:** Mature asset management • Administer a security-industry leading asset management program that takes into consideration asset

OSCO Focus Areas	Supporting Strategy, Action, or Process	Agency Strategic Plan Alignment
➢ **Value and Risk-Based Asset Management**	*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 to manage investments in a scalable/flexible manner – i.e., Portfolio Optimization, Asset Rebuilds, Discreet Asset Replacements, O&M - Sparing strategies* Partner with cross-Agency organizations to align related policy/standards/requirements, processes, and systems: *Continuous effort*	condition, criticality, health & risk (CHR) **Goal:** Modernize business systems and processes • Modernize security system operations and supporting technology • Address security requests by using flexible, scalable, and efficient solutions
Long-Term Viability ➢ **Integrated & Efficient Processes** ➢ **Data-Driven Decision Making** ➢ **Innovation & Continuous Improvement**	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: *Security System Health and Criticality Matrix* Develop performance metrics that informs asset investments and impacts to energy delivery and non-energy delivery facilities' electronic and physical security objectives *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.*	**Goal:** Sustain financial strength • Maintain cost-management discipline and execute capital plans **Goal:** Preserve safe and reliable system operations • Administer a security-industry leading asset management program • Modernize security system operations and supporting technology **Goal:** Modernize business systems and processes • Modernize security system operations and supporting technology • Address security requests by using flexible, scalable, and efficient solutions • Develop and Implement policies, standards, requirements, specifications to include cost estimation and out-year capital program forecast for Agency planning and optimization

3.2 Scope

The SAMP charts the course for delivering long-term strategic security benefits for BPA and sets asset performance objectives, identifies risks, and outlines strategies for improvement. The OSCO Asset Plan is aligned with the SAMP and identifies and describes the investments required to fulfill the more near-term strategies and objectives.

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

- Establish a sustainable security system lifecycle management program. Such capital and expense program shall cover new and O&M security 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.
- Ensure Transmission and Facilities upgrade projects and new construction projects incorporate Agency, DOE, and national level standards and requirements.
- Ensure upgrade projects and new construction by Transmission and Facilities incorporate required security measures and related costs into individual projects. All resulting security systems are 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 perimeters 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.

This SAMP applies to Transmission and Facilities that utilize or create physical and electronic security system assets. It is these organizations' 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. For further information on these responsibilities and dependencies then reference the OSCO Asset Plan, Transmission Physical Security Policy STD-D-000032, and the Critical Asset Security Plan (CASP).

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*** (critical assets) as material, equipment, software, or hardware that is used for the primary purpose of providing physical security protection. BPA's electronic security system assets (300+) is protecting over 130 separate facilities made up of NERC CIP

Medium and Low energized substations, Maintenance Headquarters, Office Buildings, Aircraft Hangars, Control Centers, and three complexes (Ross, Munro, and Celilo).

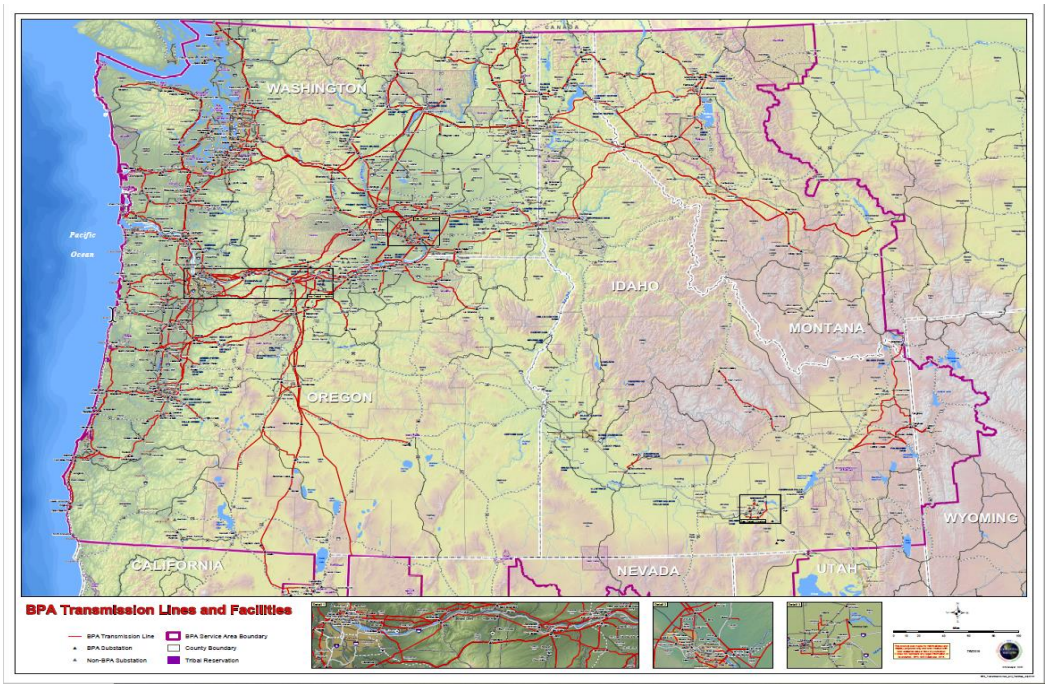
Security system asset risk management involves anticipating and avoiding events that have the potential to adversely affect OSCO program goals and tactical/strategic objectives. A security system asset within a facility or designated area serves to deter nefarious activity and must provide the capabilities of detection, delay, assessment, communication, and response. Security system assets provide:

- Protection of employees
- Protection of critical energized and non-energized 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

Individual assets or components make up security systems that collectively provide various levels of physical security protection depending on the asset being protected. Definitions of certain critical security assets may be found in the Critical Asset Security Plan (CASP) and Transmission's Physical Security Policy STD-D-000032, which are referenced in the OSCO SAMP and OSCO AP.

Figure 3.3-2, Asset Locations

BPA's geographic impact that needs to be secured has currently built 15 sites supporting full or partial NERC CIP 014 security enhancements and is currently operating over 12,000 electronic security devices in the protection of over 116 separate facilities made up of NERC CIP 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 risks for BPA sites through the comprehensive 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 risks 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 risks 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 with 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's NERC CIP 014 modeling studies, and Transmission and Facilities own capital infrastructure programs.

As BPA constructs new facilities or retrofits existing facilities, we will continue to see steady growth in the number of 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

The duration of this SAMP is 10 years with a refresh every three years unless there is a notable 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, most security measures support the Transmission Services operation of field sites.

In 2009, BPA's NERC CIP 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 NERC CIP 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. Refer to Table 9.0-1 Responsibilities of OSCO and Other Business Lines.

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, evaluated, 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/Public	Safety	Public safety management system	Non-conformance records
	Reliability	ISC-RMP, US DOE	Design Basis Threat, Facility Security Level
	Security	Security Incident Reports	Nefarious Activities, Complaints
	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	Cad Software, 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	Video management system, Alarm management systems, 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 Trustworthy Stewardship	Industry regulations and standards (NEPA) Financial system US DOE and BPA Security standards and requirements	Environmental Assessments Pollution Abatement Clearances Risk and Vulnerability Assessments
	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
	Training	Administrative database	Security awareness; Agreed professional development
	Safety	Industry regulations and standards	Safety Metrics (Lost Time Accident Rates, Days Away Restricted or Transferred, Total Case Incident Rate)

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

NERC CIP 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. In addition, as BPA addresses a recent DOE IG Inspection report on physical security and the resulting necessary corrective actions plans, impacts are expected to result with how we prioritize work with Transmission partners, as well as influence what is critical asset sites are rated as a Protection Level 6 (PL-6) under DOE protection requirements.

Aging and technologically obsolete systems

Many 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. Physical Security 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 approaches, 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
Pandemic Response	Since the inception of the pandemic, it has had "ripple-affect" of all in-flight projects as project execution methods changed the downstream impacts requiring portfolio rebalancing and a re-evaluation of financial forecasting.
Undesirable security events and evolving threat dynamics	Events driving the need for an increased security posture and the need to expand existing or introduce modern technologies to counter threats
NERC and WECC mandatory reliability standards	Demonstrating compliance increases OSCOs operating cost and continues to demand significant human resources. Increased stress-balance of various refined orders, policies, standards, and audit findings from US DOE, NERC, WECC, Safety, Engineering affecting scope/design/build of physical and electronic security systems to meet all regards to "best security practices and compliance."
Specialized material and engineering standards	Procurement and engineering costs are high resulting in research and solicitation of best and affordable engineering standards that specify the most cost-effective design features and construction material.
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. Technological obsolescence will require OSCO and Software Development & Operations to replace equipment and systems in shorter cycles, increasing the cost of its electronic security systems.
Market conditions and constraints (Design/Build) due to an abundance of commercial/residential sector work	Higher bid prices on design/build limit 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.
New Supply Chain Disruptions	Some products have significant increases in lead-time and in some cases are no longer available (IC chip enabled devices, card readers, cameras). This will have impacts on project delivery schedules and the ability to maintain project completion targets.
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.
BUD Network Bandwidth	BPA's BUD Network/Telecom bandwidth is not adequate at several BPA energized facilities and is having a negative impact on system performance. Bandwidth concerns are being addressed within the CIO for immediate action at substations lacking in proper bandwidth for BUD and security asset needs.
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, impacting the amount of work and rework needed for contract development. Availability of vendor/contractors to bid projects and accomplish work within high voltage substation environments.
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 adequate funding for security system O&M diverts human and fiscal resources away from lifecycle planning and renewal and perpetuates a reactionary approach to asset management.
Attraction and retention of high-quality talent will be challenged by an increasingly competitive, innovation-filled energy industry landscape	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 costs and duration. 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.

5.1 SWOT Analysis

Table 5.1-1: SWOT

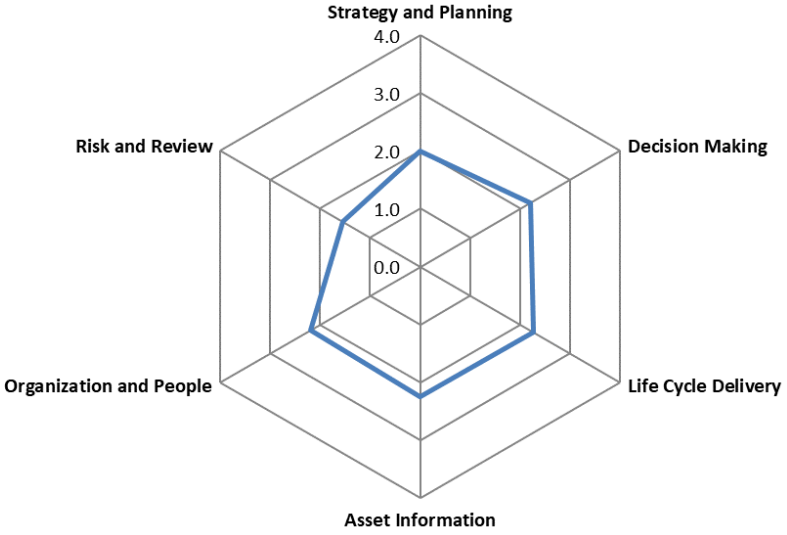
Favorable	*Unfavorable*
Strengths	***Weaknesses***
• **Security:** Increasing Agency-wide commitment to security-centric culture, where best security practices are a daily driver for decision making • **Executive Support:** Senior Leadership has embraced and pushed forward security asset management as 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 regarding 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 historical projects to empower current and forecasted projects and best security practices	• **Security:** Inconsistent adoption/acceptance of security system standards, resulting in failure to fully implement required standards with non-security led projects • **Staffing:** Capacity of current staff is not sufficient to accomplish core work or to address expansion work. Additionally, current workforce is within 4-6 years of retirement • **Aging Infrastructure:** Security systems at end-of-life foster an environment of increased security risks such vandalism, property destruction, US DOE and NERC non-compliance, technological obsolescence, etc. Furthermore, deferring replacements limits BPA's ability to control costs • **Break/Fix and "One-off" Actions:** Unplanned/tactical O&M and "one-off" actions routinely consume staff time since staffing levels of partner organizations remain low • **Transmission vs. Facilities 1:** Competing projects and process management systems between different business lines • **Transmission vs. Facilities 2:** Multiple business line ownership of facility assets (i.e., fence lines and gates) impacts the consistent delivery and tracking of such investments • **Asset Management Cultural Awareness**: Everyone has an impact to asset management and needs to be aware of their role
Opportunities	***Threats***
• **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 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 is need for over-all compliance and best security practices	• **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:** Escalation in material and labor costs in availability due to economic conditions related to COVID-19 Pandemic • **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 from a 1.5 maturity level in 2022 to a current overall maturity level of 2.1 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

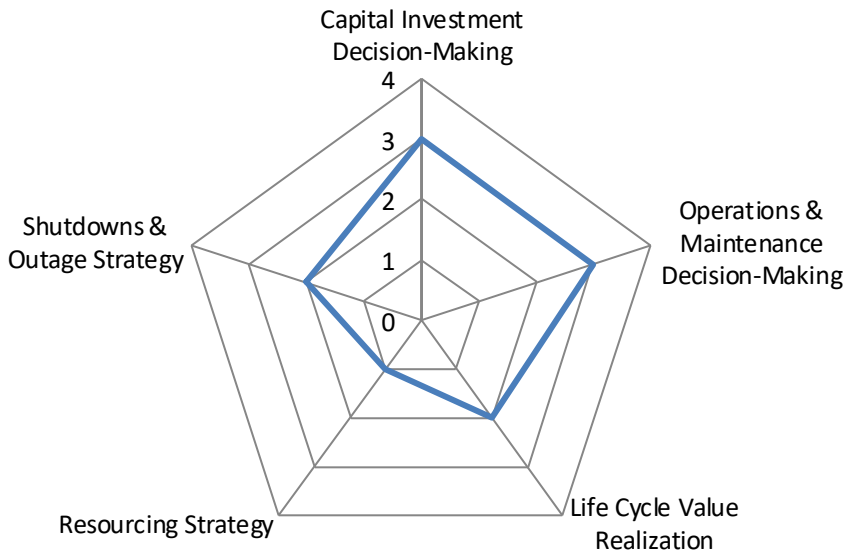
Asset Management Capabilities and Systems average a maturity level of **2.1** across all subject groups in the Institute of Asset Management (IAM) Asset Management Maturity model. The current Maturity Level score of OSCO's security system asset operations, maintenance determinations, and management function, integrated with NERC CIP 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 have been 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 systematicaly 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	Maturity level 2 **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. **Weaknesses**: Competing Transmission and Facilities capital and O&M planning and projects can interfere with OSCO's security system planning and execution. SME asset allocation and procurement timelines are needed to enhance the fidelity of strategic plans. Insufficient bandwidth issues at sites have led to reduced video assessment for security monitoring. **Changes since 2022:** Improvement with respect to Integrated Work Planning (IWP) and interagency coordination; lack of qualified PM and PE SMEs to take on projects; project scheduling has improved with IWP; material procurement has lagged due to overall market inflation, competing projects needing the material, and lack of material. All OSCO capital projects will include bandwidth needs within its estimates, scope, design, build processes using Transmission CIA and CDD/LCDD process and documentation. Completed BPA Procedure 432-1-4 Physical Security Capital Enhancements for Energy Delivery and Non-Electric Delivery Facilities. 

Decision Making	Maturity level 2.2 **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. **Weaknesses:** 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. **Changes since 2022:** BPA Finance informed OSCO the best way to increase O&M funding is through IPR allocation; O&M financials are added to new financial spreadsheet for business case development only for forecasting tracking purposes. J-orgs have a place within Transmission's revised CDD and LCDD to ensure all project management and project engineering will consult J-orgs needing to have an impact on BPA's projects. **Decision Making** 

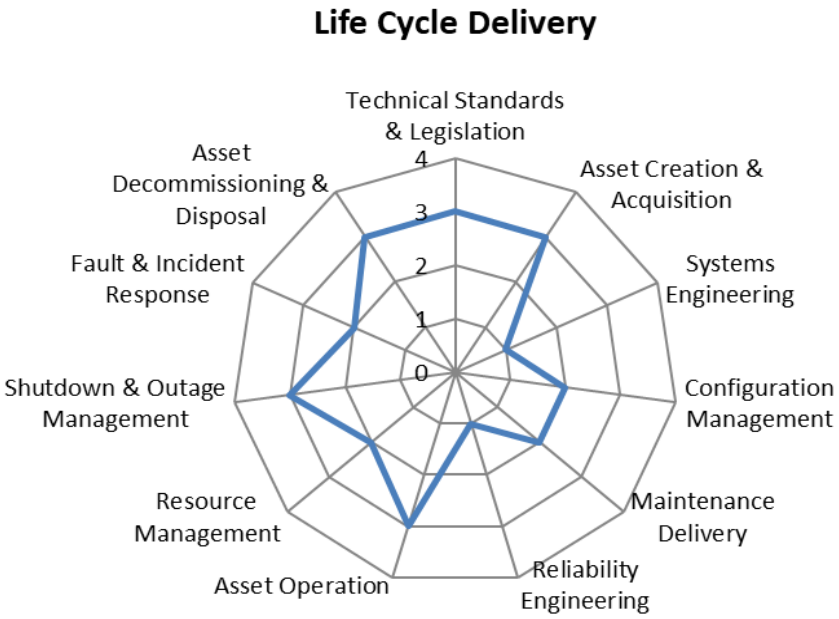
Life Cycle Delivery	Maturity level 2.3

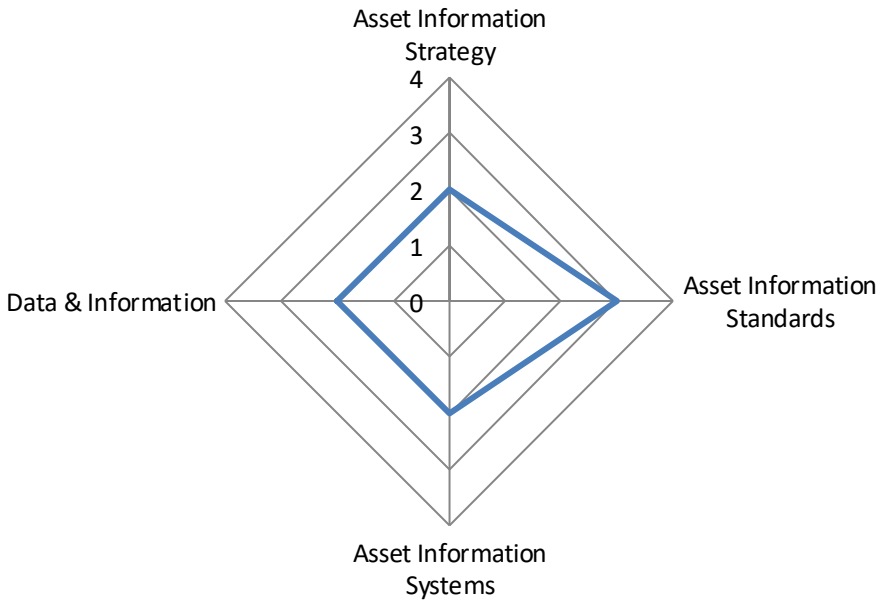
Strengths: OSCO has ensured US DOE, NERC, and BPA's best security practices, policy, standards, and requirements are adequately defined and followed through asset delivery to O&M scheduling. This is an ongoing process, and improvements are made every year, but standardization of the scoping/programming 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.

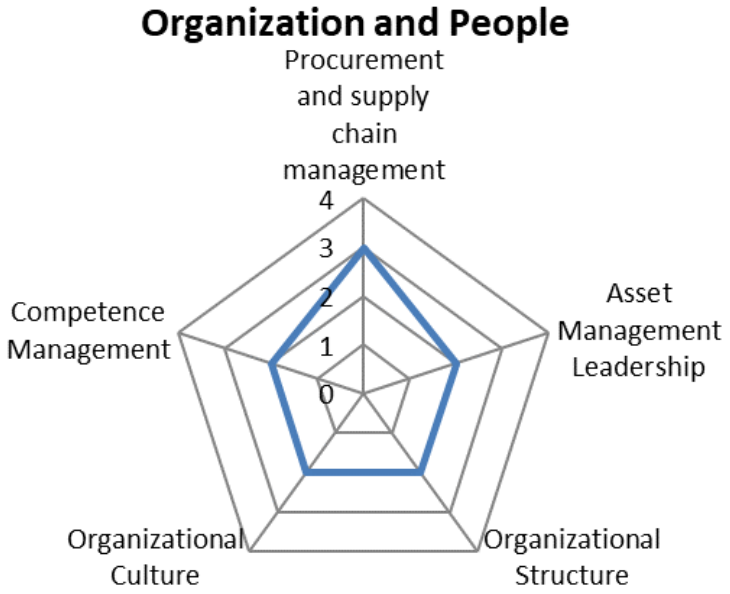
Weaknesses: Perimeter fencing standards and specifications are established yet a lack of cross-Agency cooperation for the lifecycle replacement of perimeter fences for energy and non-electric delivery facilities can lead to unsafe and unsecured BPA property.

The lack of centralized authority regarding 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.

Changes since 2022: Continued cross-agency meetings to solidify who is responsible of perimeter fence new builds, rebuilds, and maintenance in energized and non-energized sites. Completed "Right Size Scoping Effort" which integrates the new CIA process tasking for PgMs including new Project Initiation Documents and new the CDD/Limited CDD.



Asset Information	Maturity level 2.3 **Strengths:** Currently Sunflower, Alarm management systems, and Video management system are electronic security asset management systems 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. **Weaknesses:** Pre-pandemic estimates are no longer valid due to increased inflation and material/labor costs, Transmission Estimating of security system cost-information is immature due it was established within the last six years. **Changes since 2022:** Completed the physical and electronic security system estimating initiatives for Transmission "estimating shells" for cross-agency use as Transmission, Facilities, and OSCO plan and estimate projects that contain security measures. Developed the Security System Health and Criticality Matrix. Updated Policy 212-1 Property, Plant, and Equipment Capitalization - Plant Unit Catalog (PUC) spreadsheet. **Asset Information** 

Organization & People	Maturity level 2.2 **Strengths:** The full Cross-Agency security team consisting of Federal and Contract SMEs and staff is and provides a diverse range of skillsets and an elevated level of engagement. The productivity of staff has remained consistently high. Procurement and supply chain processes are in place. **Weaknesses:** Lack of defining security asset management roles and responsibilities across BPA stakeholders slows the development of 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 various 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. **Changes since 2022:** Transmission increasing PM and PE "bench-strength" regarding resourcing for OSCO's security capital program; NNT PHYSEC personnel has increased by three people. Asset management competencies and understanding have grown within OSCO due to training and practical work. 

Risk & Review	Maturity level 1.6 **Strengths:** Stakeholder engagement regarding security needs are listened to 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. 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. **Changes since 2022:** Security System Health and Criticality Matrix is complete, it is an overall tracking document to score the criticality, health, and risk of BPA's electronic security systems. 

6.2 Long Term Objectives

OSCO's primary long-term objective is to achieve asset Maturity Level 2.5 (Developing) in **Risk & Review** by or before the third update to the SAMP (2027). 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: RISK & REVIEW

OSCO and Software Development & Operations initiative for scoring and tracking security critical assets has resulted in the creation of the Security System Health and Criticality Matrix for life cycle delivery which identifies the "electronic security system, critical assets" of a site and cross-references that information with the site's

Protection Level (PL) Designation set under DOE Order 470.3C, Design Basis Threat (DBT), Section 7.2. This alignment of data allows, OSCO, Software Development and Operations (JLS), Transmission, and BPA Facilities to better apply industry standards and best practices by, incorporating security system assets into the decision-making process around management of capital, O&M, and "one-offs" projects.

BPA's security program is governed by several external oversight bodies, each with policy making authority. BPA continues to mature its ability to achieve full compliance with all the policies and standards it must implement. Change management and ongoing communications are critical in gaining momentum for full implementation of all security policy and standards for BPA facilities. Key components that will drive success include appropriate funding and executive level commitment to achieving best security practices. It is imperative that financial and personnel investment decisions prioritize security needs as a criticality program for proper IAM, best security practices, and US DOE and NERC compliance.

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 our existing standards, processes, and policy influence the cost of capital security systems and the O&M of security assets, we can establish greater visibility of lifecycle costs to create opportunities for savings and help us shift away from a reactionary approach to an initiative-taking approach for managing security assets.

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

- Specific: OSCO will collect and quantify physical security needs and asset lifecycle costs for decision-making.
- Measurable:
    - OSCO will work with internal business partners to determine delivery methods for Capital, O&M, and "One-Off" projects to incorporate security assets associated with documented vulnerability assessments and risk assessments by EOFY 2027.
    - OSCO management will work with internal business partners to determine risk acceptance or implementation of security measures related to vulnerability and risk assessments and to document resolution by EOFY2026.
- Achievable: OSCO will continue to determine where efficiencies can be gained with security system program integration.
- 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/processes etc."
- Time bound: By end of FY24. Due to a shortage of qualified Transmission Field SME support and the complexity of assessing security system health, the ability to collect and quantify physical security needs and asset lifecycle costs could be hampered.

6.3 Current Strategies and Initiatives

The current activities of OSCO's asset program strategies which have advanced OSCO's long-term objectives of Risk & Review are dependent upon Transmission, Facilities, and Software Development & Operations initiatives regarding work processes.

1. OSCO and Software Development & Operations' O&M Initiative:

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 into 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.

2. Electronic Security System Capital, O&M, and "One Off" Initiative:

OSCO along with BPA business partners administers the contract to a commercial security systems integrator for the purpose of obtaining design and construction (design-build) services for work at new and existing Energy Delivery and Non-Energy Delivery Facilities within BPA's service territory. Task orders under this contract may include both design and construction (design-build), or either design or construction services. This type of work may include, but is not limited to:

- Electronic security systems
- Electrical and fiber optic work
    - Related to electronic security systems
    - Standalone electrical and fiber optic work
- Associated incidental Architectural/Structural/Civil work
- NERC CIP 006 & 014 upgrades of electronic security systems
- Minor "one-off" repair/maintenance/upgrades to electronic security systems
- Some sites may require minimal Architectural/Civil/Structural needs and measures

3. Risk Acceptance or Corrective Action of Security Measures Initiative:

BPA's Physical Security Office will collect the identification and prioritization of security risk assessment "expense stream corrective actions" to decide which "expense stream" items will be executed based on available Transmission Field personnel, funding, and a target for execution completion. BPA's Officially Designated Federal Security Authority (ODFSA) will review the results of corrective action implementation recommendations for approval or disapproval along with a collective recommendation to the ODFSA for risk acceptance or corrective action implementation.

4. DOE IG Inspection Corrective Action Plan Initiative:

BPA's Physical Security Office recently underwent a DOE IG Inspection to review the implementation of physical protections for BPA's critical assets. This inspection resulted in two DOE IG recommendations and associated corrective action plans (CAPs) to be executed by BPA. The initiative to address these DOE IG CAPs by BPA will result in 1) BPA reviewing and defining the criteria we use to identify our critical sites; and 2) BPA addressing the prioritization of capital security projects for critical asset sites. These two areas are expected to impact the future of our asset management strategy.

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

“Critical Assets” is a term used in several contexts within the Security community. OSCO assigns in this context, "critical assets" referring to the key components of the electronic security system (ESS) that protects equipment, facilities, and personnel which OSCO must maintain in a healthy state to achieve best security practices, Federal compliance, and reduce risk of criminal activity with standards set by:

- DOE Design Basis Threat (DBT) (DOE 0 470.3C)
- DOE Physical Protection Program (DOE O 473.1A)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards 006
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards 014
- Department of Homeland Security Presidential Directive - 12 (HSPD-12)
- BPA Physical Security Policy STD-D-000032-00-02
- BPA Policy 430-1 Safeguards and Security
- BPA Policy 432-1 Physical Security

The key components of BPA’s ESS protecting Energized and Non-energized facilities:

- Physical Access Control
- Video Assessment
- Intrusion Detection
- Control cabinet and ancillary equipment
- Automated Gates (security electronics)
- Security Software

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, like a fire suppression system, plumbing system, or lighting scheme.

As described in Section 3 of this SAMP, to ensure alignment with the agency’s 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; 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 to 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 (BES) operations or outage in the event of failure.
- **Mission Essential:** Control houses, radio stations, associated facilities and backup power systems that are provided for the 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 470.3C), DOE's Physical Protection Program (DOE O 473.1A), 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 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 considers 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 overall performance requirements are officially described in the CASP. The following is a brief description of the PL 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 designated as High Impact by NERC CIP 002 and identified as NERC CIP 014 sites.
- PL 6 Medium Impact – Substations designated as Medium Impact (w/external routable controls) by NERC CIP 002 and identified as NERC CIP 014 sites. These are 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.
- PL 7 Medium Impact – Substations designated as Medium Impact (w/ERC or non-ERC) by NERC CIP 002 but are **not** designated as NERC CIP 014 sites.
- PL 7 (Other) – Substations designated as Low Impact under NERC CIP-002, or facilities not in scope for NERC CIP such as administrative buildings, MHQs, or leased buildings.
- PL 8 Personnel - PL 8 assets are personnel. PL 8 is used in conjunction with other PLs, not as in standalone PL.

Note that BPA Physical Security, working in conjunction with Transmission, will need to address outstanding DOE IG inspection recommendations and CAPs to define clearer, unified criteria for designating substations as PL-6 under DOE requirements. Typically, the designation of PL-6 sites would only have been considered based on the site being designated as a NERC CIP 014 site, as these sites pose greater vulnerabilities to the bulk electric system. Going forward, BPA will need to consider other consequence criteria, such as a site's impact to national security, public health and safety, economic security, generation, or other critical aspects associated with regional and national electric grid reliability.

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-know basis but can be discussed and explained on a case-by-case basis.

Risk Management

OSCO implements approved security assessment principles to identify and document risks, 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.

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 threat assessments, which help 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.

Security System Health and Criticality Matrix

OSCO and Software Development & Operations have created the Security System Health and Criticality Matrix which dovetails the "critical assets" (ESS) of a site and cross-references the site by Protection Level (PL) Designation set under DOE Order 470.3C, Design Basis Threat (DBT).

The team evaluates all sites containing an ESS (energized and non-energized) and assigns numerical values to determine ranking for any future security actions. This also considers the Regional/District locations to maximize time, material, and labor efforts.

- NERC High 5
- NERC Medium 4
- NERC Low 3
- ISC-RMP (MHQ/Admin) 2
- MISC (Gates) 1

As this is the first year initiating this matrix, OSCO is reviewing current critical assets having a health score to determine out-year planning. CHR data and analysis is utilized with careful consideration of all other available information such as SME input and data reporting. CHR data and analysis is an evaluation tool with several key data factors available for raw evaluation, but prioritization methods must consider a thorough understanding of the maturity of the calculated data.

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 & NERC CIP 014 (DOE PL6) 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 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 & FY22 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 NERC CIP and BPA security compliances and best practices adhered to and resulted in OSCO's FY21& FY22 capital portfolio being underspent.

As FY22 closed and FY23 began, OSCO had an expected range of uncertainty around the capital spend being larger than normal because of projected lead times and cost inflation. Contract award and other project management aspects were decided after the SOY budget process ended. On the high end, these issues resulted in an overspend of $9.3M above the $8.2M IPR budget. The recommended approach avoided making a request that may overstate the need of more funds now that the contracts and planning are completed.

Furthermore, within the Pacific Northwest Region, Security Services + Installation have seen a >1.5% increase over the past three years and expects to see >2% over the near future years.

- Buyers experience significant unexpected or hidden costs in this market. High total cost of ownership makes it challenging to budget or negotiate for these costs beforehand.
- There is a low availability of substitutes in this market, indicating that buyers will face difficulty in leveraging other products or services to secure discounts.
- Switching costs are high in the market, which makes it costly for buyers to switch vendors in search of a more favorable deal.
- Prices have been rising quickly during the past three years, which has forced buyers to act more urgently to avoid rising prices.
- Supply Chain Risk is high in this market, which reveals that vendors are likely to have difficulties in securing the necessary products and equipment for Security System Installation.
- Prices for Security System Installation have fluctuated sizably. Instability in market prices has been making it more difficult for buyers to anticipate prices and plan accordingly.

Security Fencing have seen an >5% increase over the past three years and expects to see a >2% over the next year.

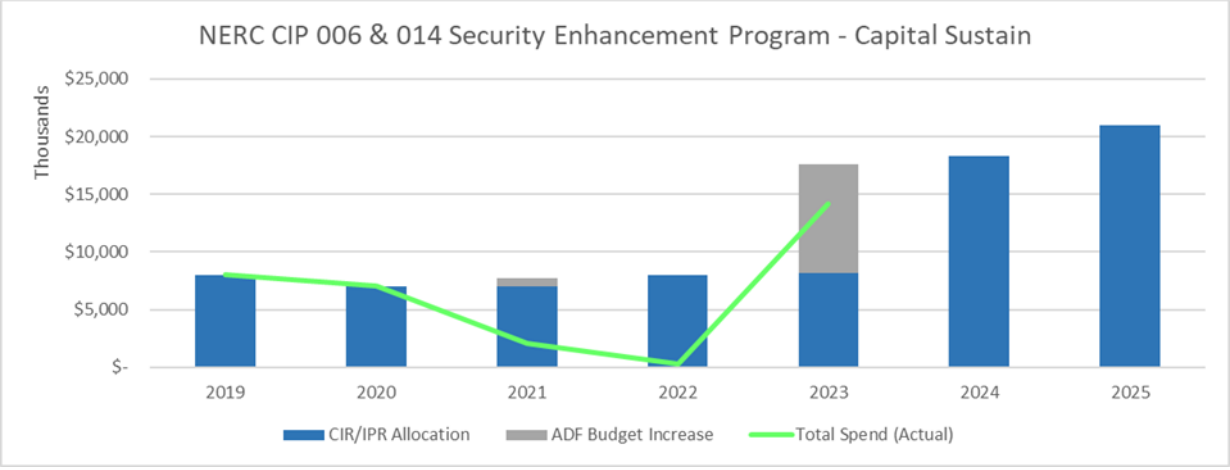
- Prices are forecast to increase quickly during the next three years
- Prices have been rising quickly during the past three years, which has forced buyers to act more urgently to avoid rising prices.
- Price drivers have been highly volatile during the past three years, which increases the likelihood of sudden shifts in market demand and/or prices.

Regional cost index document that reflects approximately 9% increase in costs in just the last year and a total of >35% increase for the past four years.

Table 8.1-1 Historical Expenditures, Capital Sustain and O&M Expense

NERC CIP 006 & 014 Security Enhancement Program	Historical Spend (in thousands) With Current Rate Case						
Capital Sustain						Current Forecast or Rate Case	
	2019	2020	2021	2022	2023	2024	2025
CIR/IPR Allocation	$8,000	$7,000	$7,000	$8,000	$8,200	$18,300	$21,000
ADF Budget Increase		$700			$9,370		
Adjusted Allocated Total		$7,700			$17,570		
Total Spend (Actual)	**$8,081**	**$7,088**	**$2,039**	**$330**	**$14,190**	**$18,300**	**$21,000**
Expense (OpEx)	2019	2020	2021	2022	2023	2024	2025
O&M SOY	$600	$650	$650	$700	$700	$1,200	$936
O&M OY	$635	$650	$650	$720	$750		
Total Spend (Actuals)	**$635**	**$624**	**$640**	**$706**	**$729**	**$1,200**	**$936**

Figure 8.1-2 Historical Expenditures, Capital Sustain



In accordance with DOE Order 473.1A, 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 (workflow 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 an elevated 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 using 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) • 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 regarding 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.

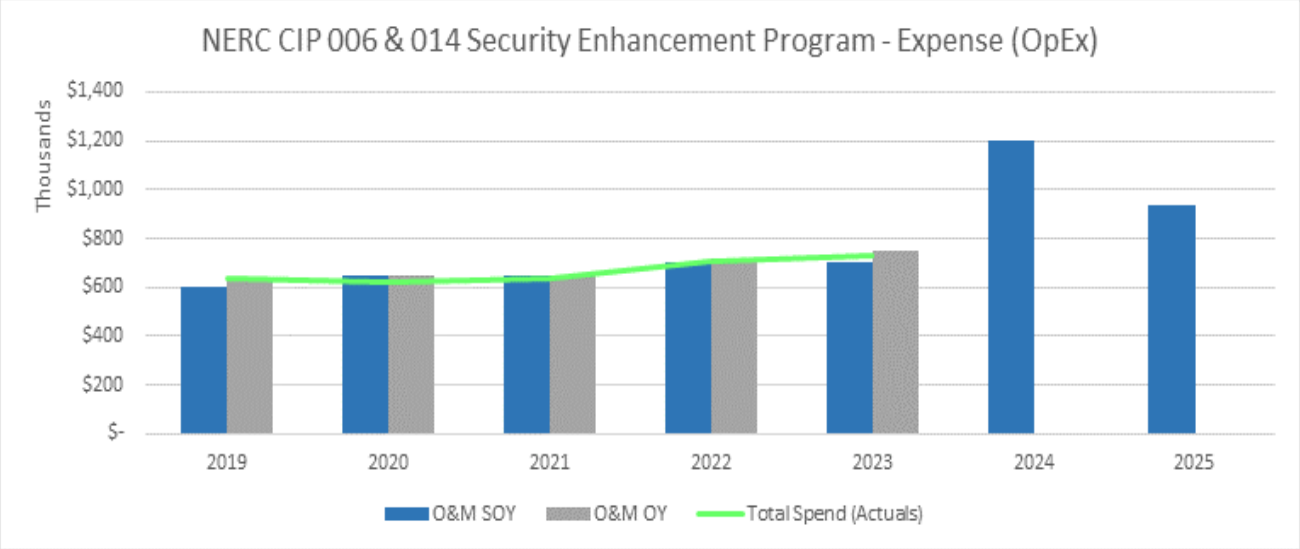
This SAMP does not account for the physical and electronic security systems that the Transmission and Facilities capital programs will add onto their assets, which has been well over 10 new projects/sites within the last two years. However, the expense streams requested by OSCO within IPR 24 will support O&M needs for all BPA electronic security systems, whether generated by OSCO, Transmission, or Facilities.

Given the age and condition of BPA’s electronic security systems, the O&M financial resources are directed towards the acquisition, renewal, and renovation phases of lifecycle development. This emphasis of O&M will yield a tremendous impact on asset condition for the period of capital project execution, this security system O&M emphasis is dependent upon Transmission, IT, and contracted design/build expertise and availability.

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 most 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 show 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 are becoming exceedingly difficult to absorb under current maintenance dollars. The decrease in the firm fix cost is 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 Historical Asset Sustain Trends vs Forecast

OSCO's capital program has completed 100% in executing NERC CIP 006 & 014 asset sustain replacements based upon previous forecasted levels as material and labor cost increase and inflation trends are rising. As of FY23/24 using the Optimal/Expected criteria levels, OSCO has seen positive indication of projects to continue the trend of 100% forecasted to 100% completion. Rate case projections for FY22 and FY24 and beyond are included in forecasting the "new norm" of Optimal/Expected needs for capital and expense budgets for perspective of the anticipated continual and future increase of BPA's overall capital portfolio found in Transmission and Facilities' SAMPs over the next few years.

OSCO's capital and expense program spending had been consistent with slight rises due to normal labor/material and inflation costs before COVID-19 pandemic, a natural pause in all capital spending due to COVID, yet O&M expense remained due to normal security needs, best practices, and Federal security compliances.

Since COVID-19 subsiding, trends-to-forecast has witnessed increased spending over the last year is related to inflation, volatile markets, imposed prices, and fluctuations in pricing for materials/components and labor costs to design/build security enhancements and measures to BPA's energized and non-energized environments. The supply chain for all commodities once thought to be readily available is currently volatile due to the post-pandemic atmosphere.

OSCO has a smaller capital and O&M program and budget than other BPA capital and O&M programs, serving a finite security need of replacement of NERC CIP 006 lifecycle management, the installation of NERC CIP 014 security enhancements, and the O&M for the electronic security systems; leading to all forecasted, sustain projects being completed as per Schedule & Scope to give a 100% success rate. As historically reported to BPA's Finance Management (for the last seven years) and asserted by OSCO's security capital sustain program that the security capital costs incurred to date have resulted in assets at the completion of the projects.

All reported work orders (past and present) are valid and represent a future benefit to BPA rate payers. There are no plans to cancel future additional security work partially or in its entirety. There is no known event (not even COVID-19 or wildfires) that prevented OSCO from canceling a project resulting in its capital budget to expense transfer during any financial reporting period. However, as stated within the OSCO SAMP, supply chain delays and resource constraints have caused delays in some projects but have always been completed and energized.

OSCO's five-year project/asset replacement execution is intended to outline the capital and expense investments required to work towards meeting the future performance standards defined in Section 10.1 in the OSCO SAMP. To do this, the projects in the future state will be prioritized in order of OSCO, Transmission and Facilities allocation terms of security, Security System Health and Criticality Matrix scoring, the asset criticality to BPA, bundled site-location, and the elevated risk of failure and degradation of the electronic security system at such respective site.

The need for security assets (e.g., electronic security systems, fences, barriers) at a particular site or facility are dependent on the criticality of the BPA asset being protected as well as site-specific vulnerabilities identified in security risk assessments. The Security Protection Level and their overall performance requirements are defined in the Critical Asset Security Plan and within the OSCO SAMP, Section 7.1.

The collaborative efforts of financial analysis of OSCO, Transmission Estimating, Transmission Project Management, and Software Development & Operations SMEs developing the best, real-world estimates possible for projects leading to "new norm" trends of pricing for future estimates. Other mitigation efforts must be managed at the CAO and Finance levels as increased funding requests come to them from the security capital and expense program managers; this is accomplished by formal IPR requests and financial change request forms through Tier II and III management to executive management approval. The increase capital and expense funding requests come through the SAMP and IPR process.

Strategic and asset planned challenges and mitigations may be referenced in various sections and sub-sections of this SAMP, such as:

- Section 5 External and Internal Influences, SWOT Analysis
- Section 6 Asset Management Capabilities and Systems
- Section 8.4 Asset Performance

- Section 10.4 Implementation Risks
- Section 10.6 Performance and Risk Impact

Trends can be addressed more tactically by referencing OSCO's past and present Asset Plans (Section 5 - Planned Capital and Maintenance Activities) for details of the five-year project/asset replacement execution strategies. This document expresses in detail:

- Managing execution, risks, and improvement strategies
- Cost trending patterns and estimated cost per project
- Site names, type of NERC CIP project to be completed
- Program/project timelines, milestones, and successes

8.3 Asset Condition and Trends

Section 10.5 below reflects Asset Conditions and Trends of security system assets as it pertains to 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 14 years old and in need of increased funding resources towards maintenance and replacement. OSCO's maintenance budget of over $700,000 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 indicates 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.

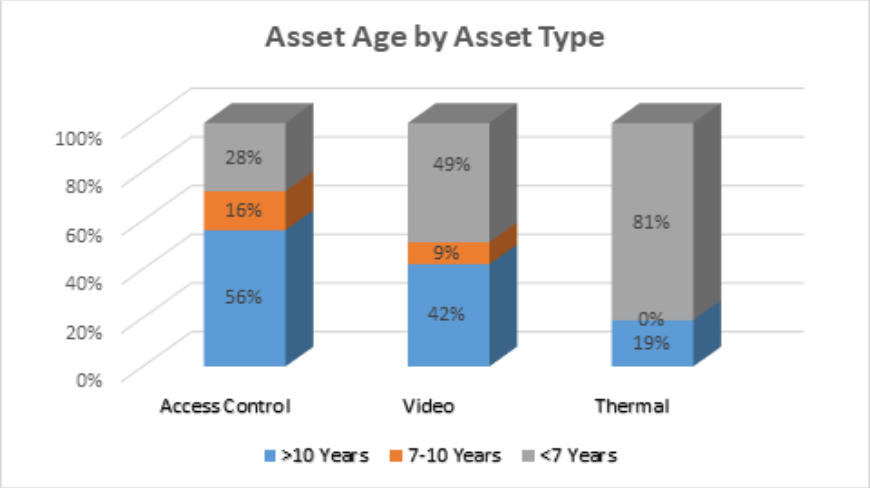
NERC CIP 014 Portfolio:

The age of OSCO's NERC CIP 014 portfolio is eight years old. Not enough data to create a long-term trend analysis has been collected regarding the security system asset condition. However, given the average lifespan of a security system is approximately five 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 8.3-1 represents the age of electronic security devices broken down by asset type. The data suggests that access control devices are quite dependable 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 8.3-1 shows that we do not have any thermal devices in the 7-10 years age range.

These devices were first introduced at substations in 2016 as 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 dependable and require little preventive maintenance, which reduces firm fixed costs. Note that these savings are offset as these are more expensive when compared to the 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 types of repairs having a greater impact on the O&M budget over time.

Figure 8.3-1, Current Asset Age by Asset Type



8.4 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 dependable, 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.

Reliability and 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. The full complement of the BPA's electronic security systems is beyond their life expectancy. However, systems and components are performing as expected, given weather conditions, electrical/magnetic frequency interferences, etc.

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. The full complement of the BPA's security systems is beyond their life expectancy. However, systems and components are performing 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 to include technology obsolescence

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:

- Financial (cost competitiveness): OSCO has not received an Asset Management period-year of tracking % SOY budgets forecasted vs spent by year metric of its Sustain and O&M program. However, all historical data on assets energized and cost is 100% as the OSCO program scope of work can be referenced in Section 3 Scope, Section 8 Historical Cost of this SAMP, and Section 5 Planned Capital and Maintenance Activities of the OSCO Asset Management Plan regarding all physical and electronic security systems projects.

  All OSCO capital project lifecycle information is tracked and can be found through Transmission's CIA process and project management SEIS which tracks all stage gates, lag time between stage gates, etc. All OSCO O&M expenses are tracked through Software Development & Operations SEIS and its O&M Work Priority Table, Table 8.1-2.
- Compliance: Compliance factors can be referenced in Section 4.2 Stakeholders and Expectations, Section 5 External and Internal Influences, Section 5.1 SWOT Analysis, Section 7.1 Criteria, and Section 10.6.5 Compliance Risk of this SAMP.
- 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 environmental conditions 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 Cad software, Video management system, 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 continues to align its replacement and maintenance work streams by utilizing the newly developed Security System Health and Criticality Matrix process/analytics to align the criticality of the site set by Transmission and Facilities; the health of the security asset at the site; and the security risk (break-in, theft, terrorism) to the site if the security assets are not maintained, Federal compliance, and best security practice values at all levels of the organization. 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 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 FY23 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 8.4-1. This data is not currently available and will be updated during the next schedule SAMP update.

Table 8.4-1 Historical Asset Performance Summary

Strategic Goal	Objective	Measure	Assets	2019	2020	2021	2022	2023
Modernize assets	Reliability: Security Compliance and Best Practices	Active up/down time of electronic security system	303	NA	NA	NA	NA	100%

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 utilizing structured electronic information systems (SEIS) software to determine electronic security system CHR and Transmission SEIS software to finalize all architectural aspects of physical and electronic security systems.

As such, 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.

8.5 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 a 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 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 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 are 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

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

**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, OHSA requirements, and building codes. As of this SAMP, heat maps have not changed in their scoring.

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 NERC CIP 006, CIP 014, and DOE PL-6 critical asset planning efforts and associated BPA standards remain the focus of BPA's approach. As we seek to address DOE IG Physical Security inspection recommendations, our goal will be to partner with Transmission to more thoroughly and collectively implement DOE Safeguards and Security requirements as a driver for our future state.

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

The need for security assets (e.g., electronic security systems, fences, barriers) at a particular site or facility are dependent on the criticality of the BPA asset being protected. The Security Protection Level and their overall performance requirements are defined in the Critical Asset Security Plan and within the OSCO SAMP, Section 7.1.

Given the recent DOE IG Physical Security inspection recommendations, BPA will need to address the adequate prioritization of capital security projects as they relate to PL-6 asset designation. Future state projects led by Transmission and Facilities will also need to account for asset criticality. Additionally, project factors need to consider site-location bundles based on geographic locations and elevated risk of failure or degradation of the electronic security system at a respective site.

To date and for future fiscal years, OSCO's and Software Development & Operations' future asset performance is dependent upon numerous 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
  - The CIO and Infrastructure Services are establishing stronger network bandwidth pathways to BPA regions lacking adequate BUD Network bandwidth for business operations and security information needs
- Future BPA capital facility expansion conducted by Transmission and Facilities
  - This should follow the Transmission and Facilities SAMP
  - Continued collaboration with Transmission and Facilities PgM and PMs regarding PHYSEC standards and requirements to fund/scope/design/build of electronic security systems for their respective expansion programs. Section 9 Project Appendices for full list of projects
- Current Transmission's Bulk Electric System (BES) substation modeling
  - This should follow the NERC and Transmission BES processes
  - Continued collaboration with Transmission Technology PgM and PMs regarding PHYSEC standards and requirements electronic security systems to support NERC compliance
- Expense (O&M) funding levels
  - Communication to the PfMT, Facilities, Finance, and Risk of the decisions to approve capital investments through the expense section of a business case, however the expense information does not flow to OSCO expense budget for maintenance. This does not ensure the necessary expense required to maintain the security assets in out-years, leaving OSCO and Software Development & Operations with insufficient funds to maintain the security system assets from investments.
- Technology changes to software and hardware associated electronic security systems and needs
  - This follows Software Development & Operations' protocols

Future Asset Performance Objectives, Table 10.1-1. Data on Future Asset Performance Objectives is not currently available. OSCO and Software Development & Operations has initiated the Security System Health and Criticality Matrix as of FY23 to measure electronic security asset performance and will include this information in future SAMPs. Currently there is 100% accountability of critical assets health and risk information in the Software Development & Operations SEIS that tracks all electronic physical access control, intrusion detection, and video assessment.

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	100%	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 systems, 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 remarkably similar, with some variations based on scale or complexity at each site.

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

In 2015, OSCO began a multi-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 added two additional sites per year to this program, focused on CIP 006 lifecycle replacement, 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. As we execute the program, it is especially important for us to effectively work with Transmission to prioritize security-related project work to protect BPA's critical asset sites.

Security system sustainment planning is driven by the larger asset planning of the Transmission and Facilities organizations and considers 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 adding security assets to protect critical asset sites based on security risk assessment recommendations, and asset health and risk of failure when we consider existing security assets. For lifecycle management, we seek to meet current standards, practices, and up-to-date hardware/software for 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 continue 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, reduce risk, and realize significant value for the security program. Often, OSCO must decide what work to postpone or cancel 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. The 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 several 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 expanded 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, NERC CIP 006 and 014, and BPA security standards. Although 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 will include cost projections to sustain local law enforcement contracts established by the Bureau of

Reclamation to ensure adequate and timely response to these facilities as BPA takes over ownership. It is our intent to provide transparency for all 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 are 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 lifecycle 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.

For any BPA organization building or modifying facilities, it is the responsibility of that organization, through established BPA standards and polices, to include planning and installation of physical and electronic security system assets as required. It is also their responsibility to include funding of 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 Business Resiliency

Technological Obsolescence

For OSCO, Software Development & Operations, Transmission, and the Facilities organization, a continuing challenge exists with managing technological change and replacing obsolete components/systems. As threat dynamics continuously evolve, we must consider modern technology solutions to help counter threats. In addition, changing Federal requirements and industry security best practices drive a need to continuously review ever-changing security system technology and engineering in several different disciplines: IT security software, electronic security system hardware, and advanced professional engineering standards.

Maintaining older security system technology is problematic and inefficient. An aging security system equipment results in an increase in breakage and system failures so a spare part inventory must be established and maintained. Maintaining a growing inventory of older technology will continue to drive an escalation of O&M costs.

As OSCO and Software Development & Operations continue to manage changes in technology, we seek to simplify security systems while also looking for improvements in efficiency and effectiveness. For example, new physical access controls and intrusion detection systems being designed and installed in BPA buildings

(new construction and lifecycle management) establish improved system performance through a consistent, simplified design with less components. The outcome is a more reliable system with reduced human performance errors, a reduction in nuisance alarms, less parts to maintain, and simpler O&M.

Resiliency

Infrastructure resiliency is defined by NERC/FERC (Docket AD18-7-000) as "… 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." OSCO electronic security systems and physical hardening projects (security fence/gate systems, security poles, and other associated infrastructure) contribute to BPA's resiliency efforts and the reliability of the grid. These projects provide BPA capabilities to deter, detect, delay, communicate and respond to a security event to eliminate or reduce grid reliability risks associated with such events.

In 2008 – 2009, OSCO began integrating NERC CIP 006 electronic security systems (ESS) into BPA critical asset sites. With an IT-designated life span of seven years, many security systems (either sub-system or as a whole) were projected to fail completely due to exceeding manufacturer stated Mean Time to Failure (MTTF). This issue would negatively affect compliance with NERC CIP standards and DOE O 470.3C, *Design Basis Threat*, as well as security system effectiveness, if replacement or repairs could not be affected in a timely manner. It would also result in tremendous maintenance cost increases and drain limited BPA and contracted resources. To manage this, OSCO launched a NERC CIP 006 "Refresh/Upgrade" capital program beginning in FY22 to remove obsolete, aging security systems and replace them with improved technology. The NERC CIP 006 capital program is an on-going/rolling program to ensure ESS continues to provide protection as designed, continue to meet regulatory compliance, and remain up-to-date and in-line with current security hardware and software needs.

OSCO's NERC CIP 014 capital program is still relatively young; however, NERC CIP 014 ESS technology must also be properly maintained through planned O&M activities to maximize its MTTF as well as evolve into a NERC CIP 014 "Refresh/Upgrade" program. As the NERC CIP 006 and 014 programs mature, a nexus and trend will occur at sites that have both programs integrated into the current O&M and "Refresh/Upgrade" cycle.

For this program to be successful, research and development (R&D) efforts must be included to support the evaluation and adoption of new security technologies. Currently, the R&D function is absorbed by the Software Development & Operations team, which includes an extremely limited number of security system technical experts to research innovative and cost-saving solutions to meet BPA's ever-changing threat climate and growing security compliance and best practices obligations. Currently, resources are not dedicated to R&D and conflicting priorities often take precedence. In addition, funding for R&D is not currently covered by OSCO's annual maintenance budget. To further program maturity and success, a robust R&D capability would allow the vetting of new security technologies to drive future system costs down, provide solutions that are more closely tailored to the needs of BPA, and ensure alignment for modern technology to be properly integrated and ran on BPA's network.

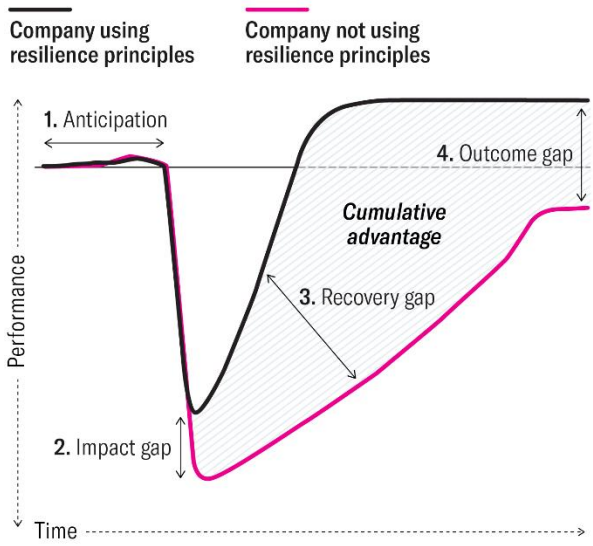
An example of positive R&D efforts includes a new security design that was developed and installed as a security system refresh proof of concept. This project was completed in March 2018 and data from before and

after the new system design showed a 100% reduction in site nuisance alarms and a 78% reduction in relay usage. The reduction in relay usage equates to a reduction in device failure and longer life expectancy. With this successful R&D effort and its continued success, all BPA energy and non-energy delivery facilities are scoped, designed, and built to this new ESS standard.

The resiliency of BPA 's electronic security and physical security assets are a key component of BPA's overall business resiliency strategies. Specifically, BPA maintains an overarching internal policy (260-2) that acts as a framework for resilience activities within all business units and related asset categories. This policy aims to achieve the following:

- A comprehensive and effective business resilience program to support the resilience efforts of internal organizations and ensure that BPA can fulfill its statutory and commercial obligations in times of emergency. This includes anticipating, withstanding, and responding to disruptive events affecting the Pacific Northwest.
- Alignment of risk management and asset management with resiliency goals.
- A consistent framework for prioritizing risk within asset categories, and documents prioritization decisions. Risks are analyzed based on category (safety, reliability, financial, environmental, & compliance), likelihood, and consequences.
- Planning efforts to detail disaster recovery, business continuity management, emergency management, grid and physical security, cyber security, insider threat, supply chain, workforce resilience, Power Services, transmission planning, and extreme weather.

It is the Bonneville Power Administration (BPA) policy to incorporate resilience concepts and activities into its business practices to enhance the BPA's capabilities to be prepared for, respond to, and recover from unexpected disruptions. Resilient agencies prepare for and connect the unrelated pieces of information in a way that makes the organization stronger and more resilient. Resiliency's purpose is to quickly bounce back from below the baseline to an operational reality higher than what it was at prior. This can be illustrated in the graphic to the right.



Currently OSCO's and Software Development & Operations' business continuity support for mission essential functions is for multiple continuity scenarios and has no specific elements related to changing environmental conditions. Given the supporting nature of these two organizations, applicable resiliency measures are currently being tracked through BPA's Business Resilience Program. OSCOs and Software Development & Operations will continue to work with the Business Resilience Program as needed. BPA anticipates and mitigates the risks that changing environmental conditions poses to its critical systems and asset portfolios throughout the entire lifecycle of an asset.

Resiliency is growing area within the utility space that requires dynamic business decision making, flexibility and adaptability. Today's technology is changing at a rapid pace. OSCO and BPA's internal organization stakeholders and partners consider technological changes and trends that influence how BPA makes business decisions in response to resiliency events.

In the increased, forward movement of security requirements for BPA, OSCO has sponsored, developed, and established security-centered maintenance and design standards. As well has influenced other Transmission and Facilities based standards and requirements regarding security system assets. This enables best practices and the ability to execute contracted work that necessitates quality control while maintaining reliability. OSCO, Transmission, Software Development & Operations, and Facilities has developed ongoing effort to improve data quality using historical projects to empower current and forecasted projects and achieve best security practices.

Resiliency principles

- **Redundancy –** These buffers systems against unexpected shocks, albeit at the expense of short-term efficiency. It can be created by duplicating elements (such as by having multiple spare parts or by having different elements that achieve the same end (functional redundancy).
- **Modularity** - This allows individual elements to fail without the entire system collapsing, albeit while forgoing the efficiency of a tightly integrated organizational design. Because a modular organization can be divided into smaller chunks with well-defined interfaces, it is also more understandable and can be rewired more rapidly during a crisis.
- **Adaptability** -The ability to evolve through trial and error. It requires a certain level of variance or diversity, obtained through natural or planned experimentation, in combination with an iterative selection mechanism to scale up the ideas that work best. Processes and structures in adaptive organizations are designed for flexibility and learning rather than stability and minimal variance.
- **Prudence**- Involves operating on the precautionary principle that if something could happen, it eventually will. This calls for developing contingency plans and stress tests for plausible risks with significant consequences, as well as financial prudence by removing debt from the financial portfolio.
- **Embeddedness** - The alignment of a company's goals and activities with those of broader systems. It is critical to long-term success because companies are embedded in supply chains, business ecosystems, economies, societies, and natural ecosystems. This helps to ensure that the company does not find itself in opposition to society and inviting resistance, restriction, and sanction.

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 NERC CIP 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.

The Optimal Expenditures of Table 10.3-1 indicate the budgets/funding needed to fully implement the SAMP, aligning the expense dollars needed to support the full capital programs of not just OSCO, but also Transmission and Facilities.

Table 10.3-1 Future Optimal Expenditures (in thousands)

NERC CIP 006 & 014 Security Enhancement Program	Rate Case FY's			Future Fiscal Years						
Capital Sustain	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
CIR/IPR Allocation	$18,000	$37,000	$38,000	$33,000	$38,000	$38,000	$20,000	$17,000	$23,000	$24,000
Expense (OpEx)										
Corporate Expense Budget	$1,727	$1,899	$2,089	$2,277	$2,482	$2,705	$2,948	$3,213	$3,502	$3,817
Expense Costs Associated with Grand Coulee Security Operations (*)	$1,086	$1,140	$1,197	$1,256	$1,318	$1,383	$1,452	$1,524	$1,600	$1,680
Total Expense	$2,813	$3,039	$3,286	$3,533	$3,800	$4,088	$4,400	$4,737	$5,102	$5,497

(This outlines the annual, optimal expense costs that BPA will need to pay to 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 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.)*

As FY24 commenced the DOE IG published a draft report, "Inspection of Bonneville Power Administration's Physical Program for Critical Assets." Although the inspection report is currently in draft, one recommendation was for BPA to ensure that BPA's construction scheduling prioritization aligns with the critical nature of its assets. In response to this recommendation, OSCO compressed our capital project schedule, which resulted in the Future Optimal Expenditures table above, to ensure critical asset sites are more urgently afforded the required protection for NERC CIP 014 and DOE Protection Level 6 (PL 6) assets. This revision also considers the limited capability of BPA capital project pipeline resources as well as the fact that there are other competing projects of importance to BPA lobbying for the same capital project pipeline resources.

Previously, OSCO's capital project schedule, which reflects estimated expenditures via the Future Expected Expenditures Table 10.3-2 below, was drafted to construct two new NERC CIP 014 security projects along with a lifecycle refresh of existing control house and relay house electronic security systems (ESS) each year. In addition, two non-NERC CIP 014 sites were included as lifecycle replacement capital projects for existing control house and relay house ESS. This created a long-term schedule of completing all NERC CIP 014 security projects in the year 2035. To compress the NERC CIP 014 security project timeline and better align with DOE IG's recommendation, OSCO has outlined the "Optimal" scenario above. This reflects a total of four (4) NERC CIP 014 security projects with ESS lifecycle replacements under construction each year, with all NERC CIP 014 projects to be completed in

2031. This change creates a project pipeline of twelve (12) projects being executed each year in a three-year cycle: Four sites in scoping, four sites in design, and four in construction.

Additionally, the numbers reflected in both tables include a dramatic increase associated with contractor material and labor inflation via capital bid processing for scope/design/build efforts. OSCO's capital needs for future fiscal years have dramatically changed due to national and regional inflation of labor and materials to near two times our previously forecasted outlook.

Forecasting O&M costs for security projects can be challenging. We must factor in new contract rate increases, parts inflation, and increased support of new/upgraded systems coming off warranty. Inflation is creating significant cost escalation for O&M activities, and the necessary increases are reflected in the above chart. inflation the O&M funding will need to be addressed and increased as stated.

OSCO develops business cases to annotate the out-year O&M needs for a project at the 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 numerous 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

Table 10.3-2 Future Expected Expenditures (in thousands)

NERC CIP 006 & 014 Security Enhancement Program	Rate Case FY's			Future Fiscal Years						
Capital Sustain	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
CIR/IPR Allocation (*Forecasted)	$16,000	$28,000	$29,000	$23,000	$30,000	$30,000	$29,000	$29,000	$20,000	$21,000
Expense (OpEx)										
Corporate Expense Budget (**Forecasted)	$1,500	$1,650	$1,815	$1,978	$2,156	$2,350	$2,562	$2,793	$3,044	$3,318
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
Total Expense	$2,586	$2,790	$3,012	$3,234	$3,474	$3,733	$4,014	$4,317	$4,644	$4,998

* Expected Expenditures are based on three NERC CIP 006 & 014 projects per year to finish the NERC CIP 014 program by FY33. Funding beyond FY33 is for NERC CIP 006 & 014 life cycle upgrades.

** FY24 IPR was $936k, Expected budget is $1,500k due to increases in material cost, number of sites, and the recompete of the current O&M security contract. Expected budget was increased though re-allocation of funds with no overall impact to IPR forecast. Optimal accounts for higher-than-expected recompete rates (based on contract rate increases from similar recompetes), as well as an increased number of un-forecasted system upgrades in recent years.

*** This outlines the annual, optimal and expected 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 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 of this SAMP. Security system assets and what they provide are the responsibility of BPA, 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.

The current "Expected" capital and expense funding is set by the previous IPR and forecasted estimates completed two years prior. However, inflation of labor and materials means that BPA estimates are significantly lower than expected "true" cost of a project no matter if capital or expense.

The risks of not receiving the optimal capital and expense funding include BPA failure to comply with US DOE and NERC orders, BPA security policies and standards, and a degraded security posture for its energized and non-energized facilities. BPA security requirements fall into the realms of a "must" and "shall" and cannot be deviated from.

OSCO's programmatic risks are weighed against the five primary enterprise level risks: safety, reliability, financial, environmental, and compliance to chart out the exposure level to the agency based on challenges across programs and is referenced in this SAMP in 10.6 Performance and Risk Impact and FY23 Asset Management Plan in Section 6.3 Execution Risks.

Mitigation efforts must be managed at the CAO and Finance levels as increased funding requests come to them from the security capital and expense program managers; this is accomplished by formal IPR requests and financial change request forms through Tier II and III management to executive management approval. The increase funding requests comes through the SAMP process as expense funding requests from the IPR.

Table 10.4-1, Implementation Risks

Risk	Impact	Mitigation Plan
BPA cultural resistance to security culture changes	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 resource "Pipeline" for project execution	May result in delayed and/or deferred projects, degrading security reliability, effectiveness, and compliance	Transmission and Facilities business partners prioritization of security projects. Make organizational changes and/or redeploy resources. In some cases, re-training employees may be 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
Delay in or lack of standardized	Challenges with consistent deliverables and slower execution during the	Using standardized estimating tools, create accurate estimates which incorporate owner project requirements and performance specs for the most frequent types of work

estimates for security systems	funding, scoping, design, and build process	
Accurate staffing forecast	Frequent changes to organizational staffing forecasts prevent a more strategic and cost minded approach to managing IT, project management and engineering disciplines	Develop flexible staffing strategies based on projected needs (emerging work) with alternate scenario contingencies. Continue working with CAO, CIO, 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 bandwidth 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:

Table 10.5-1, Trends and Primary Drivers

Time Frame	Objective	Trend	Primary Driver
1-2 years	Improve security system reliability and asset condition	Significant aging of security system assets	Aging/obsolete software and hardware technology. Increased breakage of electronic security system devices
3-5 years	Improve security system reliability and asset condition	Significant to Moderate aging of security system assets	Execution of system replacements provides some improvement. Completion of new projects/facilities (new devices added), as well as system replacements helps improve overall asset condition.
5-10 years	Improve security system reliability and asset condition	Increasing steady state, with some moderate deterioration remaining	Up-to-date technology helps improve a reliable steady state. Modern technology/system designs increase reliability and condition

Figure 10.5-1 Future Asset Age by Asset Type

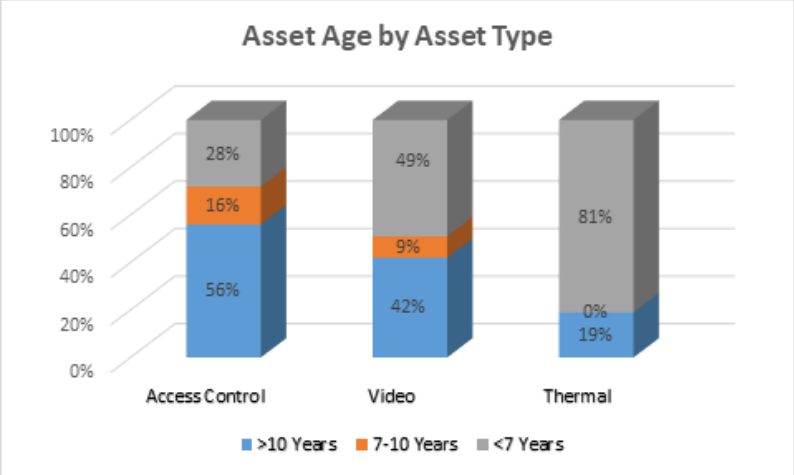


Figure 10.5-1 describes the age of security devices by asset type and does not take into consideration other infrastructure that may be used to support these systems. Examples would include the network and the fiber used to support our systems. The trends that we are seeing from a maintenance perspective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

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 the meantime 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 a slight increase in outdoor fiber failures over the past four years. OSCO is currently working with Transmission and IT engineering regarding outdoor fiber specifications for electronic security systems; however, these failures have a significant impact on the maintenance budget and can cause extended outages. These outages have a major influence 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 contractor
    - 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 highly 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 initiative-taking management of the security asset portfolio.

Table 10.6-0 Strategic Initiatives and Risks Addressed

Drivers	Initiatives	Risks of Foregoing Implementation
Security Enhancements (DOE/NERC CIP 006 & 014)	*NERC CIP 006 and 014 more intricately links security and compliance resulting in a single total* **Compliance (NERC CIP 006 & 014, DOE):** Ensure compliance with security regulations by applying mandatory security enhancements as required by NERC, DOE, DHS, and CASP, etc. **Critical Infrastructure Protection:** Installation of security systems designed to provide the appropriate level of protection for critical infrastructure designated PL 6 and PL 7	**Financial and Reputational Risk Due to Regulatory Non-Compliance:** Findings by regulatory entities within one year leading to; a) cost incurred due to physical security audit findings, b) mandated policy changes and, c) public criticism. **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: • 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 **This includes OSCO, Transmission, and Facilities capital projects currently scheduled**
Immediate Threat Mitigation	**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.	**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.

Preventative O&M Program	**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.	**Operational and Reputational Risk Due to Inadequate Maintenance:** Failing or faulty security systems and equipment leading to: • 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 BPA. Given the number of aged security assets on BPA's system, current OSCO strategy is focused on prioritizing maintenance, lifecycle replacement of NERC CIP 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 DHS ISC – 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 system needs 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 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	**Strategy:** • 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 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 modern 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 retrofit 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	**Strategy:** • Immediate: – 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: – 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 shift focuses 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	**Strategy:** • Immediate: – 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: – 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:** • 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 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 brief 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	Cost incurred due to physical security audits due to noncompliance with regulations, guidelines, and standards Negative public perception of BPA due to noncompliance
Owner/Control	OSCO, Software Development & Operations, Transmission, Facilities
Risk Mitigation	**Strategy:** • Immediate – 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 NERC CIP energized and non-energized facilities and the increasing age and number of security system deficiencies affecting BPA security assets, there are several 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 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	• Coordinate with main Stakeholders on planned investments	• Establish partnership agreements with main Stakeholders (Primary and Secondary Capacity Model options)
Unified O&M program	OSCO/ Software Development & Operations /Facilities	• Facilities implement IFM contract	• 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	• Implement alternative project delivery methods • Shift focus to Capital Renewal and Replacement	• 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	• Leverage vendor services • Contract SME support for IT and engineering disciplines	• Integrate Facilities planning, design, and execution into one group within Transmission • Software Development & Operations increased staffing levels (BFTE and/or CFTE) to manage increased demand.
Staff Training	OSCO/ Software Development & Operations /Facilities/Transmission	• Structure training program around strategic objectives	• 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 100kV, or higher and Real Power and Reactive Power resources connected at 100kV 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 group 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.
- **Federal Information Security Management Act (FISMA):** is United States legislation that defines a framework of guidelines and security standards to protect government information and operations.
- **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 the 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 the 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: Threat x Consequence x Vulnerability = 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 conditions 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 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 related to security and regulatory compliance.
- **Threat:** An adversary, undesired event (natural or man-made), person, group or organization that can accomplish 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 lines, and substations.