Bonneville Power Administration
FY2017 IT Asset Strategy

Office of the Chief Information Officer

1.0 Executive Summary

Information Technology Asset Management Strategy

1.1 Profile of Assets

The Information Technology Asset Strategy covers the technology assets hosted in the Bonneville User Domain (BUD)[1]. These assets comprise,

- 0.6% ($103 M) of the BPA's Plant In Service total capital assets ($17,236M)
- 3.0% ($32.8M) of the BPA's planned FY2016 capital spend ($1,067M)
- 2.6% ($87M) of the BPA's Departments planned FY2016 expense spend ($3,293M)

Information Technology BUD assets include: circuits, servers, storage devices, desktop systems, printers, copiers, faxes, phone systems, and software, including applications provided as Software as a Service (SaaS). The software systems covered by this strategy include critical business systems, general business systems, web applications, and task systems. Critical business systems must operate and be available around the clock (24x7)[2]. General business systems enable BPA to manage its staff, finances, facilities, supply chain, transmission assets, and services such as managing circuits and work planning. Task systems are small web based applications that enable BPA staff to more efficiently perform their work. A small sampling of task systems include: Absentee Tracking System, the Tribal Matrix website, and the NW Sub-basin Geographic Data browser. There are several hundred of these task systems.

The IT Asset Portfolio is divided into four major asset portfolios and the Project Work Plan which contains projects that create assets (software system, networks, datacenter, etc.) that are placed into production under one of the four asset portfolios. Each asset portfolio has its own asset plan. We use these asset plans to create our overall IT Asset Strategy.

The Office Automation, Network, and Datacenter Portfolios collectively form the information technology infrastructure that supports both users and systems. We will use infrastructure throughout this strategy to refer collectively to these three portfolios. Table 1 describes each of these asset portfolios.

Critical Assets

Critical IT assets are defined by the functions they support and/or have a 24x7 availability requirement to support critical services on an hourly basis. A critical system supports one or more of the following functions:

- *Real time or preschedule transmission or power scheduling*
- *Hydro operations*
- *Marketing (deal capture, day ahead trading)*
- *Short term forecasting, planning and loads*

There are 20 critical business systems in the Critical Business System sub-portfolio. There are 3 critical IT services in the Network portfolio which includes network, telephone, and DNS services. Email is the final critical service and is in the Datacenter portfolio.

[1] This strategy does not cover technology assets residing on the operational grid network. Grid network systems monitor and manage the status of the electric grid. These management systems include our SCADA (supervisory control and data acquisition) and AGC (Automatic Generation Control) systems.

[2] Criteria for Determining Critical Business System Designation; 5 April 2010, Official File – NJ-6 (IR-11-12). For a complete listing of the 20 critical business systems, see the IT Application Strategy, chapter 6, Applications Portfolio.

Asset Portfolio	Office Automation	Data Center	Network
Assets	Desktops, laptops, printers, software, peripherals to include IP addressable devices such as scanners, etc.	Servers (infrastructure servers, application servers, database, etc.) operating systems, database management systems, and management tools	Data, voice, and video networks. Includes cabling, switches, routers, firewalls, IDS, management software, and PBXs.
Asset Category Activities	○ Refresh of network printers and desktops/laptops ○ Upgrading workstation software ○ Adoption of new technologies ○ Bringing or maintaining systems in compliance with architectural standards and security controls	○ Refresh of servers and storage ○ Migrating to new server operating systems ○ Adopting new technologies (virtual storage, server virtualization, cloud services, etc.) ○ Enhancement of data center (improving bandwidth, improving backup and recovery, server consolidation, etc.) ○ Bringing or maintaining systems in compliance with architectural standards and security controls	○ Refresh of network infrastructure (routers, switches, hubs, firewalls, cabling, etc.) ○ Enhancement of network infrastructure (remote access, wireless access, etc.). ○ Adoption of new technologies (tele-presence, messaging convergence, IPV6, etc.) ○ Bringing or maintaining systems in compliance with architectural standards and security controls

Table 1.1: Infrastructure Portfolios

The fourth portfolio is the Application Portfolio which includes the sub-portfolios for Critical Business Systems and General Business Systems. The Application Portfolio covers:

- Proposals for delivering new functionality
- Upgrades and/or enhancements (typically expense)
- Software as a Service (SaaS)
- Applying system or security patches
- Implementing new features to meet business needs
- Correcting bugs or erroneous computing conditions
- Implementing annual changes such as tax code changes
- Retirement and/or disposition of systems
- Maintaining systems in compliance with the enterprise architecture and security controls

1.2 Objectives of this Strategy

There are two major outcomes to the strategy:

- Evolving the infrastructure to meet emerging security threats and providing reliable services while lowering operations and investment costs to enable those cost savings to be used to meet business needs.

Prioritization

New systems are added through projects. All projects are reviewed by the Agency Prioritization Steering Committee (APSC); projects with total investments under $3M are selected and prioritized by the APSC based on relative business value. Those projects with investments greater than $3M are forwarded to the Agency's capital prioritization process to compete for funding.

- Meeting strategic and emerging business needs by providing business solutions which deliver demonstrable positive net value and benefits to the Agency and the Northwest.

IT's goals align and support Bonneville's Key Strategic Initiatives (KSI). The IT Asset Strategy and associated IT Asset Plans directly support Bonneville's Asset Management Strategy KSI. IT's emphasis on tracking value and seeking operational efficiencies (responsible cost management) support the Long-Term Financial & Rates KSI. IT is actively engaging and working with business units to develop roadmaps to identify the future resources needed to meet business objectives. IT's involvement in developing the Business Information System roadmap is an example of planning to enable and support the Reliable, Efficient & Flexible Operations KSI. Chapter 2 in the IT Asset Strategy contains a more robust list of objectives and a discussion of IT goals.

To support reliability, infrastructure assets are refreshed based on a combination of industry best practices and BPA's desire to optimize value in its investment. As a rule, BPA maintains hardware one to two years beyond industry best practices. Although this approach does increase the risk of equipment failure in the latter year of operations, historically this has not had an adverse impact on BPA's environment. Discussion of sustain refresh rates can be found in Chapter 2 of the IT Assess Strategy and is summarized in Appendix C, Table C.1, which shows these refresh rates.

There is not a standardized refresh schedule for IT application systems. We maintain IT applications while the systems continue to meet business needs and remain cost effective. Maturing our ability to measure the business value provide by each application/system is a cornerstone of this approach. Upgrades and replacements are considered discretionary and must be programmed through an Asset Plan and prioritized through the APSC and the Agency process if the investment is greater than $3M.

1.3 Strategic Challenges

IT at BPA faces a number of challenges, which can be grouped into the following bins: Compliance, IT Challenges, and Strategic Partnership:

Compliance

- Increasing NERC-CIP Regulation
- Rising bar for Security
  - Evolving threats
  - Cyber Security Operation Center
  - Cyber Analysis capabilities
  - Refactor/replace legacy system to address security vulnerabilities (OMB)
- Federal Guidance
  - Implementing ICAM/HSPD-12
  - Implementing IPv6
  - Transitioning to Trusted Internet Connections (TIC)
  - OMB cloud first guidance
- COOP and Disaster Recovery

IT Challenges

- Rate of change in IT
- Rise of cloud based solutions and impact on Capital vs. Expense funding
- Consumerization of IT (managing smart phones, tablets, and other consumer products)
- Completing for capital and expense for projects >$3M
- Managing expense commitments for project execution, enhancements, and covering net new O&M costs
- 25% of IT workforce projected to retire by 2022 and 50% by 2028

Strategic Partnership

- Aligning IT and business objectives through asset plans (identifying out-year new projects and investments)
- Developing strategies to address aging applications/business systems – Examples: Creating Enterprise and Geospatial multiyear roadmaps
- Prioritizing development and deployment of new assets (business solutions) based on net value
- Establishing business boards to prioritize workloads based on business needs
- Project approvals contingent on the availability of expense funds to maintain
- Identifying and Tracking business value

We discuss these challenges in detail in the overview and the chapters covering each asset category. However, it is important to note that SaaS and other cloud based solutions will prove to be challenges in out-year budgeting for capital and expense. See the Uncertainty in Capital versus Expense side bar.

Our approach to OMB Cloud Guidance is to adopt cloud solutions when the solution yields cost neutral to lower total cost of ownership. We have identified some use cases where cloud solutions meet these conditions, these include: disaster recovery, development areas, and data analytics. We expect other use cases as cloud solutions mature. In this vein, we are encountering a number of situations where the vendor only offers Software as a Service (SaaS). We currently have about a score of SaaS solutions.

Uncertainty in Capital versus Expense

We programmed capital for out-year projects – we do not typically know if a cloud based solution is viable in advance of analysis of alternatives. Cloud based solutions cannot be capitalized (no tangible BPA owned asset) and instead need expense funding. This uncertainty in type of funding introduces uncertainty in the capital and expense requirements in a given year. This uncertainty is not in the total programmed spend, combined yearly capital and expense, rather in whether we have over or under programmed for capital or conversely expense. We will need to identify strategies that will allow us to handle these variations in capital versus expense requirements.

In the past IT had deferred infrastructure projects in order to meet business needs and this resulted in an aging infrastructure. With the completion of the desktop and datacenter modernization projects, most of the IT infrastructure is now back on a standard refresh schedule. The exception is the network. Our capital program includes projects to both upgrade our network and implement IPv6 as mandated by OMB.

Improving our security posture continues to be a major component of our program. This is especially true in light of the 2015 Office of Personnel Management data breach. Our program includes implementing mandatory use of Personal Identity Verification cards, enhancing configuration management (an example is the roll out of Tripwire as part of the datacenter modernization project) and ensuring our software solutions are secure. This may include refactoring code to meeting higher security standards/controls – standards and controls have evolved over the years as security threats have evolved and increased. Some systems cannot be refactored to correct deficiencies and others may need to be replaced.

Managing retirements in the upcoming years will present a challenge as 25% of the IT workforce is projected to retire by 2023 and will continue to increase to 50% by 2028. IT will need to develop mechanisms to onboard new employees in a manner to minimize disruption to services and ensure a transfer of knowledge.

1.4 Major Elements of the Strategy

We are shifting the emphasis of our asset strategy from being heavily tilted toward achieving cost efficiencies to the combination of becoming a more effective strategic business partner and leveraging technology to achieve both business needs and cost efficiencies.

Each IT Asset Portfolio category has its own unique challenges, risks, constraints, and need for methodological improvements. We discuss these issues in detail in the chapters covering each portfolio.

Critical assets must meet Continuous Operations (COOP) requirements. Our non-critical business assets also have 'return to operation' requirements after a major event, commonly referred to as Disaster Recovery (DR), which range from hours to up to a month. Each of the four major asset portfolios contains availability improvement initiatives that are being woven into a combined strategy to achieve and meet both COOP and DR business requirements. Our System Life Cycle (SLC) will require new projects to identify and address COOP and/or DR requirements to ensure we are delivering assets that meet business availability and recovery requirements.

In addition to aiding in the control of Office Automation costs, we will be able to leverage myPC to expand our telework capabilities[3]. Our myPC environment will enable staff to use their own computers and mobile devices to access network resources remotely.

[3] myPC can also be leveraged to ensure desktop services and access to network resources during COOP or disaster recovery events.

We have begun to strengthen the partnership between business lines and IT to help develop longer-term strategies and roadmaps for our business systems. The Business Enterprise Services Strategy team is developing a strategy and roadmap for our major Human Capital, Finance, Contracts, Billing, Transmission Asset Maintenance, Project Planning, and Supply Chain systems (see chapter on Application Portfolio for details). The roadmap is expected to be completed in FY2016 and will address when to replace or refresh major systems. For example, the roadmap will address when to replace our billing system (scheduled to be out of vendor support in FY2020) and future direction for our ERP (Enterprise Resource Planning) system which is approaching 15 years in service.

1.5 Results to be achieved

Table 2 highlights major initiatives we are planning over the upcoming years and will be updated as we complete our business strategies such as the Business Enterprise Systems and the Geospatial Strategy. The infrastructure initiatives are fairly well known due to a well-defined refresh rate. However, there are unknowns associated with the infrastructure portfolio. For more details on anticipated results and uncertainties, see each of the asset portfolio chapters in the IT Asset Strategy.

The major unknown in the Infrastructure Portfolio is the degree and speed with which cloud based solutions can be adopted for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Adoption of IaaS and PaaS can help IT avoid making future major capital investments in on-premise data centers while providing geospatial failover for disaster recovery and continuous operations. If IaaS/PaaS cannot be leveraged, IT will need to coordinate with Facilities to program for existing datacenters to be reconditioned (approximately in 2020) and to be expanded for DR.

OMB Cloud First

Bonneville Power Administration is a federal entity with OMB direction to consider cloud based solutions which include systems available through FedRAMP. Leveraging FedRAMP, particularly for IaaS and PaaS, provides Bonneville with third party evidence that a vendor meets FISMA moderate security control requirements.

Portfolio	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Datacenter	DMZ Virtualization	Refresh CBS Servers & Storage	Refresh IVC Blades Servers	Backup Service Refresh			Refresh CBS Servers & Storage		Backup Service Refresh			Refresh CBS Servers & Storage	
	Move email to cloud	Move VDI DR to Cloud											
	Leverage Cloud for General Business System Disaster Recovery			Decision on Leveraging Cloud for Critical Business Systems Disaster Recovery and enable Disaster Recovery capabilities									
	Enable Cloud based Analytics	Move VDI DR to Cloud		Complete move of External Web to Cloud									
	Move home Drives to cloud	Refresh General Business Datacenter			Decision on moving IVC (General Business Systems) to		Plan move to Cloud	Move General Business Systems to Cloud		Scale down/retire IVC			
	Move Test & Development to Cloud	Adopt Application Performance Monitoring											
	Windows 2012 & 2016 Primary OPS	Retire all Windows 2008	Windows 2016 & 2018 Primary		Retire Windows 2012 OPS		Retire Windows 2016 OPS		Retire Windows		Retire Windows 2020 OPS		Retire Windows 202
Network		Field Network Device Refresh				Core Network Refresh			Field Network Device Refresh				Refresh Fiber & Cable Plant
	Adopt TIC		Refresh VoIP	Transition to IPv6 (internal						Refresh VoIP			
	Refresh Firewalls	Refresh IDS		Refresh Firewalls	Refresh IDS		Refresh Firewalls	Refresh IDS		Refresh Firewalls	Refresh IDS		Refresh Firewalls
Office Automation	Refresh Desktops & Laptops	Refresh Desktops & Laptops	Upgrade Desktop OPS	Refresh Thin Clients	Refresh Desktops & Laptops	Refresh Desktops & Laptops	Upgrade Desktop OPS	Refresh Desktops & Laptops	Refresh Desktops & Laptops	Refresh Desktops & Laptops	Refresh Thin Clients	Upgrade Desktop OPS	Refresh Desktops & Laptops
	Implement Role Based Provisioning												
	Thin Client Penetration 40%		Thin Client Penetration 50%		Negotiate New Enterprise License					Negotiate New Enterprise License			
	Implement Portable Persona		Plan for 3D Printing	Implement 3D printing									
	20% software titles available through self service		40% software titles available through self service		75% software titles available through self service								
Applications	Ops Log Replacement	Cascade Upgrade/Replacement		Columbia Vista Upgrade	Pisces Upgrade	Billing Upgrade	Cascade Upgrade		Columbia Vista	Pisces	Billing	Cascade	
	CAISO Replacement	Stream System Improvement				CAISO Upgrade	Stream System				CAISO		Stream System
	EE Lighting Calculator	NERC CIP 5 Access Control		TAS Line Upgrad	Treaty Non Treaty Upgrade	EE Lighting	Netcracker Upgrade		TAS Line	Treaty Upgrade	EE Lighting	TCIS Netcracker	
	2020 BPA Solar Power Forecasting			Fleet Upgrade	Vegetation Upgrade			Solar Power Upgrade	Fleet	Vegetation Management			Solar Power
	Structured Data Management (SDM)						Upgrade SDM					SDM	
	Safety &Health Analyti	Demand Response (post demo)				Safety & Health		Demand Response			Safety & Health		Demand Response
	ATC Optimization - Scenario & Analytics							ATC Opt					ATC Opt
	IT Service Management		TAPM Replacement						TAPM				
	Facilities CMMS	CBS Data Re-architecting				CMMS Upgrade					CMMS		
	TCIS Netcracker Upgrade		Customer Portal						Custom Portal				
	AMS Replacement						AMS Upgrade					AMS	
	Complete Business Information System Strategy					Business Information System (BIS) Upgrades						BIS Upgrades	
	Data Management (Structure & Unstructured)			Enable Disaster Recovery capabilities for General Business System				Data Management Upgrade					
	Adopt Maturity Model		Advance Level in Maturity Model	Advance Level in Maturity Model									
	CSC2: Inventory of Authorized & Unauthorized Software												
	Power Reporting Analytics		V System Replacements or Upgra				Power Reporting					Power Reporting	
	Market Evolution Work		Energy Efficiency (Post 2028 Discussion)				Market Evolution	Energy Efficiency				Market Evolutio	Energy Efficiency
	Endur Replacement	PNNL Situational Awareness						Situational Awareness					Situational Awareness

Legend: **Efficiencies** **End of Life/ Replacement** **Upgrade** **Expand**

Table 1.2: Identified Investments

1.6 Spending levels

Table 3 provides our projection for our expense and capital spend profile. Projects with a total cost greater than $3M must go through the Agency prioritization process and be "green-lit" – competing with other non IT projects based on the projects' net economic value to the Agency. This introduces some uncertainty in the IT spend profile, since IT may not know if a given project will be "green-lit" in the proposed year, deferred, or dropped. Due to this uncertainty, Table 3 has two summary lines. The first summary line is the Total Target Spend, which includes all the sustain, compliance, policy commit, and expand projects that are within IT's authority to approve through the Agency Prioritization Steering Committee along with the projects that have already been 'green-lit'. The second summary line includes the capital and associated expense of the projects that must be 'green-lit' through the Asset Management Council's Agency Prioritization process.

Spend Profile(20 April 2016) ($M)	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Total Expense	$79.0	$85.3	**$83.8**	**$95.0**	**$97.1**	**$98.4**	**$100.5**	**$101.1**	**$101.8**	**$102.5**	**$104.5**	**$105.2**	**$106.4**	**$107.6**	**$108.9**	**$110.1**	**$117.52**
Operational Expense			$78.8	$90.0	**$92.1**	**$96.8**	$98.9	$99.5	$100.2	$100.8	$101.5	$102.2	$103.4	$104.6	$105.9	$107.1	$108.32
Expense to Execute on Capital			$5.0	$5.0	**$5.0**	**$1.6**	$1.6	$1.6	$1.6	$1.6	$3.0	$3.0	$3.0	$3.0	$3.0	$3.0	$9.2
Total Capital	$43.0	$31.2	**$35.8**	**$25.0**	**$25.0**	**$25.0**	**$8.1**	**$8.1**	**$8.1**	**$8.1**	**$8.1**	**$15.0**	**$15.0**	**$15.0**	**$15.0**	**$15.0**	**$ 15.0**
Total(Capital + Expense) Spend Profile	$122.0	$116.5	$119.6	$120.0	**$122.1**	**$123.4**	$108.6	$109.2	$109.9	$110.6	$112.6	$120.2	$121.4	$122.6	$123.9	$125.1	$ 132.5

Table 1.3: 2016 Planning Cycle (CIR/IPR 2016) IT Asset Capital and Expense Projections ($M)

We are also anticipating more cloud based solutions in the out-years which will require expense instead of capital funding. We do not know at this time the degree to which we may adopt cloud based services. This lack of knowledge introduces uncertainty in the amount of capital versus expense we will need in a given year; however, this uncertainty should not significantly impact the total expected spend.

Given the rapid rate of change in IT, coupled with emerging business and compliance requirements, there is uncertainty associated with the proposed funding profile. Table 4 includes a list of drivers that are introducing uncertainties into the IT funding profile. These uncertainties are discussed in detail in the Overview chapter and each of the asset portfolio chapters.

	Impact	
Uncertainty Driver	**Expense**	**Capital**

Adoption of larger number of cloud-based solutions than planned will require increase in expense requirements and corresponding reduction in capital requirements.	**Increases**	**Decreases**
Unplanned regulatory compliance due to emerging security threats.	**Increases**	**Increases**
Larger than anticipated capital program (more projects >$3M) requires expenses to execute projects (funds for SME resources to plan capital projects – without planning, capital cannot be executed) and support Net New O & M.	**Increases**	**Increases**
Unlikely to see any substantial infrastructure savings to offset net new O&M (current goal is to constrain growth to rate of inflation or below).	**Increases**	**Neutral**
Unplanned emerging business need resulting in unscheduled projects.	**Increases**	**Increases**
Managing retirements may drive costs up to allow overlap for knowledge transfer and mentoring before staffing level cost through hiring in at lower grades (current IT workforce is at high grade).	**Increases**	**Neutral**
FITARA requires all IT acquisition to occur under the CIO. As IT acquisitions that have been occurring in other organizations (often referred to as shadow IT) are identified and moved under the CIO, the IT budget will increase.	**Increases**	**Neutral**
Budget constraints may push out developing and/or implementing strategy roadmap resulting in the delay of projects which shift spending to the out years.	**Defers**	**Defers**
Upon completion of strategies (Business and Geospatial strategies) we may find that we have underestimated the cost of projects to implement on strategy roadmap.	**Increases**	**Increases**

Table 1.4: Expense and Capital Uncertainty Drivers

We are now, and will continue, working to keep IT annual increases to less than 2% (impact of net new operation costs from delivering new business system) above inflation.

Our mission is to serve BPA by providing timely and cost-efficient automation solutions, meeting the needs of the Agency.

2.0 Information Technology Overview

This chapter presents a collective overview of the overall state of information technology assets, providing the organizational goals for these assets, funding levels to meet performance objectives, a high-level assessment of the status of these assets, and the high-level risks confronting these assets and our asset strategy. Subsequent chapters will cover each asset category in detail.

The F2016 IT Asset Strategy continues to build on direction laid out in the FY2014 Strategy. The major elements include:

- Strengthening alignment between automation investments and Agency strategic initiatives
- Reducing infrastructure costs through technology and adopting maturity models
- The trend of increased need for expense and reduced need for capital
  - Anticipation of increased number of systems that will need major upgrades, requiring expense funding instead of capital
  - Anticipation that more solutions will use cloud based services (aligned with OMB's cloud first guidance)
    - Introduces uncertainty in capital and expense spending levels due to needing expense funds to implement cloud based solutions instead of capital funds
    - Move to cloud should not increase total spend (capital and expense); however, it will change the type of funding dynamically and IT may not have time to program the required expense levels needed to support its investment portfolio
- Increasing emphasis on a proposed investment's business value, to include:
  - Tracking the business value after the asset is delivered in to production
  - Using the trend in business value and amount spent on enhancements as one indicator on the health of an asset

The goal of the Agency's Asset Strategy is to maximize the long-term operational and economic value of our assets. This goal is accomplished by ensuring assets operate efficiently and effectively and provide the capacity and capabilities needed to meet health and safety, reliability, availability, adequacy, environmental, security and other standards, striving to minimize total economic costs over the long-term. The Information Technology Asset Strategy has developed four goals covering IT assets that align with the Agency asset strategy and span the four IT asset portfolios.

Business Value

New IT systems generate business value realized by the Agency and individual business units while IT incurs new support costs. In other words, new systems create a net new upward pressure on the IT expense budget.

2.1 Information Technology Asset Goals

1. Enable BPA to reliably and securely, in accordance with Federal and industry regulations and laws, use IT resources to effectively and efficiently perform work while maximizing utilization of IT resources. (ITAG 1)
2. Optimize total cost of ownership by ensuring the total lifetime benefits an asset delivers equal or exceed costs of investment and operations: planning new investments for upgrades and/or replacements when annual operational cost approaches or exceeds annual benefits. (ITAG 2)

3. Prioritize investments using net economic benefits to the Agency and strategic fit; delivering assets that meet the business unit's immediate requirements and are flexible and extensible to be leveraged to meet future strategic business objectives, resulting in reduced future delivery times and least total cost of ownership. (ITAG 3)
4. Institutionalize Operational Excellence through the adoption of maturity models to drive continuous improvement processes, practices, and service delivery to maximize the value of our IT assets and to reduce the cost of operations and maintenance. (ITAG 4)

These goals are mapped in each of the IT sub-portfolio category chapters, to the sub-portfolio strategies.

2.2 Performance Objectives

We are transitioning from being primarily focused on achieving cost efficiencies in our IT services (reducing and controlling costs) to a dual strategy that leverages technology to continue to achieve efficiencies (both in IT services and business services) while becoming a stronger strategic partner in identifying and delivering the right assets (solutions) that enable BPA to achieve its business objectives. We will discuss both aspects of this strategy in detail, beginning with cost efficiencies.

Our past intense focus on cost efficiencies has severely limited exploring new technologies outside of specific capital projects and delayed the implementation of many general service innovations – innovations that span more than one business unit. In other words, we have been experiencing a competition between cost efficiency and innovation with cost efficiency being favored over innovation. However, in the recent years, IT has begun to transition from its intense focus on cost efficiencies to a combination of leveraging innovation to transform BPA and using innovation to continue to achieve efficiencies.

2.2.1 Expense Performance

In FY2005 BPA centralized information technology functions and services from multiple units across the enterprise with the mandate to reduce and contain the cost of information technology through improved and efficient management of information technology assets. The overarching strategy has been to drive costs out of infrastructure operations through a combination of:

- Reducing cost and complexity through standardization,
- Adopting new refresh strategies,
- Increasing automation of information technology tasks, and
- Continuous process improvement.

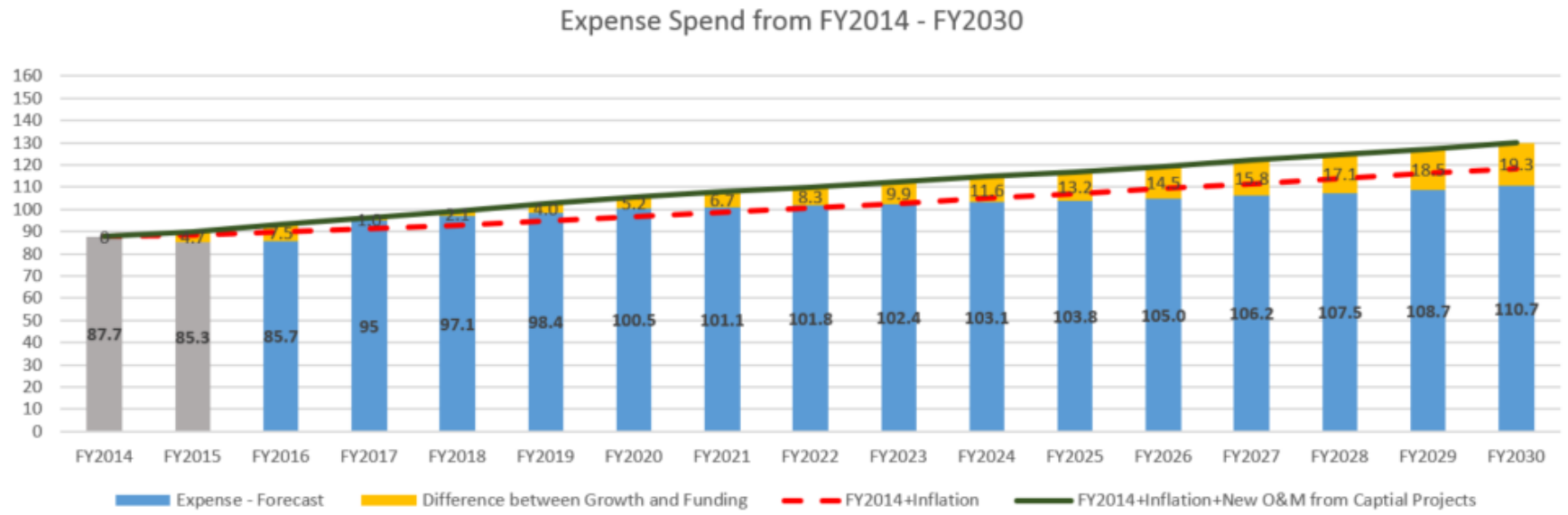


Figure 2.1: Information Technology Expense Profile

We have already begun to leverage innovation through our infrastructure capital projects to help deliver future cost efficiencies.

- Virtual Desktop Infrastructure
- Virtual and consolidated datacenter
- Virtual Storage Area Networks (vSAN)
- Managed print services

We are also exploring Infrastructure as a Service (IaaS) as a cost effective alternative for disaster recovery which could be an effective alternative to a capital intensive investment in brick and mortar disaster recovery.

Not all of these top IT projects will result in cost efficiencies. The top project, improve security, represents some net new cost to the IT operations budget. One of the major initiatives IT began in FY2014 was standing up and operating a 24x7 Cyber Security Operation and Analysis Center (CSOAC), which is placing an upward pressure on the IT operations budget from new staffing requirements.

Returning to Figure 2.1, there is a large increase in expense funding from FY2014 to FY2015. Drivers for this increase include:

- Programmed operations & maintenance costs resulting from moving 23 new systems into production in FY2014 (our current capital spend of $30M a year since FY2013 results in net new operations and maintenance costs of $1.9M)

- Changes in network circuits to provide additional bandwidth and network resilience, and to align with DOE guidance to conform with Trusted Internet Connection policy
- Cabling to phase out aging CAT 3 cabling and move to CAT 6a cabling to support VoIP and Power over Ethernet (POE)
- Adopting tablets
- Upgrading firewalls - expected to now require expense due to lower server costs; however, programmed capital in FY2012
- Refreshing BPA's internet site (external facing DMZ) – expected to now require expense due to lower server costs; however, programmed capital in FY2012

Although there is uncertainty in the rate at which cloud based solutions will be adopted, which creates uncertainty in the type of funding needed to execute on projects, expense versus capital, the combined expense and capital is expected to remain approximately the same with either a rapid or moderate adoption of cloud based services. Given our current expected work plan of $40M a year, we expect net new operations costs of $1.9M through at least FY2024. As efforts to develop and mature business roadmaps continue, new initiatives may be identified that require a realignment or adjustment of future resource profiles.

Tracking Business Value

We have been maturing our business cases over the last several years to improve identification of the business benefits. Until FY2013 we had not implemented a formal process requiring the business units to track and measure the business value over time. We are now requiring projects to not only identify business benefits, we are also requiring a formal Post Implementation Audit Plan be put in place and signed off by both the business owner and the IT Asset Manager. The audit plan documents the metrics the business will put in place to measure the business benefits from the new system. The business owner will present a report on the business value to the APSC 6-12 months after the system goes live. The IT Asset Manager will review business value metrics on an annual basis. We are institutionalizing these practices through the SLC.

3.0 Office Automation Portfolio

Assets in the Office Automation Portfolio are organized into three major categories:

- Hardware: the physical IT devices provided to staff to enable them to accomplish their missions.
    - Fixed computing devices (traditional desktop PCs and thin clients)
    - Mobile computing devices (e.g. laptops, smart phones, tablets)
    - Imaging devices (e.g. network or personal printers, copiers)
    - Multimedia/presentation devices (e.g. projectors, conference room flat screens)
    - Specialized devices (e.g. ergo keyboards, scanners, cameras, track balls)
- Software: the desktop software titles provided to employees to help them accomplish their missions. There are currently over 3,500 titles on the approved software list.
- Tools: the management software and expertise used by the support staff to manage the Office Automation assets and service delivery.

These assets touch almost everyone in BPA by providing a personal computing environment, mobile devices, print capabilities, and desktop software.

3.1 Goals, Objectives and Strategies

The over-arching goal is to provide cost effective and reliable desktop services to enable BPA to perform its mission and achieve its business objectives. There are multiple strategies and combinations of strategies available to IT to achieve a balance between improving services, cost effective delivery of services, the delivery of new and/or evolving reliable desktop services, and the ability to provide continuous operations in the face of natural or man-made disasters. These strategies and the objectives they support are listed in tables 3.1 and 3.2. They all point to the need for IT to continue to build on standardization and to move to leveraging automation and maturing processes in order to continue to evolve to a more agile and cost effective Office Automation environment. As is discussed in section 3.2 Asset Current State and Accomplishments, the evolution in standardization needs to go beyond hardware and encompass role based provisioning processes. It must provide a broader set of standard personal computing device form factors from which business clients may choose, based upon their business role. Many business clients will need additional mobility options, and younger staff members will be accustomed to and expect greater variety in meeting their business needs. IT will need to meet these expectations and needs in a cost effective manner and a combination of role based provisioning and self-service will help IT achieve both.

Office Automation strives to balance end user freedom with IT control to achieve efficiencies, reliability, and security objectives.

Objective/ Alignment with IT Goals	Outcomes	Status and Comments	Supporting Strategy	Measures
Leverage technology to achieve business objectives and meet business clients' needs. **Aligns with:** ITAG 1 – P[4]	• Self-service is enabled to allow users self-provisioning of selected software titles. • Single Sign-On is leveraged wherever possible to increase security and convenience. • Leverage virtual desktop infrastructure to enable business clients to use the personal computing form factor of their choice, to enable Bring Your Own Device (BYOD), and to improve delivery time of lifecycle refreshes. • Adopt cloud based email, file storage, SharePoint, and Skype for Business to improve business access to services.	Sequencing applications to enable streaming to desktop – large inventory of titles to work through. Leverage disaster recovery for virtual desktop infrastructure (VDI) to support telework. May need to introduce flash memory to meet user performance expectations and multiple image pools to mitigate sequencing issues.	• Role Based Provisioning • Virtual Desktop Infrastructure • Self Service • Automation • Cloud Services • Application Self Service	• 10% of approved desktop software is available through a self-service portal by EOY2018, 25% by EOY2019 • Enable BYOD by EOY2017 • 15% of desktop titles are packaged and delivered via application streaming by EOY2017; 25% by EOY2018 • Single Sign-On is implemented by EOY2018
Services are delivered and asset components are maintained in compliance with Federal laws and regulations. **Aligns with:** ITAG 1 – P ITAG 3 – S	• Automated tools are used to track and confirm compliance between deployed software and software licenses. • Implement tools to validate personal computing devices are delivered and maintained in documented and approved configuration. • Enable two factor authentication through the use of HPSD-12 mandated Personal Identity Verification (PIV) card for logical access to computing resources in support of OMB Identity, Credentials, and Access Management (ICAM) program. • Personal computing devices are patched in accordance with policy and BITA standards.	USGCB compliance is built in to Windows 7 desktop images and Active Directory group policies. Asset management components of SCCM, SCCM Expert, and process engineering are taking place to assure compliance with software licensing. Ability to use PIV/Smart Card/ICAM – 2 factor authentication is evolving.	• Virtual Desktop Infrastructure • Improved Remote Access • Automation • License Tracking	• All network users use PIV Cards for logical network access by EOY2016. • Scanning tools verify and validate personal computing resources comply with approved baselines. • 100% of desktop software licenses are tracked and validated to be in compliance by EOY2017. • 100% of desktop security patches occur within BITA timelines.
Processes and practices are aligned with industry practices to deliver secure,	• Desktop hardware and software refreshes are sufficient to meet reliability and security objectives while optimizing the total cost of ownership. • Increase use of virtual desktop infrastructure to reduce the cost of personal computing devices and client support.	Have moved from basic to standard for four key capabilities: Change & Configuration Management, Incident Management, Problem Management, and System Monitoring. Completion of the	• Standardized Refresh Rate • Device Ratio • Automation • License Tracking	• 40% of clients are using virtual desktops for the majority of their network access by EOY 2018; 50% by EOY2019 • Efficiencies from virtual desktop infrastructure and

[4] Each objective relates to a single primary goal indicated by "P"; objectives may also relate to secondary goal(s), indicated by "S".

Objective/ Alignment with IT Goals	Outcomes	Status and Comments	Supporting Strategy	Measures
reliable services with the least total cost of ownership. **Aligns with:** ITAG 4 – P ITAG 2 – S ITAG 3 – S	• Explore and leverage RFID, as appropriate, to enable cost effective tracking and inventory management of office automation hardware assets. • Software usage is tracked to reclaim unused/underutilized titles and make them available to other end users, as well as to enable reduction of titles due to low utilization or redundant function. • Advance along maturity model for desktop services. • Adopt hardware and software provisioning techniques, to include authorization, based on standardized business roles (Role Based Provisioning).	transition from the standard to the rationalized level has been targeted for FY2017. Have implemented remote assistance to improve first call resolution. Established and maintaining a knowledge library to reduce problem resolution time.	• Process Maturity • Managed Print Services • Application Self Service	reclaiming software titles enable operations and maintenances costs to be controlled below EOY2016 expense budget plus inflation through FY2020 • Advance along maturity model for key processes Change & Configuration Management, Incident Management, Problem Management, and System Monitoring. Achieve Level 2 by EOY2018, Level 3 by EOY2020. • Reduce personal computing device ratio to 1.1 by EOY2019

Table 3.1: Office Automation Portfolio Objectives

Portfolio Strategy	Benefits	Challenges/Issues	Asset Portfolio Outlook
Role Based Provisioning: Evolve Standardization to provide standard hardware, software, and authorization based on standardized business roles.	• Provides devices and software that meet business requirements. • Assists in identifying mobility requirements. • Assists in software rationalization. • Aids in controlling costs. • Reduces onboarding overhead and improves security.	• Defining standardized roles, to include permissions, will be time consuming and require business cooperation.	• Standardizing devices has already been done and proven effective in controlling cost. • Software rationalization has proven to be extremely difficult; tying rationalization to business roles will help move this initiative forward.
Standardize Refresh Rates: Refresh devices in accordance with Table 2.1 refresh rates.	• Minimizes total cost of ownership by taking into consideration reliability/repair costs and replacement costs. • Lowers impact to users from equipment aging.	• Extends refresh beyond industry best practices. • Requires budgetary discipline in order to program appropriate funding to maintain rates.	• Funds, support staff, and processes positioned to support and maintain standardized refresh rates.
Virtual Desktop	• Improves management and security with	• Thin client devices must be aligned	• Have achieved initial 34% thin clients penetration.

Portfolio Strategy	Benefits	Challenges/Issues	Asset Portfolio Outlook
Infrastructure(VDI): Provision effective computing resources with a Virtual Desktop Infrastructure(VDI): • Thin clients • Application streaming • Telework/Remote Access	reduced labor costs from central administration. • Enables application streaming - reduces cost of deploying software. • Thin client units have 7-10 year lifecycle with lower desktop refresh costs, lower power consumption, and reduced disruption to end user. • Enables telework – any device, anytime, anywhere. • Enables secure BYOD. • Supports disaster recovery.	with users' functional needs (e.g. field user requiring a rugged device would not be a candidate for thin client while most knowledge workers would be candidates). • Some clients hesitate/resist replacement of traditional computing devices with thin client. • Packaging applications for streaming has proven demanding.	Upcoming desktop refresh and role base provisioning provides an opportunity to increase thin client penetration. • Application streaming is improving application deployments and has mitigated cost and client disruption from operating system and office suite upgrades. • Application streaming will enable user self-service for application provisioning. • May need to implement solid state drives to improve VDI performance. • May need to create multiple pools of virtual client images based on business needs.
Automation: Leverage automated workflows for provisioning new equipment, improving patch management, delivering applications, and monitoring & repairing system/application errors.	• Improves operational reliability through providing consistency of actions and outcomes. • Reduces time to provision and deliver operational resources. • Ensures devices are delivered and maintained at known secured baselines. • Ensures speedy response to system and device failures, reducing time for return to operation. • Reduced cost and faster implementation of security and operational patches.	• Requires labor investment in setting up and configuring tools. • Monitoring tools need to be tuned to reduce the number of false positive alerts.	• Slow implementation of management tools; however, deployment of myPC (BPA implementation of VDI) is helping to accelerate deployment and adoption of management tools. • Use management and monitoring tools to ensure operational reliability and to reduce operations costs. • Use of patch management tools will improve security while reducing cost of deploying critical patches.
License Tracking/Usage Monitoring: Track and monitor software license deployment and software utilization.	• Ensures license compliance, enabling identification and removal of unlicensed software. • Allows BPA to repurpose underutilized licenses to reduce and control software license costs. • Could assist in the overall reduction of the number of software titles supported.	• Constrained IT staff time will be needed to implement, tune, and manage monitoring tools and to create reports. • Users may be resistant to having seldom used titles removed.	• License tracking and monitoring tools deployed. • Self-service provisioning portal will aid in reducing client resistance to having seldom used titles reclaimed.
Application Self Service: Allows request and download commonly	• Reduces time and red tape to provision software titles. • Reduced administration costs.	• Strong dependency on applications being packaged for streaming for popular titles.	• Implement capabilities by EOY2019.

Portfolio Strategy	Benefits	Challenges/Issues	Asset Portfolio Outlook
used software titles through a web interface	• Improved client satisfaction. • Supports license repurposing	• Requires web portal with automated workflow/processes.	
Process Maturity: Improve processes through adoption of a maturity model.	• Improves the quality of service to end users, reducing the time to repair systems or deliver new resources. • Supports Operational Excellence through implementing efficiencies and creating a culture of continuous improvement.	• Some IT staff are concerned that finding efficiencies may translate into lower staffing levels.	• Adoption of a maturity model has been slower than anticipated. Deployment of myPC has forced re-evaluation of timelines in moving up the maturity model.
Managed Print Services: Continue to evolve Managed Print Services(MPS)	• Consolidates devices to reduce energy consumption, reduce consumable costs, speed replacements, and streamline support. • Follow-me printing will reduce the annual volume and rate of consumables. • Improves security of printing sensitive documents.	• The temptation and current practice is to continue to use printers past their refresh date. This increases toner cost and can cause print driver issues when upgrading to new operating systems.	• MPS has been implemented and has sufficiently reduced the number of network printers and the cost of consumables from a high of $1.2M per year to $250K. • MPS has demonstrated that personal printers and scanners are not necessary and these devices will be retired as they reach their refresh dates.
Cloud Adoption: Develop cloud-based service delivery	• May support least total cost of ownership for specific services (e.g. email, home drives, SharePoint, etc.)	• Must validate cloud based solutions are both cost effective and reliable. • Must validate active directory federation.	• Complete proof of concept by Q2 FY2016. • Make decision to move email and other services to cloud by Q3 F2016.

Table 3.2: Summary of Office Automation Strategies

3.2 Asset Current State and Accomplishments

The Office Automation Portfolio maintains personal computing devices to support approximately 4,400 staff members. IT has completed deploying a virtual desktop infrastructure (VDI), including disaster recovery redundancy, with a 30% penetration of thin clients. VDI has proven to support our telework, with a peak participation of over 1,400 concurrent teleworkers during one snow event, and is positioned to provide network connectivity during and after a major disaster. Penetration of thin clients has begun to wane due to a combination of an increasing user desire for mobile devices, backlog of software titles that require packaging to enable them to be delivered via streaming, and VDI performance.

The Office Automation Portfolio has been successfully controlling cost and increasing security through hardware standardization. Providing business clients' hardware and software based on business roles will be our next evolution in standardization (see sidebar). Additional accomplishments include:

- Implemented a Public Key Infrastructure to enable two factor authentication using the mandatory OMB issued Personal Identity Verification (PIV) card. By the end of FY2016, all administrative network logins will require using the PIV card, allowing BPA to comply with Homeland Security Presidential Directive-12 and OMB.
- Managed Print Services (MPS) has greatly reduced the number of network printers and personal printers with the intent to retire personal printers as they reach their refresh age. As a result of MPS, costs of printer consumables have dropped from $1.2M to $250K annually.
- Implemented and deployed tools to track and meter software on personal computing devices. Information on software usage will allow us to reassign under-utilized titles, identify titles for rationalization, and prioritize titles for software packaging for streaming. All of these activities will assist in controlling software costs.

Role Based Provisioning (RBP)

Identifying and documenting role based provisioning will (a) assist with aligning users' desire for mobile devices with business objectives, (b) aid in software rationalization by matching software titles to business needs – leading to reduced numbers of titles that will need to be packaged, and (c) may lead to identifying additional role based VDI image pools beyond the current one general pool/image. Having RBP will help with on-boarding new staff. Applying RBP as we enter the next personal computing device refresh cycle in FY2018 should help increase the thin client penetration and reduce the ratio of personal computing devices to users, and help control user demand for peripherals.

In FY2016 we will be renewing our Enterprise Agreement with Microsoft, which will allow us to re-baseline to a lower number of primary personal computing devices/users, transitioning from a per-device to a per-user based license model. Our expectation is that our desktop Microsoft License costs will both drop and be contained in the future.

3.3 Risks

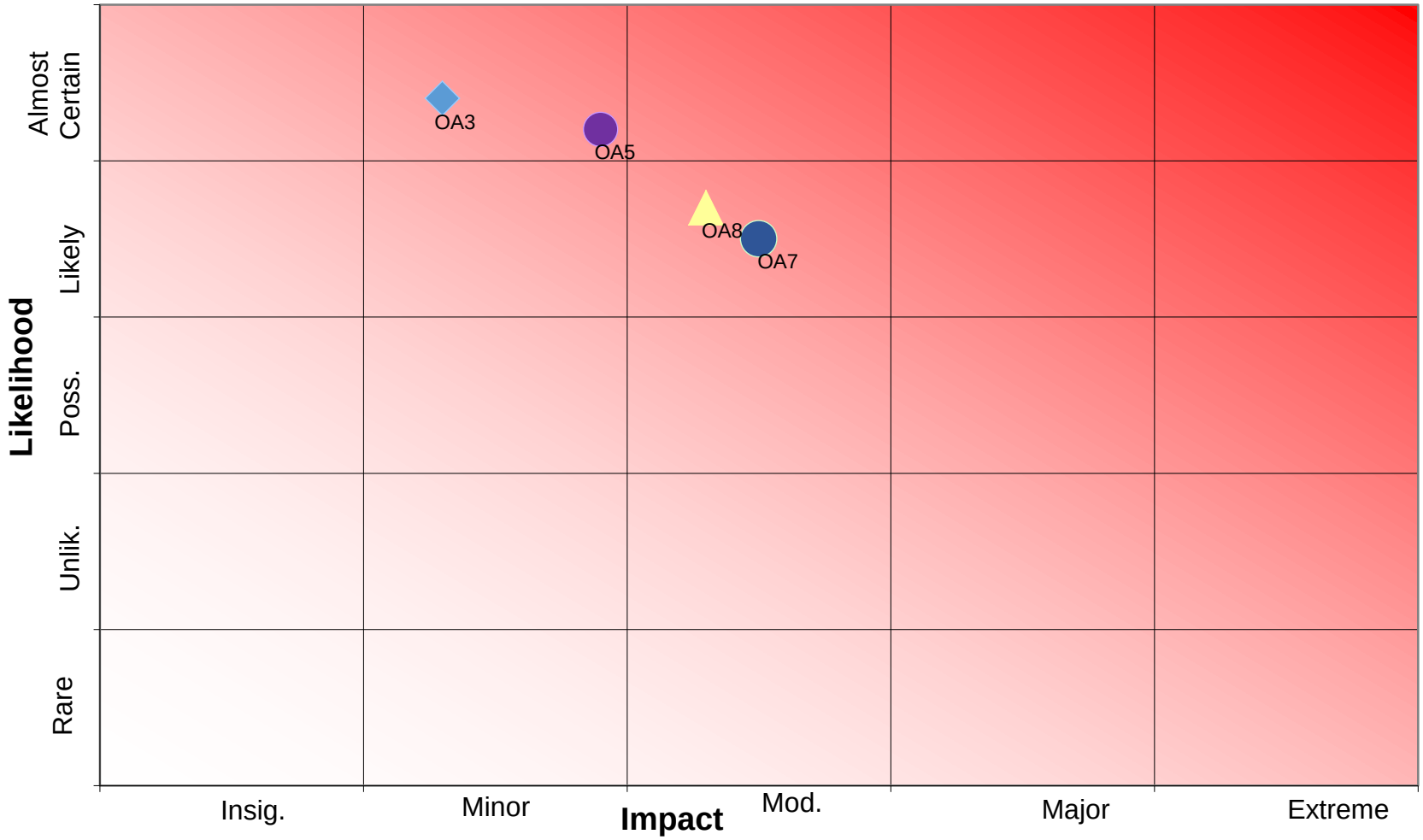


Figure 3.1: Office Automation Risk Map

ID	Risk		Mitigation
	Likelihood	Impact[5]	
OA3	Failure to maintain accurate inventory and deployment information for hardware and software assets.		• Identify and implement automated management software tools to track software titles and software usage, and deployed hardware. • Review and improve current process for tracking hardware assets; investigate RFID tagging and other automated methods. • Work with IT Program Office to validate and refresh current license base. • Prepare and deliver clear and concise direction to all staff describing these roles and responsibilities. Collect signed memo of understanding from staff members. • Place accountability and consequence language into performance plans.
	Almost Certain	Minor ($100K-$1M)	
OA5	Failure to close disconnect with business users on IT resources and meeting future business needs.		• Review and improve current process for reclaiming software licenses. • Utilize management software tools provided by DMP to identify and meter all software titles. • Develop a methodology for renting software and role-based provisioning.
	Almost Certain	Minor ($100K - $1M)	
OA7	Failure to achieve full business value from Virtual Desktop Infrastructure (VDI) due to lower thin client penetration than planned.		• Increase the number of applications that are packaged and consumed in the virtual environment. • Develop role based provisioning that identifies business roles that should use thin clients. • Leverage desktop/laptop refresh cycle to enforce provisioning thin clients where appropriate. • Introduce solid state drives to improve thin client users' performance. • Explore increasing the number of VDI pools to accommodate users groups that need applications that cannot be packaged.
	Likely	Moderate ($1M-10M)	
OA8	Failure to fully utilize VDI to support teleworkers and to support disaster recovery due to DOE guidance prohibiting use of Personal Identification Verification(PIV) cards in non-Government Furnished Equipment.		• Explore using Level 3 multifactor authentication tokens as alternate to PIV cards for non-government furnished equipment (non-GFE) • Work with DOE Multifactor Authentication Working group to allow use PIV card in non-GFE
	Likely	Moderate ($1M-10M)	

Table 3.3: Office Automation Portfolio Risks

[5] Agency-Level Consequence Scale

3.4 Future Initiatives and Funding Considerations

The Office Automation Portfolio has not identified any need for capital funds through FY2024. Individual items within this portfolio (e.g. cell phone, workstations, laptops, printers, etc.) fall below the threshold to qualify for capital funding.

Although the expense budget in the Office Automation portfolio is expected to grow at or below the rate of inflation, there are certain pressures to provide goods or services that could increase the rate of growth, depending on how they are addressed. These pressures include the consumerization of IT (adopting and managing tablet devices, smart phones, etc.) and business requirements for additional peripherals and software. New additions to this portfolio may have a dramatic upward pressure on the funding for this portfolio. These expected new additions include:

- Support for Unmanned Aerial Vehicles (Office Automation aspect would include hand held controls and interfaces with personal computing devices. There will also be impacts on Network Portfolio for transmitting data, and Datacenter for storage of aerial images and other telemetry data)
- Mixed Reality Personal Computing Devices (these devices superimpose data onto the environment that users are interacting with. An example of these devices is the Microsoft HoloLens)
- 3-D Printing (Uses may include creating working models of substation and other components. These printers may become capital expenditures)
- Changing user interfaces from keyboard and mouse (e.g. voice input, touch sensitive, eye tracking, etc.)

Developing and maintaining role based provisioning will be a major tool in controlling hardware and software costs. These new additions will need to be integrated in the business roles to control the speed and extent to which these new additions will be adopted. There will also need to be conversations and decisions around which components of these new additions will be included in the Office Automation Portfolio and which components (and associated costs) belong in other IT asset portfolios.

Additionally, if we experience a large and unanticipated increase in agency staffing, this will result in a corresponding increase in both hardware/software cost and ongoing Office Automation support labor costs.

Table 1.2 and Appendix B contain a partial list of projects for this portfolio.

4.0 Datacenter Portfolio

The Data Center Portfolio covers the computational services and resources (e.g. servers, Fiber Channel switches, data storage), and infrastructure components necessary to operate the BPA's Critical Business Systems, Enterprise Systems (see chapter 5 for a discussion of these assets), and virtual desktop services (see chapter 3). The Data Center Portfolio contains assets that the typical end users seldom think about. However, this portfolio does contain services that are of interest to the most users, including email (includes controlling spam email), file services, and for 20% of users, the technology stack that delivers their desktop services.

Due to the key services that the datacenter delivers and supports, the datacenter must support a number of initiatives that cross one or more asset portfolios. These cross portfolio initiatives include:

- Enabling Single Sign On (SSO) which allows application users and desktop users to be authenticated and authorized using one password or PIN
- Refactoring user credentials that contain partial social security numbers (the practice was discontinued in 2004)
- Providing the infrastructure to deliver virtual desktops
- Providing a disaster recovery solution for
    - Enterprise Systems
    - Virtual Desktops and telework
- Leveraging the cloud to deliver datacenter services
    - Providing disaster recovery
    - Creating elastic enclaves to support data analytics
    - Hosting development and applications in the cloud
    - Hosting infrastructure in the cloud for internet presence and collaboration

In addition to supporting cross portfolio initiatives, the datacenter portfolio is contending with increased Federal regulation. These include support for:

- Homeland Security Presidential Directive – 12 (HSPD-12) to enable multifactor authentication
- Office of Management and Budget (OMB) cloud first directives
- Federal Information Technology Acquisition Reform Act (FITARA) to reduce datacenter power consumption and number of datacenters

These assets are used by almost everyone in BPA by providing the enterprise-wide applications and shared resources that enable the reliable execution of BPA's mission, and the interface to those resources that is available anytime, anywhere.

4.1 Goals, Objectives and Strategies

The over-arching goal is to provide cost effective, reliable, and agile datacenter services to enable BPA to perform its mission and achieve its business objectives. Similar to Office Automation, there are multiple strategies available to IT to achieve a balance between regulatory compliance, improving services, cost effective and timely delivery of services, the safe delivery of new and/or evolving reliable datacenter services, and the ability to provide continuous operations in the face of natural or man-made disasters. Tables 4.1 and 4.2 describe the strategies and the objectives they support. Together, they describe the need for the datacenter services to continue to integrate with Office Automation to build on standardization and to move to leveraging automation and maturing processes in order to continue to evolve into a more agile and cost-effective datacenter environment that thrives on integrity, short time to delivery, and collaboration.

The datacenter has been transforming from traditional dedicated resources to consolidated and virtualized assets in order to more effectively and efficiently meet accelerating business demands, and to prepare to evolve this strategy to a cloud based implementation that will further promote reliability, availability, and security, and support green operating initiatives.

Objective/ Alignment with IT Goals	Outcomes	Status and Comments	Supporting Strategy	Measures
Maximize resource utilization while providing capacity to meet systems' current and projected average and peak resource requirements. **Aligns with:** ITAG 2 – P[6] ITAG 3 - S	• Capacity monitoring is used to achieve optimal resource balancing of key server and storage resources. • Capacity planning is used to project future needs, acquiring and deploying additional resources prior to over-subscribing existing resources. • Use most effective storage solution based on workload (e.g. JBOD, VSAN, SAN, Cloud Storage) • Develop a practice of resource allocation based on work-load profiles in order to control growth and cost of resources. • Use cloud elasticity for systems/workloads for variable/high workloads including development.	Collection of capacity data has improved with the advent of virtual environments. Server virtualization has increased physical hardware utilization. Capacity is in place to meet current and estimated needs through the next refresh cycle through continual optimization. May need to introduce solid state disks to optimize storage performance and maximize use of existing storage capabilities.	• Implement management tools. • Consolidate and virtualize servers. • Implement tiered storage. • Adhere to refresh schedules.	• Reduce current fleet of 838 physical servers to 400 or fewer by 4th quarter FY2016. • Non-infrastructure production server resource utilization average is greater than 45% during core business hours by end of 4th quarter FY2016.

[6] Each objective relates to a single primary goal indicated by "P"; objectives may also relate to secondary goal, indicated by "S".

Objective/ Alignment with IT Goals	Outcomes	Status and Comments	Supporting Strategy	Measures
Proactively monitor data center resources and services. **Aligns with:** ITAG 1 – P ITAG 2 - S	• Monitoring tools are deployed, tuned, and scripted to automatically respond to threshold events, preventing disruption of production services. • Information from monitoring tools is merged to enable event correlation, reducing time to restore services. • Establish end user experience performance monitoring.	 Hardware resource monitoring is well established. Service monitoring has stalled and is being restarted. Storage monitoring tools initially failed, but have been replaced and are progressing. Full Implementation of System Center is ongoing.	• Implement management tools. • Implement automated services.	Provide monthly usage reports and real-time snapshots monitoring all: • IVC production servers' key resources (e.g. CPU, etc.) • SAN disk space
Deliver secure, reliable, efficient, and predictable services through the effective use of management tools. **Aligns with:** ITAG 1 – P ITAG 4 - S	• Recurring tasks are automated using management tools, ensuring repeatable and consistent outcomes. • Provisioning servers adheres to documented baselines. • Standardize and automate data restores and storage provisioning resulting in faster turnaround for requested services, reduced costs, and reliable services.	 Windows Sever 2008R2 baselines have been established. Simple use of imaging is currently employed, and more advanced automation for delivery of base images and layered applications has been started. Automated deployment of the Operating System has been implemented in development using System Center Configuration Manager. Majority of servers are deployed on VMware using template – need decommission process.	• Implement management tools. • Implement automated services.	• Enable capacity planning for all production servers and SAN devices, providing monthly reports beginning 4th quarter FY2016.
Achieve reliable and available services to support and meet BPA's Continuity of Operations Requirements (COOP). **Aligns with:** ITAG 1 – P ITAG 3 – S	• Leverage replication capabilities in storage solutions and databases to protect structured and unstructured data to ensure Return To Operations (RTO) and Recovery Point Objectives (RPO) can be met, leveraging cloud offerings where appropriate. • Leverage cloud services for General Business Systems Disaster Recovery requirements • Move desktop disaster recovery to cloud in FY2020.	 Business Continuity efforts are continuing to identify the next level of business functions needing continuity support for their automation. Lacking COOP/DR for General Business systems – looking to leverage cloud services as cost effective and reliable alternative to on premise solution.	• Implement management tools. • Implement automated services. • Adopt Cloud Services	• Exercise COOP plans for Critical Business Systems twice a year. • Develop non-CBS COOP/DR capability and exercise twice a year by EOY2017.

Objective/ Alignment with IT Goals	Outcomes	Status and Comments	Supporting Strategy	Measures
Services are delivered and asset components maintained in compliance with Federal laws and regulations. **Aligns with:** ITAG 1 –P ITAG 3 - S	• Continuous monitoring tracks compliance with baselines and detects unauthorized changes from the baseline. • Servers provisioned through the use of automated management tools to ensure each deployed server adheres to a documented baseline. • Configuration tools are used to create audit trails on configuration changes. • Implement HSPD-12 requirement for multifactor logins using public key infrastructure and federal PIV card. • Leverage cloud services, when cost effective, to adhere to FITARA data center reduction requirements and to adhere to OMB cloud first directive.	NIST-based server baselines are being used for new builds, and USGCB compliance is built in to desktop images.  Automated tools for monitoring and validating configuration baselines have been implemented. Automated patch management tools and processes are being improved to increase operational reliability and system security.	• Implement management tools. • Implement automated services. • Implement tiered storage.	• Continue configuration monitoring for all production servers with monthly compliance reports. • Make use of IaaS/PaaS cloud services. • Consolidate Datacenters.
Processes and practices aligned with industry practices to deliver secure, reliable services with the least total cost of ownership. **Aligns with:** ITAG 4 – P ITAG 2 – S ITAG 3 – S	• Data Center hardware and software refreshes are sufficient to meet reliability and security objectives while optimizing the total cost of ownership. • Costs of new investments balanced with operations and maintenance costs to achieve an optimized total cost of operations.	 Some base processes were improved through ITIL, but further progress is on hold. A program, Information Technology Service Management (ITSM), consisting of three projects has been proposed and accepted. These projects should help move processes and practices up the maturity model.	• Implement management tools. • Increase automated services. • Consolidate and virtualize servers. • Implement tiered storage.	• Self-service provisioning is enabled by EOY2017. • Adopt a maturity model by Q1 2017. • Establish timelines for advancing along maturity model by Q2 2017.

Table 4.1: Data Center Portfolio Objectives

Portfolio Strategy	Benefits	Challenges/Issues	Asset Portfolio Outlook

Implement management tools to monitor and maintain data center assets.	• Monitor health and status of hardware and services with alerting.
	• Enable capacity planning to optimize resource utilization.
	• Long term, reduce cost of operations by transitioning from reactive to proactive maintenance.
		• Establishing a monitoring team to leverage and manage capabilities.
		• Instilling discipline and creating culture to embrace monitoring and proactive maintenance.
		• Project was de-scoped and these monitoring objectives still need to be implemented under regular O&M.
		• Redundant tool sets need to be consolidated and/or retired.
			• Operations is committed to establishing proactive monitoring of
			  • Server health
			  • Configuration monitoring
			  • Service performance

Implement automated services to provision new equipment with certified baselines, enable proactive event scripting, and enable roll-backs of unauthorized changes.	• Enables deployment of devices provisioned with certified baselines increasing operational reliability while reducing costs. • Enables execution of predetermined automated actions (scripts) based on monitoring thresholds.	• Selection and implementation of software that links workflow with license tracking software/database. • Instilling discipline and creating culture to embrace automation of routine tasks.	• Industry best practices currently embrace adopting and expanding IT automation as a key component of increasing operational reliability and reduction of ongoing operating costs. • Currently own tools necessary to enable automated services.
Consolidate and virtualize servers to optimize utilization of resources.	• Reduces number of physical servers leading to lower hardware costs, license costs, lower staffing levels/costs, and lower power consumption. • Enables reduction of data centers and associated resource/maintenance costs. • Supports moving to cloud services.	• Requires use of management and monitoring tools to achieve and manage consolidated and virtualized servers. • Some applications, e.g. GIS, currently do not perform as well in a virtual environment as on physical servers. • Some legacy systems cannot be supported in a virtual environment.	• Industry best practices embrace adopting and expanding server consolidation and virtualization.
Implement tiered storage.	• Reduces total cost of storage while reducing overhead associated with data backups and recovery. • Optimizes performance to meet workload demand. • Allows technology to match requirements, providing the right solution to the right workload.	• Data retention needs to be more widely defined and enforced. • Data archiving needs to be defined and addressed. • Overcoming hesitation to employ cloud services.	• Implementing tiered storage is a key component of industry best practices to control the growth, costs, and power consumption associated with storage. • Analyzing usage to identify workloads. • Introducing solid state disks will facilitate workload storage strategy. • Implementing JBOD for Exchanged has reduced storage costs by a factor of 15. • Implementing vSAN for CBS storage has reduced cost of storage by a factor of 3.

Portfolio Strategy	Benefits	Challenges/Issues	Asset Portfolio Outlook
Adhere to established refresh rates.	• Optimizes total cost of ownership with operational reliability and stability.	• Higher maintenance costs over 3 year refresh cycle.	• Majority of industry has adopted a 3 to 4 year server refresh cycle with 3 years being the norm for high transactional, high concurrent user organizations. • BPA's systems are low transactional, low concurrent user systems with emphasis on system stability. A 5 year cycle optimizes total cost of ownership and system stability for BPA.
Adopt cloud based services. Candidates for the cloud include: • Email • Web conferencing • Web presence • Archive Services • Dev activities • Data analytics • Collaboration	• Leverages reliability and economy of scale of large data centers leveraging cloud's inherit capabilities ○ High reliability ○ Site failover (COOP/DR capabilities) ○ Backup/recovery/archiving ○ Hardware refresh ○ Security to achieve lower cost of operations and lower carbon footprint from optimized data center.	• Additional or increased bandwidths for circuits to cloud based services may offset savings. • Performance of cloud based services needs to be monitored and managed. • Interoperability issues need to be evaluated. • BPA needs to develop cloud architect skills. • Active directory federation. • Governance of cloud based services. • Shift in type of funding from capital (on premise solutions) to expense funding needed to support cloud based services.	• Federal government is moving to cloud based services with agencies like USDA and GSA leading the way moving to email cloud services. ○ OMB has issued a cloud first guidance/directives. ○ FITARA calls for the reduction of data center power usage and overall reduction in the number of federal government data centers. • J is conducting a small scale pilot to investigate benefits and drawbacks to adopting cloud based services.

Table 4.2: Summary of Datacenter Strategies

4.2 Asset Current State and Accomplishments

The Datacenter Portfolio includes 855 servers to support development, test, production and failover (Alternate Data Center) environments as of the beginning of FY2016. These servers are primarily located in Headquarters, the Ross Complex, and at several of the field sites. Servers are also located at the Alternate Data Center to provide COOP capabilities for the Critical Business Systems. As of the beginning of FY2015, across all environments (test, development, and production), the datacenter portfolio included 1.2 Petabytes of usable SAN storage.

Efforts to implement storage management and monitoring capabilities and the move toward workload storage is still ongoing. However, we have started to see efficiencies. Our current estimates for a usable TB of storage on enterprise SAN is $5,000 per usable TB of storage per year. In FY2014, we have moved email storage off of SAN to Just a Bunch Of Disk (JBOD) at 10% the cost of SAN, while still meeting performance requirements. While this technology shows promise in other areas as well, it is not necessarily appropriate for all workloads. In FY2015, we implemented virtual SAN (vSAN) - a type of Software Defined Storage - for Critical

Business Systems development environments, delivering storage resources at 25% of our cost for traditional SAN. This drive for efficiencies and moving to workload storage has contributed to containing and controlling storage costs. We will continue our efforts to optimize the cost per TB of storage while meeting specific performance requirements. This will include investigating cloud based storage for home drives and archiving.

Included in the datacenter portfolio is the technology stack (servers, storage, and software) needed to deliver a virtual desktop infrastructure (VDI) providing daily service to approximately 1,000 staff members. VDI also supports all of BPA's teleworkers, serving a peak of over 1,400 teleworkers during one snow event. Our VDI capabilities have become so embedded in our daily operations that failover capabilities have been established at our Alternate Scheduling Center. The support and maintenance has fallen within the Datacenter Portfolio and has placed upward pressure on the number of servers in the datacenter being supported in the Datacenter Portfolio.

In addition to supporting systems, and virtual desktops, the datacenter activities have positioned us to meet key OMB mandates and objectives. This includes leveraging our Public Key Infrastructure (PKI) that we are now using to comply with the mandate to use HSPD-12 PIV smart cards for network logins. Our consolidation and virtualization of server resources onto blade servers will enable us to meet FITARA objectives to reduce datacenter power consumption and to contribute to the reduction of federal datacenters. Although not all servers are candidates for virtualization and projects are delivering new requirements for servers, we have reduced the number of physical servers by approximately 40% from the initial baseline. At the same time, we have been examining a strategy for adopting appliances. Appliances are combinations of servers and storage optimized to perform functions. The promise of appliances is lower total cost of ownership through a combination of optimized hardware and optimized management practices. We have adopted the Oracle Exadata appliance, but email and SQL evaluations revealed that workload-based units in farm configurations were a better fit.

4.3 Risks

Figure 4.1 and Table 4. 3 cover the major datacenter risks and mitigation approaches.

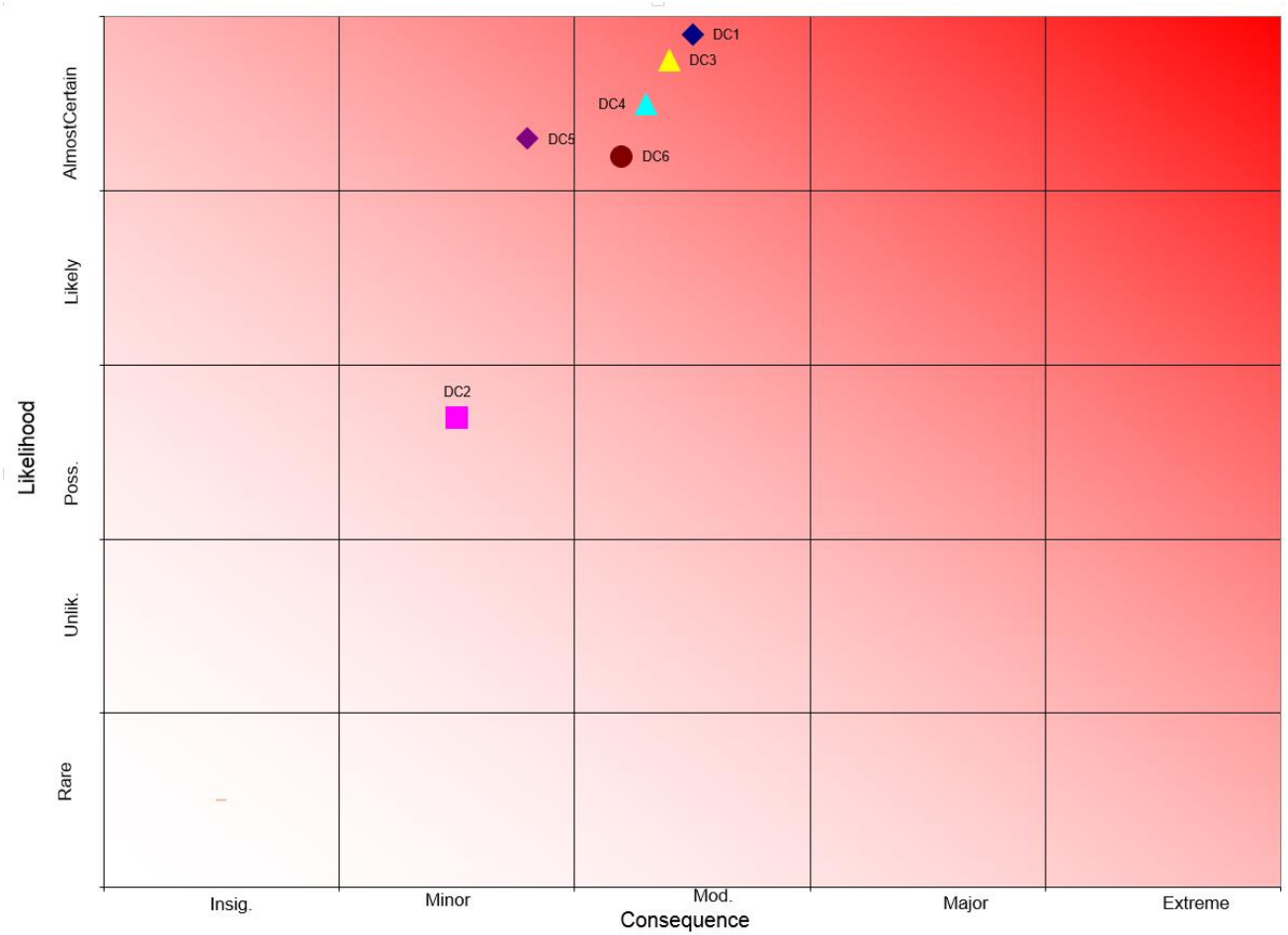


Figure 4.1: Major Datacenter Risks

ID	Risk		Mitigation
	Likelihood	Impact	
DC1	Failure to maintain current baselines to meet known and emerging security vulnerabilities.		Deliver and maintain NIST compliant baselines for current products. Remove (or isolate) products no longer under vendor support – not receiving security patches.
	Almost Certain	Moderate ($1-10M)	
DC2	Failure to maintain servers in documented security baselines to meet compliance requirements.		Tripwire and SCCM have been deployed to monitor compliance with baselines. SCAP compliance monitoring is periodically conducted. (This risk is being mitigated and may be dropped in next IT Asset Strategy)
	Possible	Minor ($100K-1M)	
DC3	Failure to achieve cost efficiencies and security improvements from maintaining individual servers and older operating systems due to the business requirement to host unsupported or poorly supported legacy systems.		Work with business information owners to identify legacy systems that are not adequately supported by the vendor. Maintain the asset plans with activities to retire the legacy systems that are not supported by the vendor. Submit nomination to APSC to approve and prioritize projects to retire poorly supported systems.
	Almost Certain	Moderate ($1-10M)	
DC4	Failure to implement capacity planning leading to either over-subscribing (degraded performance) or under-subscribing (idle servers).		Mature capacity planning and optimized existing architecture – retire legacy services.
	Almost Certain	Moderate ($1-10M)	
DC5	Failure to implement proactive monitoring to prevent service disruption.		Monitoring tools and processes need to begin to monitor quality of service and to establish thresholds for alerting.
	Almost Certain	Minor ($100K-1M)	
DC6	Failure to adequately staff, with sufficiently trained personnel, to leverage monitoring and automated solutions.		Implement workforce strategy and ensure hiring is aligned with the workforce strategy.
	Almost Certain	Moderate ($1-10M)	

Table 4.3: Data Center Portfolio Risks

4.4 Future Initiatives and Funding Considerations

The Data Center continues to offer opportunities to control costs through efficiencies while improving service delivery and reducing out-year costs. This includes in-place improvements in efficiency for some systems, as well as moving to cloud-based solutions when system refreshes approach and total cost of ownership supports the transition (e.g. cloud based services are cost neutral or lower cost than on premise solutions). In addition to technology improvements and efficiencies, we have opportunities to achieve process efficiencies through the adoption a maturity model. However, it will take a number of years to move up a maturity model and achieve process efficiencies and to enable operational reliabilities.

Outlook:

- Capital for sustain activity should begin to fall, with a commensurate rise in expense as functions are transitioned to the cloud rather than refreshed on premise.
- As automation increases and cloud services are employed, a greater emphasis on collaborative solutions architecture with the business should ensue, shifting expense from maintenance to solutions.
- We're likely to experience a mid-term peak in total funding, followed by a post implementation decrease, as major enterprise software systems require resources for upgrade and/or replacement.
- The overall expenditure profile should roughly mirror the rate of inflation plus new contracts.

Table 1.2 and Appendix B contain a partial list of projects for this portfolio.

5.0 Network Portfolio

The Network architecture is sometimes viewed as a delivery mechanism to provide computer applications to end users, wherever they may be located, as well as other types of electronic communications. The services delivered through the Network Portfolio can best be described as utility services in the sense that end users expect the services to be available without thinking about them, just like the electric power in their offices. It provides the first bastions of cyber safety, while providing clients with the ability to be agile and dynamic in the ways in which they work. As a result, these asset objectives tend to have an internal IT aspect to them. However, video conferencing, tele-presence, and mobile connectivity are areas where business units and IT can partner to develop network service objectives and strategies to maintain or enhance existing services, and to implement new services, such as wireless access points, where requirements dictate. Although there is a long-standing tradition of blaming the network in a tongue-and-cheek manner for all cyber ailments, the truth is that BPA's networks have a very long record of stable availability and performance.

Networks form the silent, solid foundation upon which all IT automation activities are constructed.

5.1 Goals, Objectives and Strategies

The primary goal of the Network portfolio is to provide the interconnection that allows data and applications to combine to form information delivered to the end client wherever and whenever they demand it, and to do this transparently to such an extent that the network isn't noticed. The strategies that support this effort are to keep the network assets current in terms of versions and patches, and well documented, to enhance security through device authentication and authorization, to provide redundancy that allows on-line upgrades and supports continuous operations, and to improve monitoring and management that supports dynamic prioritization and growth planning. And as clients require additional mobility to support their efforts across distributed campuses, the Network portfolio will continue to expand its wireless capability to satisfy these demands. Tables 5.1 and 5.2 detail these goals and strategies.

We have established an environment of reliable performance communications that enables our business partners to envision solutions that make best use of interconnected systems, and enables new levels of personal productivity through mobile technologies.

Objective/ Alignment With IT Goals	Outcomes	Status and Comments	Supporting Strategy	Measures
Provide secure and reliable voice and data network services to enable the BPA to perform its functions and to coordinate and communicate internally and externally. Aligns with ITAG 1 - P ITAG 3 - S	• Detection and prevention (ISE / NAC) of attempted unauthorized access. • Capacity and redundancy to meet general availability and return to operations objectives, and specific Continuity of Operations (COOP) objectives. • Sufficient network capacity to ensure quality of service to enable users to access IT resources to perform their jobs. • Secure Access, security (firewall), and bandwidth to the public internet are sufficient to meet emerging cloud computing requirements and remote access to BPA IT resources.	 • BPA's telecommunications backbone has a longstanding reputation for delivering secure, reliable, and highly available voice and data services throughout the BPA. • Power fluxes at some substations produce momentary loss of network services. Services are typically quickly restored. Business impact has been minimal. The network group worked with TE in 2015 to increase resiliency significantly in Montana and is working in the area of TeaKean Butte and Dworshak now. Power issues still account for 70% of Field network outages. • Parts availability becomes an increasing challenge as systems approach end of life, risking continued reliability. In 2015 the network group replaced all Metro client access switches and is over 70% completed with Field client access routers/switches. Field will be completed in 2016. DMZ switches are also scheduled to be replaced this year. End-of-life VTCs are scheduled to be replaced in 2016. End-of-life PBXs are scheduled to be retired in 2016 (assuming Enterprise Board approves project). BPA network gear will be in excellent shape at the end of 2016. • Secondary circuits are not able to provide connectivity with sufficient bandwidth when primaries fail. The network group continues to increase bandwidth to many BPA sites while also reducing costs. The savings are then applied to other bandwidth needs. OMET may provide additional relief to Field sites as well but we do have a contingency plan.	• Refresh Cycles • Operational Excellence	• Deliver 99.9% network availability in Headquarters, Ross and Munro though FY2018 to enable BPA to coordinate and communicate effectively. • Deliver 99.9% phone service availability though FY2018 to enable BPA to coordinate and communicate effectively. • Reduce the yearly number of Wide Area Network disruptions to field sites by 50% of FY2010 disruptions by end of FY2017.

Objective/ Alignment With IT Goals	Outcomes	Status and Comments	Supporting Strategy	Measures
		• ISE / NAC was implemented previously for Wireless Access Points and are scheduled to be implemented for Wired devices in 2016. • Internet Speeds are scheduled to increase 10-fold in 2016. • COOP documentation will be thoroughly revised to reflect the mass change of equipment with new capabilities (especially on phones).		
Leverage technology to meet BPA business objectives. Aligns with ITAG 3 - S	• Reliable video conferencing and tele-presence capabilities (VoIP). • Reliable phone services to enable the BPA to coordinate and communicate internally and externally (VoIP). • Secure and reliable Wi-Fi access. • Secure and reliable services for mobile users. • Unified messaging/communication capabilities are provided (VoIP). • Continuous monitoring program tracks performance and utilization in order to predict and proactively mitigate performance issues.	 • Through the use of proven, scalable technologies and adaptive, low-latency, high-availability architectures, BPA's voice and data needs and objectives have been, and will continue to be, met and/or exceeded. • BPA must evolve WAN circuits to provide sufficient bandwidth to support emerging business requirements such as streaming video/video broadcast, VoIP, and video teleconferencing. OMET completion will provide relief. • Continue to replace existing CAT 3 & 5e cable plant with CAT6a LAN cabling to support increased LAN bandwidth requirements and requirement for Power over Ethernet (for Wireless Access Points / Phones / other devices). • Telecommuting and expanded business outreach is generating increased usage of the BPA audio conference system and circuits. Adoption of VoIP and Unified Communications will increase the reliability and capability of these systems. At the beginning of 2016 BPA has about 600 VoIP phones and should complete the transition in early 2017. BPA audio conferencing system will be replaced by WebEx by mid-2017. WebEx is	• Refresh Cycles	○ Expand Voice over IP implementation to HQ by EOY 2016 and Ross by EOY2017 (assuming Enterprise Board approves). ○ Integrate soft phones in to environment, plan completed by 1st quarter FY2018 ○ Implement a Unified Communications roadmap by 2nd quarter 2017 ○ Provide infrastructure support, bandwidth and connectivity to cloud services as business requirements emerge.

Objective/ Alignment With IT Goals	Outcomes	Status and Comments	Supporting Strategy	Measures
		being used for external conferencing (audio and video) now.		
Services are delivered and asset components maintained in compliance with Federal laws and regulations. Aligns with ITAG 1 – P ITAG 3 - S	• Continuous monitoring program tracks compliance with baselines and detects unauthorized changes from the baseline (implement Tripwire and Nessus). • Risks mitigated to acceptable levels to enable the BPA to perform its functions. • Begin network migration to use IPv6 (FY2018/19). • External-facing connections are Trusted Internet Connection (TIC) compliant. • Smart Cards used in two factor authentication for network access (ICAM project). • System Security Plans (SSP) are documented and approved.	 • Although late in meeting Federal mandates to operate IPv6 protocols on the network, momentum is building to make a concerted effort to move this initiative forward. The business need to accomplish this has been quite low to date. Industry measures show only 10% penetration for IPv6 at present. Prudence would dictate BPA allow the technology to mature in the Enterprise space. • Federal initiatives across the government for Trusted Internet Connection (TIC) have languished in budget set-backs for some years. However, there has been sufficient progress in this area to have some agencies that BPA communicates with demand that communication utilize TIC. We will have to address this very soon. • Continuous monitoring has been implemented for CheckPoint Firewalls. Tripwire and Nessus implementation has been impacted by staff turnover in other groups and resource shortages in Networking.	• Refresh Cycles	• Implement IPv6 by EOY2019 to comply with OMB guidance to develop plans and transition to IPv6. • Implement Smart cards for network logons by EOY2016 to comply with HSPD-12 directive to use Smart Cards for network access. • Migrate to TIC for externally facing internet connections by EOY2018 to comply with OMB mandates.
Processes and practices aligned with industry practices to deliver secure, reliable services with the least total cost of ownership. Aligns with ITAG 4 – P ITAG 2 – S ITAG 3 - S	• Network hardware and software refreshes are sufficient to meet reliability and security objectives while optimizing the total cost of ownership. Costs of new investments are balanced with operations and maintenance costs to achieve an optimized total cost of operations.	 Although some effort has been expended to adopt a maturity model and advance along its curve, adoption has been very slow to materialize. This is not unique to the network portfolio, but rather systemic across all of the IT organization. The network group has made significant progress in refreshing network hardware and appliances. They have replaced virtually all client access devices and reduced total number of device types by 1/3 and manufacturers by 80%. In 2016 only legacy	• Operational Excellence	• Establish the maturity model to be used throughout the IT organization by Q3 FY2016. • Evaluate status of key processes (Change & Configuration Management, Incident Management, Problem Management, and System Monitoring) in relation to the maturity framework by EOY2017.

Objective/ Alignment With IT Goals	Outcomes	Status and Comments	Supporting Strategy	Measures
		server support will remain and that will be retired in 2017 when final moves are made to IVC.		• Map the current status into the maturity model and develop plans to advance the maturity level, by Q1 FY2018. • Achieve next maturity level for all operational processes by EOY2018.

Table 5.1: Network Portfolio Objectives

Portfolio Strategy	Benefits	Challenges/Issues	Outlook
Execute on established refresh cycles to optimize total cost of ownership.	• Provides for orderly, non-disruptive, and cost effective insertion of new technology.	• Long lifecycles for network and phone devices result in delays in implementing new technology and deploying new capabilities. • Next network refresh cycle will need to plan for: ○ Implementation of IPv6. ○ Expanding Voice over IP to HQ and Ross. ○ Increased adoption of telecommuting/mobility places greater demand on conference bridge systems and circuits. ○ Expanded wireless access points with integration into network. ○ Possible deployment of soft phones.	• Phone and network systems must achieve 99.9% availability or better. While past experience has demonstrated excellent reliability and stability, these systems are pervasive, and upgrade implementations are complex and long in duration. ○ Network refresh scheduled for FY2020 timeframe. ○ Phone refresh schedules include migration to VoIP and use of VoIP handsets and/or softphones in the FY2016-FY2018 timeframe.
Institutionalize Operational Excellence to improve service delivery, increase work throughput, and achieve efficiencies.	• Implementing and incorporating a maturity model into daily operations will improve operational reliability while reducing maintenance labor costs. IT can expect to see a reduction in operations labor costs of 10% [7] by advancing a level in the maturity model.	• IT culture has not lent itself to change and/or documenting processes and their supporting roles. This will require change management to be completely successful. • Although a few specific technologies were implemented during the first attempts, it was difficult to agree on which maturity system to implement, and support has waned.	• Industry has embraced ITIL to improve operational reliability, improve quality of service, and to reduce cost of operations. • IT in general may re-start the effort to implement a maturity project to move IT operations from basic to standard level for four key processes.

Table 5.2: Network Portfolio Strategies

[7] Ross & Weill, Harvard Business Review, Nov 2002.

5.2 Asset Current State and Accomplishments

The current Network Portfolio includes 1,000+ network devices and 2 PBX systems spread across the metro region and the field. The network has been providing solid performance over the last five years with no service disruption of core services in Headquarters or the Ross Complex. Branch offices have seen minor disruptions due to issues with external circuit providers resulting from fiber being cut or other issues that are generally quickly resolved. The majority of service disruptions to field sites are the result of unconditioned power used to run on-site equipment in remote locations, and it has proven to be cost inefficient to attempt to provide conditioned power in these locations. This may change with new DATS implementation. Managing this diverse and disparate collection of assets across a large geographic area offers distinct and daunting challenges, requiring a phased and iterative process that can span multiple fiscal and calendar years and includes the coordination and cooperation of IT, Transmission Services, Power Services, and a variety of governmental and private sector service providers.

Several OMB mandates and other upgrade/modernization projects have driven the Network Portfolio to modernize equipment and cabling. Specific technologies on the near horizon include IPv6 compliance, expansion of wireless services, LAN/WAN bandwidth upgrades, ubiquitous computing (tablet computing), and broadcast streaming media services such as VoIP and video. It is expected that the business will make selective moves to cloud services over the coming years, which will require the Network portfolio to ensure access (circuits – generally public internet) and security (firewall) and bandwidth to meet business demands. A review of our leased network circuits reveals that increased bandwidth and redundancy will be required to support those services, resulting in higher annual service contract costs for leased circuits. These same pressures will drive the need to upgrade local cabling plants in several locations throughout the agency in the near future.

Accomplishments include:

- Data: Core circuits upgraded to Gb. Scheduled to move to 10 Gb in FY2016. Modems have been retired. Frame Relay also retired. MPLS have upgraded to Gb at HQ and Munro. Many field sites have been updated 100 Mb or above.
- Client Access: HQ client switches have been completely replaced. Will provide Gb to all desktops as well as PoE. Redundant control cards have been installed into switches for in-service software upgrade (ISSU) to allow for regular patching without impact to clients. Field has had over 70% replacement and should be 100% by mid CY2016 except for about 30 ASR routers.
- Data Center (legacy) is being compressed to remove unsupported equipment. Internet gateway routers and Business Partner Routers were replaced.
- Firewalls: DMZs have had main firewalls upgraded. CheckPoint Firewalls were upgraded from 4 to 12 cores. Upgraded critical VPN and Citrix Netscalers.

5.3 Risks

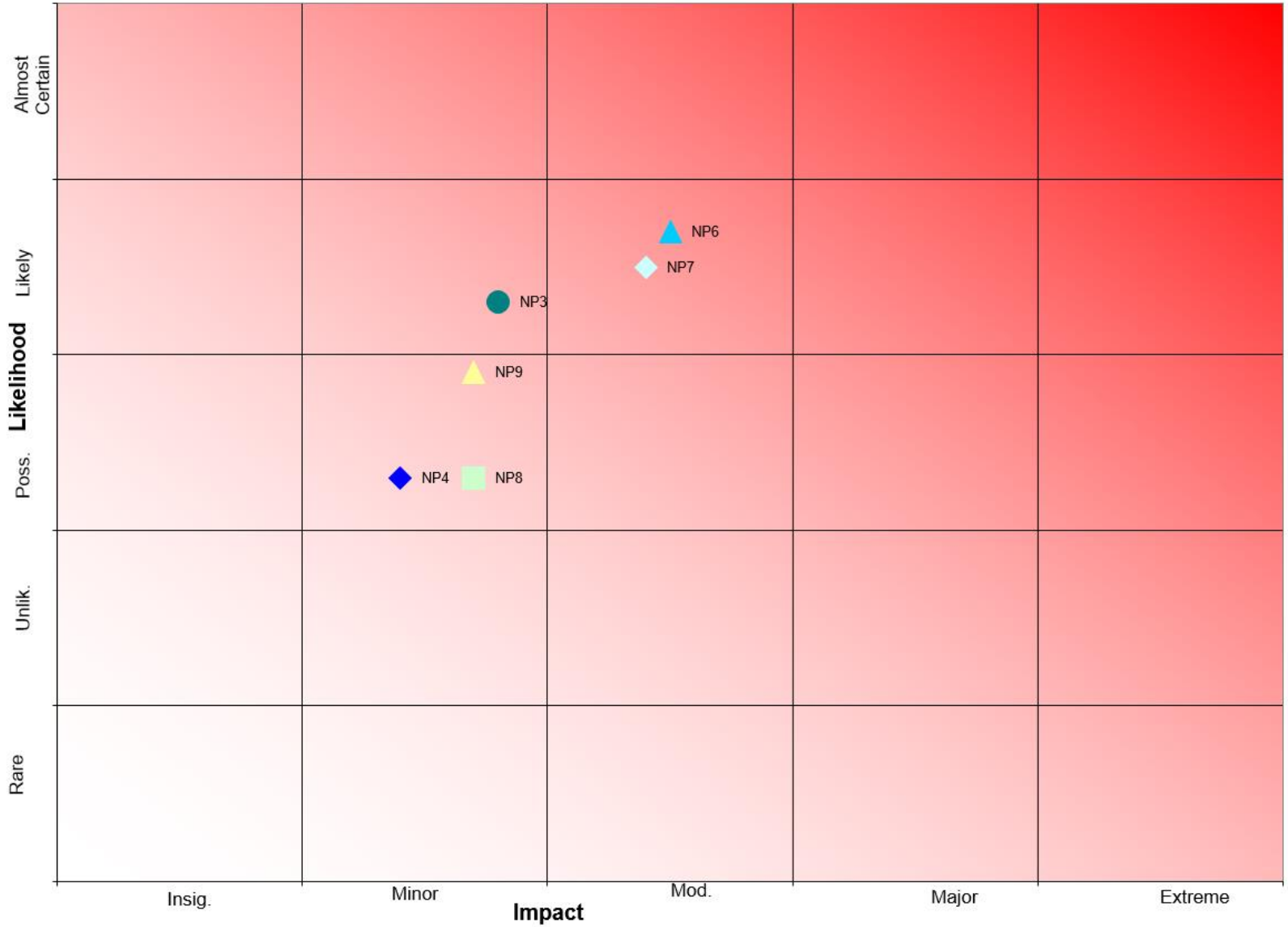


Figure 5.1: Network Risks

ID	Risk		Mitigation
NP3	Failure to implement and leverage the necessary monitoring tools to enable expansion, maintenance, troubleshooting, and reporting on existing and future networks.		Implement purchasing guidelines requiring the inclusion of management and monitoring tools, plans, and methodologies to be implemented with each new purchase. Since Cisco is our primary provider, inculcate their native management and monitoring tools into daily operations of the network. Leverage additional Sunflower modules to effectively track status of network component inventories. FY2016/17 work to implement monitoring and alerting.
	Likely	Minor ($100K - $1M)	
NP4	Failure to position and prepare BPA's systems and services to meet emerging security threats.		Work closely with Cyber Security to maintain existing security infrastructure Intrusion Detection Systems (IDS) (next-generation firewalls moving to prevention, ISE/NAC, etc.) while harnessing emerging technologies and methodologies to further enhance our security coverage. CTO baselines established and implemented.
	Possible	Minor ($100K - $1M)	
NP6	Failure to plan, prepare, and position resources to migrate to IPv6.		Establish business plan and project proposal to meet this regulatory requirement. Implement external facing IPv6 followed by future internal migration to IPv6.
	Likely	Moderate ($1M - $10M)	
NP7	Failure to plan, prepare, and position resources to migrate to TIC.		Establish business plan and project proposal to meet this regulatory requirement. Work closely with DOE to ensure adequate service availability, and performance in relation to cloud services hosted in FedRAMP facilities
	Likely	Moderate ($1M – $10M)	
NP8	Internet bandwidth could be consumed at a higher rate or larger peaks than can be met by capacity.		Track utilization growth patterns with Cisco monitoring tools, collect expected capacity increase requirements from MyPC/Mobility and cloud initiative efforts, and predict timelines for service upgrades. Implement annual disaster capacity testing.
	Possible	Minor ($100K - $1M)	
NP9	Video conferencing and collaboration demands may overwhelm network performance.		Leverage network assessments being performed through current VoIP project, along with Cisco monitoring information, to track and predict network bottlenecks, and plan appropriate upgrades.
	Possible	Minor ($100K - $1M)	

Table 5.3: Network Risks

5.6 Future Initiatives and Funding Considerations

It is also possible that unknown initiatives may emerge in the FY17 – FY18 timeframe that will have network portfolio implications.

Outlook:

- Labor and materials expense growth is expected to remain relatively flat, matching the rate of inflation.
- Additional sites
    - Additional Transmission sites are regularly added to the network as they no longer consider BPAnet connectivity as optional. These have been averaging about 1/month.
    - We added a number of sites for NERC-CIP5 this year
    - We may need to add an additional 87 sites to comply with HSPD12 by 2019
- Contracts will grow in the near term due to:
    - TIC compliance
    - VoIP capacity demands
    - ADC/BSDR capacity demands
    - Growth in adoption of SaaS solutions

Overall, the network portfolio expense profile will experience growth at the rate of inflation plus new contracts.

Table 1.2 and Appendix B contain a partial list of projects for this portfolio.

6.0 Application Portfolio

The Application Portfolio currently accounts for 41% of the IT expense budget with 15.5% providing system enhancements to meet emerging business needs. This portfolio presents unique challenges in describing its objectives as each one of the over 100 major systems in the Application Portfolio has its own set of objectives. For example, the Customer Billing System strives to produce timely and accurate bills while Columbia Vista creates generation forecasts to support inventory and revenue projections. Due to this unique situation, individual systems' objectives will be maintained in the individual asset plans that compose the Application Portfolio. Here we will only present the BPA level objectives of the Application Portfolio.

Assets in the Application Portfolio differ from the hardware assets in the Datacenter, Office Automation, and Network portfolios as hardware assets have proscribed refresh rates based on industry best practices. In the past, applications have been kept in service until the business owners initiate a request to replace the application. We are starting to build the capabilities to track the business value being delivered by an application to forecast the point where the cost of maintaining the system exceeds the business value being delivered by the application. The intent is to take action to ensure the business value always exceeds the operating cost of the system. This action may be to upgrade the application, replace the application, or just retire the application. Building the capabilities to track business value will be dependent on business units developing and maintaining business metrics. The intent is to hold annual post investment reviews to monitor the net economic benefit ratio and to use this metric to indicate when we need to upgrade, replace or retire the application.

In addition to business value, BPA as a federal entity has guidance to refactor or replace systems to meet evolving cyber security requirements. One method we will use to adhere to this guidance is to implement assessments based on ISO 25010 to identify systems that may need action. We will also require that commercial applications and services acquired by the Agency be maintained at a version supported by the vendor.

Another aspect of increasing both application security and reliability is managing personal productivity applications (Excel and Access applications) developed by end users. These tools are developed by end business users for their own personal use; however, they may share these tools with other business users or the applications become a key component of a workflow. These tools are seldom kept current on the product version nor are these tools built with security in mind. When issues arise with these tools, the business units often ask IT to take over maintenance. This creates unplanned workloads and resource demands on the Application Portfolio to close security issues and address both productivity and reliability problems.

Applying these new practices will result in higher enhancement costs and replacement projects. Until we mature these practices we will have uncertainty in forecasting of out-year resource requirements. Until our practices mature we are using the rule of thumb that major

applications will need an upgrade after 5 years of service and a major upgrade or replacement every 10 years. Given industry trend towards Software as a Service (SaaS), the expectation is that replacements will increasingly turn to SaaS solutions. However, since we cannot know the type of solution years out, we are currently programming capital for replacements.

Although we have developed business continuity capabilities for our critical business systems, we have not done so for our general business systems. This is an area that overlaps with the Datacenter Portfolio. Following OMB's "Federal Cloud Computing Strategy February 8th, 2011", one of the alternates we will evaluate is hosting business continuity for our General Business Systems in the cloud. We will also be looking at the cloud for hosting external web applications. As we move to the cloud and adopt more SaaS (we currently have 20 SaaS solutions) we also need to develop a more disciplined and holistic data integration strategy. The overall goal is to achieve hosting 20% of our systems in a cloud based solution.
A major initiative that will help control development and operations costs, while improving system reliability and security, is adoption of a software maturity model. The first step includes identifying and adopting an appropriate maturity model. The adoption of a maturity model is a major undertaking, taking several years to achieve a net return on the investment. However, one of the key outcomes from adopting a maturity model is instilling the processes and discipline necessary to build security into the system throughout the system's lifecycle.

We have established partnerships with our business lines for the purpose of tracking and monitoring our major systems' business value to ensure our systems deliver more value than the cost of operations.

6.1 Goals, Objectives and Strategies

The Applications Portfolio strives to implement software development and maintenance practices built on standardized processes and methodologies that align with the chosen maturity model. This overall strategy is expected to keep operational costs low by placing an emphasis on configuration over development: select COTS packages first, and modify business process where needed instead of modifying COTS code that creates unique solutions. Standardization will also lead to shareable and reusable objects, contributing to lower overall costs. An end goal is to provide an Applications Portfolio that is more easily maintained and remains modern and relevant through prudent asset lifecycle management.

Our applications deliver performance and value through standardization that drives integrity, reliability, and availability.

Application Objectives	Outcomes	Status and Comments	Supporting Strategy	Measures
Evolve and leverage systems' capabilities to meet emerging business objectives. **Aligns with:** ITAG 2 –P ITAG 3 –S	• Develop and/or buy COTS solutions that leverage and, where possible, contribute to Service Oriented Architecture and data abstraction. • Develop and maintain a library of Enterprise reusable components and services to reduce development time, development costs, and maintenance costs. • Extend existing systems to meet emerging business needs, where feasible, through reusing services/capabilities, or by adding additional modules.	 Improving reuse though the establishment of Solution, System, and Integration Architects. All new projects now must consider existing systems in Analysis of alternatives. Collaborative Standard Team – a team of software developers establishing standards to facilitate and promote object reuse.	• System Architecture • Leverage System Life Cycle	• Update BITA to include Cloud Architecture with supporting Service Oriented Architecture and Integration Architecture • Solution Architect reviews and makes recommendation on all Analysis of Alternatives and System Designs.
Asset Plans include tactical and strategic evolution of systems that balance business unit's requirements with BPA objectives. **Aligns with**: ITAG2-s ITAG3 –S	• Asset Plans have multi-year activities scheduled for enhancements, upgrades, and replacement for each individual system as a result of the Information Owner and Information System Owner working together to create these plans. • Establish metrics, creating transparency on costs, value, and performance. • Annual review of each system's Total Cost of Ownership.[8]	 Several business units are engaging to develop roadmaps which help develop asset plans. However, there has been little work on creating metrics to track business value for legacy systems.	• Asset Plans • System Architecture	• Extend asset planning to 10 year windows by EOY2018. • Establish metrics to measure business value for top 15% resource intensive systems by EOY2018. • Perform annual review of Business Case (net value/TOC/NEBR).
Services are delivered and asset components maintained in compliance with Federal laws and regulations. **Aligns with**: ITAG1 – P ITAG3 - S	• All systems are covered by a current System Security Plan or approved GSS. • Monitoring tools are in place to detect and report on changes in application baseline – changes are verified and validated as authorized changes. • Service levels are established for each system to include availability and Return To Operation (RTO) requirements. • New solutions are cloud ready per OMB cloud guidance. • Legacy systems are refactored or replaced to meet evolving security standards per OMB guidance.	 Established System Security Plans define and monitor application baselines. There is increased rigor around change management. Continuity capabilities for Critical Business Systems are proven, however General Business Systems need to have continuity services developed, Have established ISO 25010 based system assessments.	• Leverage System Life Cycle System	• System Security Plans will be reviewed and updated annually or upon major system enhancement. • 10 systems undergo ISO 25010 Assessment annually. • BITA maintains standards for COTS and in house development to ensure solutions are cloud ready.

[8] Determining value and Total Cost of Ownership must be extended to include the substantial number of Task systems maintained by JS; although, individually each Task system represents a small to modest cost, collectively these Task systems represent a sizable investment and operating cost.

Application Objectives	Outcomes	Status and Comments	Supporting Strategy	Measures
Processes and practices aligned with industry practices to deliver secure, reliable services with the least total cost of ownership. Aligns with: ITAG4 – P, ITAG2 – S ITAG3 – S	• Establish criteria for determining a "maintain" versus "upgrade" or "replace" decision. • Maturity framework is in place for software development and operations.	 The SLC is being extended to improve rigor in ensuring solutions provide least Total Cost of Ownership and viable net economic benefit ratio.	• Leverage System Life Cycle • Software Maturity Model	• Identify software maturity to govern development and maintenance by EOY2017. • Move to next level of maturity model by EOY2020. • Update BITA with criteria for determining a "maintain" versus "upgrade" or "replace" decision by EOY2017.

Table 6.1: Applications Portfolio Objectives

Portfolio Strategy	Benefits	Challenges/Issues	Outlook
Asset Plans: Develop individual system asset plans covering maintenance, enhancements, and eventual replacement.	• Builds partnership between IT and business units. • Identifies out year support costs. • Establishes performance and value metrics. • Identifies risks. • Tracks life cycle and helps set replacement/retirement targets. • Individual plans will contribute to the Application Portfolio which will contribute to IT Asset Strategy.	• Business units and IT are not accustomed to developing and using metrics. • Most business units are not accustomed to thinking more than a year ahead on their system needs. • It will take time and resources to develop asset plans covering the major IT systems.	• Efforts are underway to begin developing asset plans for the top five Critical Business Systems and top five BPA Commercial Enterprise systems. • Development of system level asset plans is already in the System Life Cycle, systems being delivered in FY2016 will need to provide the maintenance team with the initial asset plan. • Steering committees have been established for several key systems, e.g. FMS and Hrmis, which can be leveraged for managing asset plans.
System Life Cycle(SLC):	• Maturing the use of the SLC through the maintenance cycle will require both training and change management. Maintenance currently is accustomed to simply making business requested changes with minimal adherence to SLC.	•	• System work products called out by the SLC are being created by projects. Through training coupled with change management these work products will be maintained to improve and control the evolution of systems to meet emerging business requirements and to identify when systems should be upgraded or replaced.

Portfolio Strategy	Benefits	Challenges/Issues	Outlook
System Architecture: Develop plans to leverage existing system capabilities, for improving interoperability and for implementing Service Oriented Architecture.	• New systems will be implemented to leverage and reuse existing capabilities instead of delivering similar/redundant capabilities, which drives up BPA's IT costs. • Reduces time to deliver new systems. • Improves interoperability and reduces data integrity issues.	• Project managers and project sponsor are accustomed to thinking in terms of best of breed and business unit needs & benefits versus BPA needs and benefits. • Project managers and sponsors often view considering BPA needs as unwelcomed scope creep with a negative impact on their project's budget and timeline. • Has proven difficult to reserve resources for establishing business analyst and system analyst positions, as well as staff with both skills and aptitude to fill positions.	• The project management is maturing to ensure BPA needs are considered and included into projects where feasible and appropriate. • The IT department has not developed mature system architecture nor a comprehensive approach to implementing a Service Oriented Architecture. Availability of resources is slowing progress; outlook is for continued constrained resources and slow progress through FY2016. • With the development of the ISO 25010 assessment model, both our business and IT can speak in the same quantitative terms thus clearing the blurry line between given non-functional compliance requirements, best practices and functional business needs. The continued support for the assessment model is gaining support from both business and IT.
Application Performance Monitoring: Move to proactive monitoring of quality of service.	• Combines incident, problem, and change management to identify most problematic alerts. • Identifies problems and implements corrective actions (where possible) to avoid service disruption. • Aligns with industry best practices.	• Establishing response thresholds and developing corrective action scripts are labor intensive – requires a commitment of resources to receive benefit. • Organizational boundaries coupled with roles and responsibilities have impeded deployment of application monitoring in the past. • The majority of IT needs to develop an operational understanding and implement. • Project managers have not been including application monitoring capabilities as a system requirement (see previous bullet). • Need to develop consensus on application monitoring capabilities.	• Limited application monitoring was implemented in FY2011; resources constraints may delay maturity until FY2016. • Including requirement for application monitoring in SLC ensures new systems will be delivered with this capability. • CBS has made improvements in monitoring systems; still need to make improvements in end user experience monitoring.
Software Maturity Model: Adopt a maturity model to improve quality and predictability of software development and	• Provides guidance for developing or improving processes that meet the business goals. • Provides guidance for quality processes, and provides a point of reference for	• Currently there is large diversity in the approaches project and maintenances teams use in developing and maintaining systems. Change management will be needed to select and adopt a common model.	• CBS began an effort in FY2014 to first identify a software maturity model and then plan the piloting and adoption of the maturity model. This effort is viewed as a critical endeavor to improve the agency development capabilities and will take several years

Portfolio Strategy	Benefits	Challenges/Issues	Outlook
maintenance activities.	appraising current processes. • Provides essential elements for effective and continuous process improvement.	• High rate and number of new projects beginning in FY2010 to date has made it difficult to devote resources to identifying and implementing a software development maturity model.	from conception to reach the higher levels of a maturity model. • CBS has effectively utilized the results of the ISO assessment model. CBS has engaged the CTO's office in requesting an annual assessment cycle utilizing the model. This capability needs to be adopted by the rest of IT. This is predicated on increasing the capabilities of the CTOs office.

Table 6.2: Application Portfolio Strategies

6.2 Asset Current State and Accomplishments

We have taken steps to control spending and the cost of information technology for BPA through managing the costs of our infrastructure assets. However, we are facing stiff challenges as new applications are delivered through the Project Work Plan and are placing upward pressure on the Application Portfolio expense budget from new service contracts and labor for operations and maintenance. In past years, cost for new systems (service contracts and O&M costs) have been offset through a combination of reducing system enhancements and deferring hardware refreshes. This strategy, coupled with the rapid pace of automation from FY2009-FY2013, has resulted in limiting resources needed to make enhancements. As a result, business units have expressed disappointment in IT's ability to make enhancements to their current solutions to meet emerging business needs. In other words, IT has been developing a backlog of business requested system enhancements.

Without understanding the business objectives and metrics to measure performance and value, the question of the amount of value these enhancements are providing cannot be answered. Should IT plan to allocate more or less resources to enhancements to optimize value and performance? For example, is it more cost effective to (1) upgrade versus enhance/modify the system (usually through customization) than to (2) replace the system versus upgrade.

In addition to the monthly service costs, IT labor is required to support SaaS solutions. This is counter intuitive to the concept of subscribing and having a service delivered by an external provider. The IT labor in operations and maintenance phase comes in the forms of:

- Creating and maintaining data integration with the hosted solutions,
- Working with the provider to resolve operational issues,
- Coordinating with the business unit and vendor on system enhancements,
- Coordinating with the business unit and vendor on testing system changes.

6.3 Risks

In reviewing the risks with application subject matter experts, it has been determined that a number of risks have been mitigated downward in terms of likelihood and consequence and as a result they have been dropped. In addition, one new risk around data quality (GBS16) has been added. The risk heat map for our Critical Business Systems (CBS) and General Business Systems (GBS) is provided in Figure 6.1.

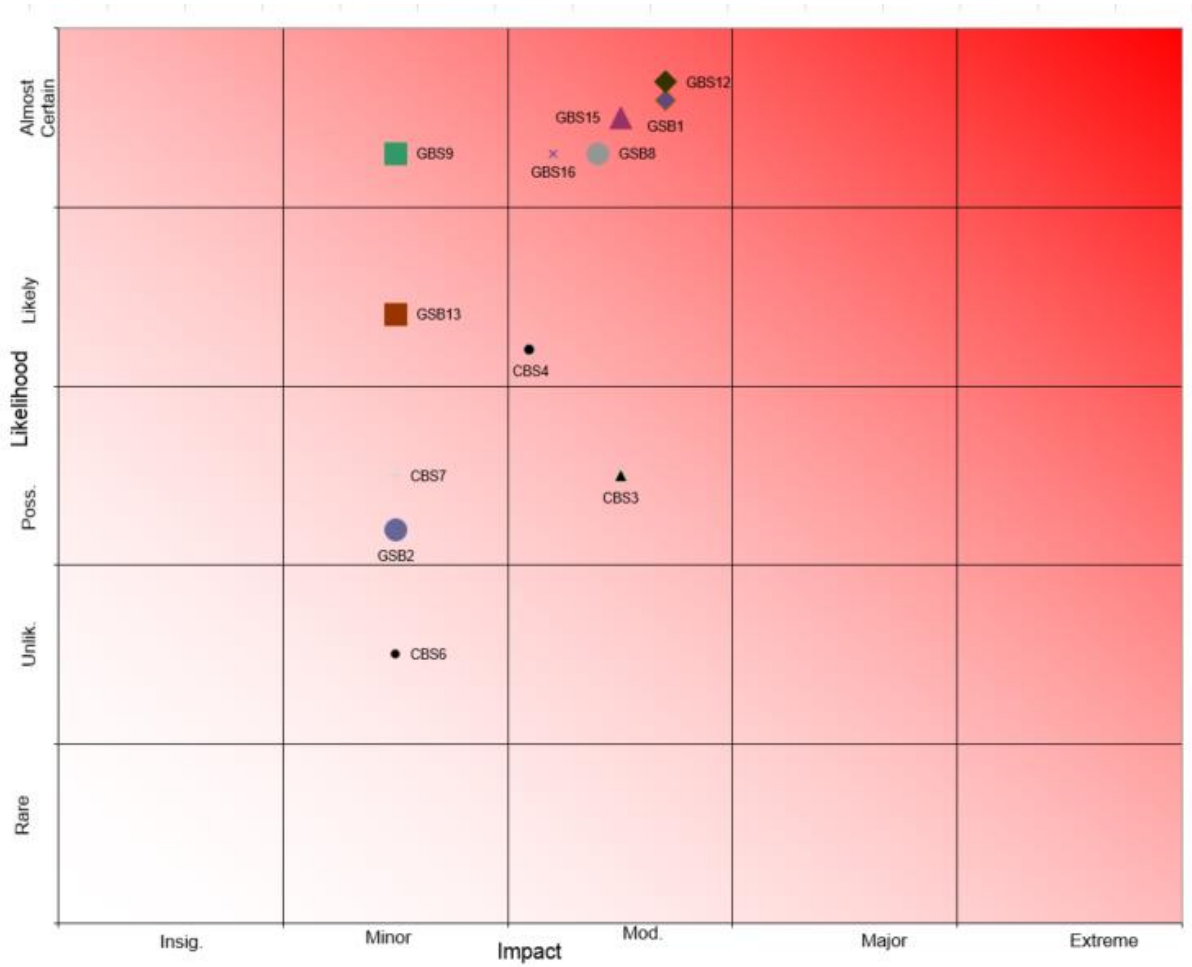


Figure 6.1: Application Portfolio Risk Map

ID	Risk		Mitigation
	Likelihood	Impact	
GBS1	Failure to fund resources to enhance systems at levels to meet business units' expectations.		• Asset Plans in PPM include operation & maintenance costs, planned enhancements, and proposed new investments. • Business cases developed for new investments; business value clearly identified.
	Almost Certain	Moderate ($1-10M)	
GBS2	Failure to implement controls which enable support teams to support development, test, and production with current available resources.		• Implement change management processes under the IVC project in the FY2015-FY2016 timeframe. • Implement a maturity framework for software development – FY2016 timeframe for non-CBS systems. • Leverage automation and tools to reduce manual activities and increase productivity – FY2016 under ITSM project.
	Possible	Minor ($100K-1M)	
GBS8	Failure to coordinate between IT and business units to ensure resources are marshalled and positioned to meet business units' current and future needs.		• Continue to work with business units to develop business cases for both capital and expense projects. • Combination of creating Asset Plans coupled with establishment of Asset Strategy has aided in mitigating this risk. • Document cost of Shadow IT and impact on IT budget.
	Almost Certain	Moderate ($1-10M)	
GBS9	Failure to position resources to address and meet emerging compliance requirements (e.g. A123, NERC CIP, eDiscovery, NIST standards, etc.).		• Recognize unpredictable workload and budget based on historical spending. • Prioritize resources to remediate issues/findings from red teams and auditors.
	Almost Certain	Minor ($100K-1M)	
GBS12	Failure to have a mechanism in place to align resources (staff, and support of service contracts) to securely and reliably maintain newly delivered systems.		• Work with APSC to ensure adequate resources are in place to cover any new service contracts and labor costs as criteria for approving a new project. • Investigate possibility of benefiting organization(s) transferring a portion of their savings to the maintenance organization to cover new expense from the delivery of new systems/applications. • Ensure new costs are in Asset Plans – IT Asset Strategy programs 8.2% of investment cost for new support.
	Almost Certain	Moderate ($1-10M)	
GBS13	Failure of business to adhere to IT processes for resource allocation and prioritization.		• Better Business alignment and strategy through the development of business roadmaps and Asset Plans. • Business acceptance of resource constraints and APSC prioritization. • Improve PMO structure around small projects.
	Almost Certain	Moderate ($1-10M)	
GBS15	Failure to a have a Software as a Service (SaaS) strategy to control costs and risks associated with adoption of SaaS services to include an exit strategy.		• Develop cloud strategy to include covering the selection, implementation, use, and exit strategy for cloud services such as SaaS. • Ensure decision to implement a cloud service includes a robust business case. • Ensure robust risk analysis performed on potential cloud services prior to adoption.
	Almost Certain	Moderate ($1-10M)	
GBS16	Lack of standards in how we manage data and data quality.		• Define data quality measures by subject area. • Continue to develop plan for the implementation of a CIM with the business. • Update/define roles around data provider and data consumer. This will help in improving discussions around data quality and the SLA's needed to support it. • Formalize the role of data stewards/data stewardship (i.e. accountability).
	Almost Certain	Moderate ($1-10M)	

Table 6.3: BPA Commercial and Enterprise Portfolio Risks

ID	Risk		Mitigation
	Likelihood	Impact	
CBS3	Failure to anticipate changes in business (e.g. Wind Integration, Sub Hourly, Dynamic Transfer, Regional Dialog, TPIP, Smart Grid, etc.) and to have resources marshalled to enable these process changes.		• Work with the business lines to anticipate market and industry changes as far ahead of time as possible. Power and Customer Services are working on developing roadmaps. • Information Owner Boards and Steering Committee are helping to mitigate this risk. • Portfolio Managers working with Information Owners to identify future business needs. • Capturing planned future activities, both capital and enhancement, in Application Asset Plan is helping to mitigate this risk; Asset Planning still needs to mature to completely mitigate this risk. Asset Plan will also identify staffing/budget levels.
	Possible	Moderate ($1-10M)	
CBS4	Failure to have adequate access to business analysts and subject matter experts to address the expanding scope of requests from business units.		• IT workforce strategy specifies the need to create and maintain a layer of permanent federal workers filling the roles of business analyst and system analyst. However, implementation of this strategy may be delayed due to priority placement of previously disadvantaged applicants.
	Likely	Moderate ($1-10M)	
CBS6	Failure to have adequate resources to support dispersed geographic locations.		• To the extent possible use remote technologies coupled with operations such as monitoring, server control, problem, incident and change detection/configuration management to mitigate the lack of on-site staff at ADC. Currently there is not enough onsite staff to operate ADC for an extended occupation. Adopting technology (e.g. VM Site Manager) has mitigated this risk.
	Unlikely	Insignificant ($0-100K)	

CBS7	Failure of Commercial Off The Shelve (COTS) and Software as a Service (SaaS) solutions to provide responsive service, adequate quality control, and continuous service.		• Use contract hold-backs as incentives for vendor to perform to BPA's satisfaction.
			• Review contracts before each renewal for possible renegotiation of the service level based on past performance of the vendor and future BPA needs. Review COTS/SaaS providers
			  • Bandwidth for providing enhancements and improvements
			  • Quality Assurance practices
			• Meet with vendor technical staff regularly to provide feedback on their performance.

	Possible	Minor ($100K-1M)	

Table 6.4: Critical Business Systems Portfolio Risks

6.4 Future Initiatives and Funding Considerations

Current and future forecast has 70% of the capital investment portfolio supporting new systems to meet compliance, policy commitments, or automated business solutions to deliver business value. As a rule of thumb, the net new annual operation and maintenance (O&M) costs (support costs, software maintenance licensing costs etc.) associated with a new system is on average 8% of the investment costs. With the current capital portfolio set at approximately $30M per year, this results in an annual growth in net new annual O&M costs of approximately $1.7M. Although the new systems automated business solutions are delivering

business value to business units and/or the Pacific Northwest, these business benefits do not directly reduce the IT operation and maintenance costs; instead, these new systems create a steady growth in the Application Portfolio's support costs.

A new trend has emerged over the last three years that needs to be accounted for in both the funding and staffing strategy for supporting the Application Portfolio (OMB directive). This trend is the adoption of Software as a Service (SaaS). This trend has IT contracting with a vendor to provide automated systems and services from the vendor owned and operated facilities. This introduces data integration, security, and funding issues that need to be carefully worked out.

Outlook:

- The Applications Portfolio is the primary driver of IT budget increases as it strives to meet regulatory and business line demands for additional automated features and functionality, while maintaining or re-imagining legacy applications.
- It is imperative that the business lines develop out-year requirements planning that aligns with Agency objectives to keep cost increases between 3% and 5% over the next ten years.

Table 1.2 and Appendix B contain a partial list of projects for this portfolio.

7.0 IT Project Management Office (PMO) Work Plan

The IT PMO Work Plan is a collection of capital and expense business technology investments and initiatives prioritized by the Agency Prioritization Steering Committee (APSC), approved by the CIO, and executed by the IT Project Management Office (PMO). The IT PMO Work Plan does not in and of itself have assets, rather assets delivered under this work plan will become an asset in either the Network, Data Center, Office Automation, or Application Portfolios.

The capital work plan capital investments have been averaging approximately $30M per year for the last four years. For the last five years approximately 40% of the investments have been for projects supporting the infrastructure sustain program (replacing servers, storage, high-end plotters, and network equipment). With the major infrastructure programs coming to completion, the sustain program will drop to approximately 20% of the capital work plan. Going forward for the next few years, 80% of the capital work plan will be delivering new systems into the Application Portfolio. New systems will result in new operations and maintenance (O&M) costs. At BPA, a new system typically has a net new annual O&M cost of 8% of the total the investment costs. At the expected capital spend rate this translates to an annual O&M growth in the Applications Portfolio of $1.9M to support these new systems.

With the infrastructure sustain program coming to completion we have some major initiatives to address key business systems that are either losing vendor support or have been in service for over 16 years and need to be re-examined to see if they are still meeting business needs. In the past two years, the PMO has been investing resources and attention in improving processes and reducing risks associated with the IT PMO Work Plan by following the Portfolio, Program, and Project Management Maturity Model (P3M3). As a result of this alignment, the IT PMO Work Plan Objectives have been updated.

Some of the major challenges facing the Work Plan include:

- Adoption of cloud based services which introduce uncertainty in costs and type of funding (expense versus capital)
- Addressing EOL systems and impact on work plan/budgets
- Tracking business value and operating costs
- Maturing to the target levels in the P3M3 maturity model
- Working with business units to understand and document long-term future automation needs

We will experience a short-term shift from an emphasis on infrastructure sustain efforts to concentrate on re-energizing aging applications to align them with more prudent and valuable asset lifecycles.

7.1 Goals, Objectives and Strategies

The IT PMO overarching strategy is focused on adopting the Portfolio, Program, and Project Management Maturity Model (P3M3) maturity framework covering project management. Table 7.2 describes our current state and the future state we are targeting for each capability in terms of the P3M3 model. The table also includes the benefits from achieving the target maturity level.

Our projects are managed and delivered in a precise and disciplined manner that promotes repeatable success strategies, and adheres to requirements and guidelines directed by the US government and the Department of Energy.

Objective/ Alignment with IT Goals	Outcomes	Status and Comments	Measures
Investments will balance the immediate needs of the business units with the overarching Agency strategic initiatives/objectives in the selection and delivery of solutions. Aligns with ITAG 3 – P ITAG 2 - S	• Selected investments span and enable achievement of BPA's strategic initiatives. • Following the SLC, capital and expense projects are sourced from asset plans and forwarded to the IT PMO for APSC consolidation and consideration. • Develop and/or buy COTS solutions that leverage and, where possible, contribute to Service Oriented Architecture and data abstraction.	 Focus and emphasis on the business case is ensuring the right IT portfolio is prioritized to meet strategic initiatives and achieve benefits. Selection of investments is maturing to include review of business benefits and measuring business benefits.	• Maintain a mapping of Capital Work Plan projects and Agency Strategic Initiatives/Objectives/Risks. Mapping will allow visualization of how portfolio is meeting Agency needs. • Perform Post investment reviews to track how well project/solution delivered on business benefit objectives.
Deliver maintainable and cost effective solutions for APSC prioritized investments. Aligns with ITAG 2 – P ITAG 3 – S	• Ability to fund future maintenance costs of a project is a decision criterion in prioritizing and approving an investment. (No project is allowed to deliver a solution that has not validated the ability to support operations and maintenance).	 APSC is now reviewing estimates of solutions' maintenance costs as project moves into execution phase and again prior to project transition to close out.	• IT asset plan accepted by IT Asset Manager and Information Solution Owner. • Track operation costs and business value to ensure business value exceeds operations costs for expansion projects.
Processes and practices aligned with industry practices to deliver secure, reliable services and quality products with the least total cost of ownership. Aligns with ITAG 4 – P ITAG 2 – S	• Projects deliver systems following the System Lifecycle (SLC), to include delivering system security plans, and adhering to FISMA controls (NIST SP 800- 53R3). • Portfolio, Program, Project Management Maturity Model (P3M3) level 3 is achieved. This includes, but is not limited to, benefit management and realization (documenting business benefits, and performing post investment review of benefits).	 We have adopted the Project Management Maturity Model (P3M3), aligning governance processes with industry practices. We are taking additional steps to improve and strengthen those processes and practices to assure the most effective TCO that can be achieved.	• Move PMO capabilities from current state to future state (level 3 in P3M3 for Portfolio Management, Program Management, Requirement Management, and level 4 for Project Management).

Table 7.1: IT PMO Work Plan Objectives

Portfolio Strategy	Benefits	Challenges/Issues	Asset Portfolio Outlook
Adopt and advance along Portfolio, Program, and Project Management Maturity Model (P3M3).	• Replace the 9 in-house cuff systems with 1 COTS system. • Risk management model with costs directly associated with likelihood, impact, and severity. • Decrease turnover and better align skillsets with project staffing needs.		• Implemented tool to improve portfolio management. • Continuing to work towards achieving targeted levels in P3M3 maturity Model
Mature Requirement Management.	• Aids in solidifying scope. • Assists in business transformation planning. • Reduces risks.		• Implemented requirements management tool; tool is being used by all projects.

Table 7.2: IT PMO Work Plan Strategies

7.2 Asset Current State and Accomplishments

We have reduced the annual capital expenditures from an average of $40M/year (FY2011-FY2013) to an annual capital program of approximately $30M (FY2014-FY2017). The major accomplishments of the IT PMO Work Plan can be summarized as:

- In FY2014 we delivered 20 go-live projects.
- In FY2015 we completed 13 projects in the Capital Work Plan.
- In FY2016 there were 17 projects approved to continue, Capital Work Plan continues to complete a high number of projects to support critical Agency business objectives.
- In order to mature our analysis of business benefits and business cases in general, we now require that business owners and information system owners develop a set of measurements to capture actual versus projected benefits from deployment of new systems. Results are reported back to the APSC.

7.3 Risks

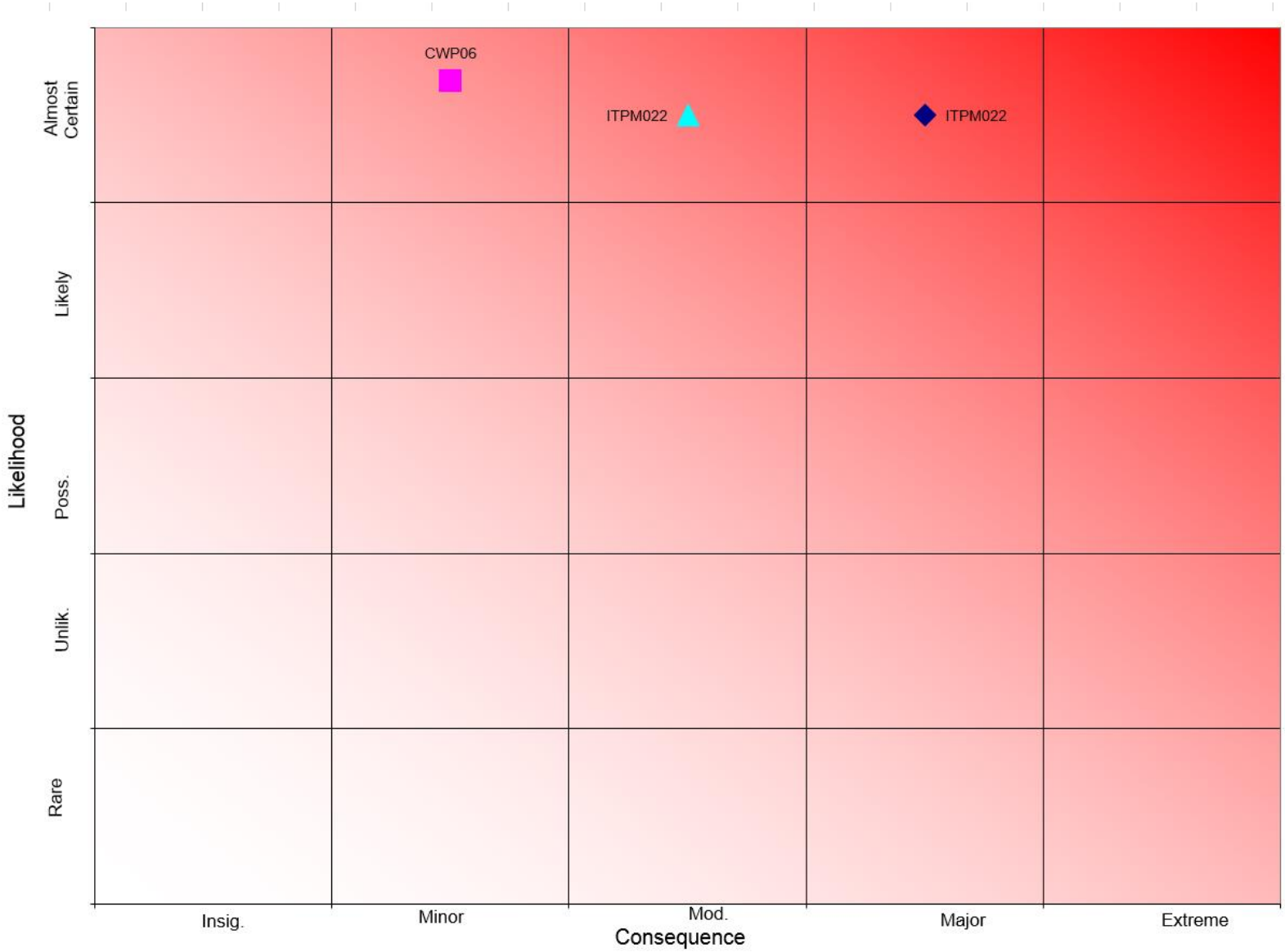


Figure 7.1: Capital Work Plan Risk Map

ID	Risk		Mitigation
	Likelihood	Impact	
CWP06	Failure to assure increased O&M expense budget for post-delivered project systems.		Provide a formal mechanism for O&M recipients to properly reflect budget changes needed to support newly delivered projects. This should include any work necessary to decommission existing applications/systems being replaced by the new delivery.
	Almost Certain	Minor ($100K - $1M)	
ITPMO22	Failure to fully scope and accurately estimate the Business Information Systems costs to inform the FY2018/2019 rate cases.		Finance will lead stakeholders in a yearlong road mapping and scoping effort for the Business Information Systems which include our Enterprise Resource Planning systems. The cost will vary greatly depending on whether key systems need to be upgraded, replaced or migrated to software-as-a-service. The variance in costs will range from a low of $20M to a high of $100M. The road mapping and scoping effort will not be completed until EOY2016.
	Almost Certain	Major ($10M - $100M)	
ITPMO21	Failure of software development to mature at a comparable level to the PMO hinders IT's ability to effectively execute on new capabilities, and deliver on mission critical investments, while balancing the demands of operating and maintaining production systems.		Partner with software development on a maturity model (e.g. CMMI, ITIL) to measure progress. Another mitigation is to separate development and production management.
	Almost Certain	Moderate ($1M - $10M)	

Table 7.3: IT PMO Work Plan Risks

7.4 Future Initiatives and Funding Considerations

Refresh of key business systems beginning in FY2017 may drive our annual capital program back towards $40M per year for FY2018-FY2020. With major infrastructure sustain projects coming to completion, we are projecting a reduction in capital spending on core sustain for the next few years and will be addressing a backlog in business automation projects.

We are actively working to widen the planning horizon to seven years, which is very challenging for information technology solutions. The drivers behind widening our planning horizon include enabling us to better:

- Align investments with Agency initiatives,
- Identify and validate business value/benefits for each investment,
- Plan for any necessary business organization change,
- Identify connections and dependencies between investments,
- Marshal and plan resources to implement solutions, and
- Forecast our budget requirements.

We have just begun taking our first steps in examining a broader planning window. We are aligning our efforts with the Agency's Capital Planning and Asset Strategy initiatives. In particular, we are using and maturing each of our Asset Categories' Asset Plans to estimate out-year investment requirements. To be successful in this approach, we must partner and become strategic partners with the various business units throughout the Agency. We are leveraging our PMO Portfolio Managers, our operations managers, and our IT Asset Manager to engage with our business partners to help them articulate their future business needs and to capture them in the Asset Plans. We are forming joint strategy teams with our internal business partners to address topics from Enterprise Systems to data quality to business intelligence.

The results of partnering with our business units and maturing our asset plans are the major Capital Work Plan Initiatives detailed in Table 3.3 through Table 6.3**.**

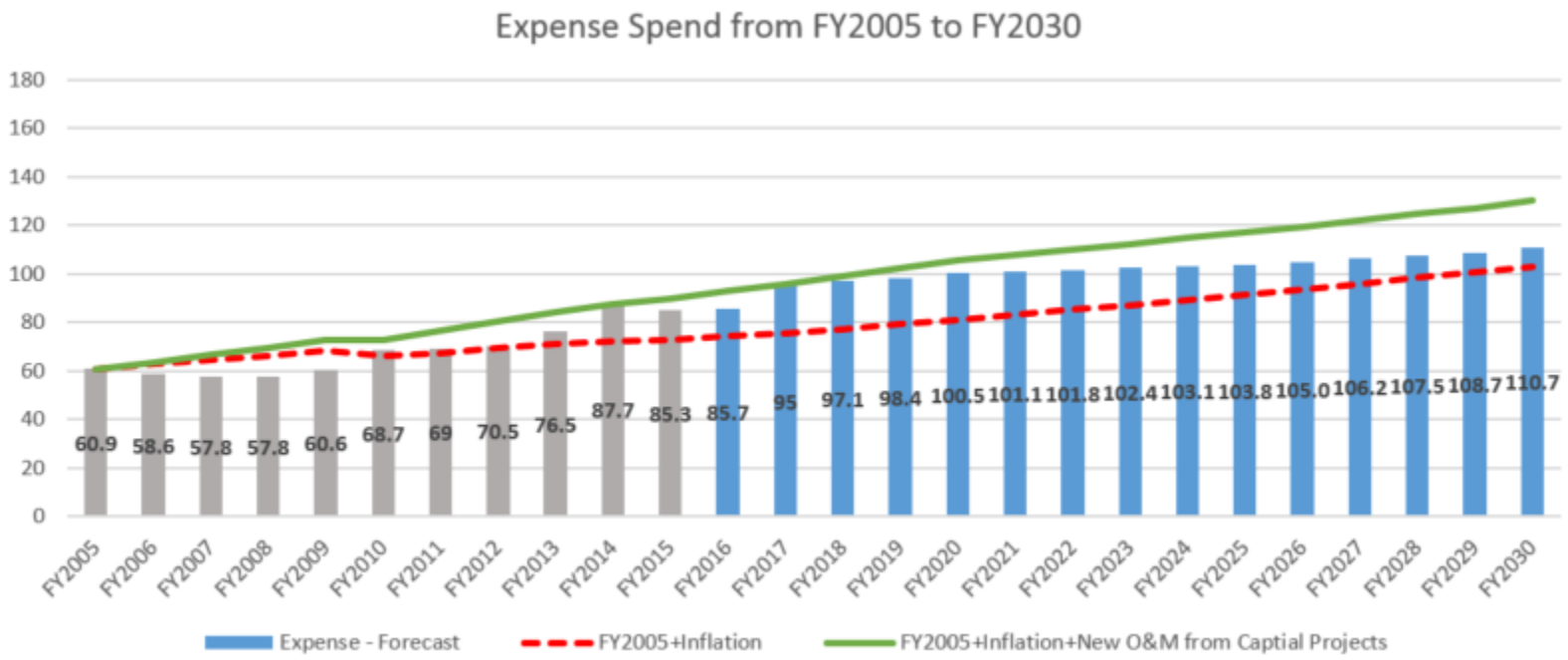
There is also a great deal of uncertainty around costs of an investment, especially until we have time to understand business needs and requirements, have gone through analysis of alternatives, and selected a solution. As we go through these phases, we are able to reduce the uncertainties around the investment in terms of both timing and budget.

Another example of where we encounter uncertainty is in projects like Business System Disaster Recovery. Although we have begun planning on this FY2016 project, there are a range of possible solutions that have significant difference in both the cost and type of funds needed to execute. These alternatives range from using cloud-based IaaS (this would be an expense funding requirement) to host our disaster recovery capabilities, to building on premise redundant system capabilities that require a large capital funding component.

Additional uncertainties that can impact our projections include:

- Emerging compliance requirements
- Mitigation requirements for emerging security threats
- Rate at which cloud based solutions are adopted, which has an impact on whether to use expense versus capital

Appendix A: Historical and Projected Expense Profiles



Appendix B: FY2017-FY2019 Projects

	2016	2017	2018	2019	2020
Infrastructure	**$ 2.5**	**$ 13.1**	**$ 16.4**	**$ 7.0**	**$ 6.0**
DMZ Virtualization		$ 1.7	$ 1.7		
Business Systems DR		$ 6.5	$ 6.5		
Network Client Connectivity	$ 2.5	$ 0.9			
Infrastructure Refresh/Simple Capital		$ 4.0	$ 8.2	$ 7.0	$ 6.0
Corporate	**$ -**	**$ 2.4**	**$ 5.8**	**$ 4.0**	**$ -**
IT Service Management		$ 0.9	$ 1.4	$ 2.4	
Hyperion Replacement		$ 1.3	$ 0.6		
Structured Data Management		$ 0.4	$ 2.0		
Customer Portal		$ -	$ 0.8	$ 0.8	
Facilities CMMS		$ 1.0	$ 1.0		
Procurement Compliance Infrastructure		$ 2.9	$ 0.8		
Safety & Health Analytics		$ 0.9	$ 0.9		
Asset Suite Upgrade	$ -	$ 0.7	$ 2.3	$ 0.5	
Billing Information System Replacement	$ -	$ 1.7	$ 3.5	$ 3.5	
Power	**$ 3.1**	**$ 4.5**	**$ 2.7**	**$ 3.5**	**$ -**
Pisces Web	1.5	1.6			
Outage Tracking Systems	$ 0.4	$ 0.9			
Treaty non Treaty	$ 1.2	$ 0.1			
Solar Forecasting Rebuild			$ 1.0	$ 2.0	
CAISO Replacement		$ 1.1	$ 0.2		
CBS Data Re-Architecture		$ 0.8	$ 1.5	$ 1.5	
Energy Efficiency (Post Focus 2028 Disc)		TBD	TBD	TBD	
Market Evolution Work		TBD	TBD	TBD	
Demand Response (Post Demonstration, Post-Auto grid)		TBD	TBD	TBD	
Weather Application Refresh		TBD	TBD	TBD	

Transmission	**$ 1.9**	**$ 5.8**	**$ 19.3**	**$ 15.1**	**$ 6.2**
Vegetation Management Systems	$ 1.9	$ 0.4			
Transmission Field Scheduling System			$ 1.5		
RAS Data Management		$ 0.3	$ 0.4		
Fiber Management System		$ 0.1	$ 1.7		
Radio Frequency Management				$ 0.1	$ 0.2
Simulation Analysis		TBD	TBD	TBD	
Transmission Revenue Forecast System		$ 0.6	$ 1.0		.
Transmission Estimating System Replacement		$ -	$ 0.5	$ 2.0	
Stream System Improvement		TBD	TBD	TBD	
NERC CIP 5 Access Control		TBD	TBD	TBD	
Real Property Enterprise System			$ 1.5	$ 3.0	$ 1.5
Network Model Manager		$ 1.1	$ 2.0		
Asset Information System		$ 1.5	$ 2.5	$ 3.5	$ 2.5
Replace/Eliminate Chess		$ 0.5	$ 2.0		
ATC Optimization Scenario Management		$ 0.1	$ 0.8	$ 0.1	
Substation Predictive Analysis		$ -	$ 0.5	$ 1.5	
ATC Opt Measurement Analytics			$ 0.9	$ 2.1	
Substation Design Automation			$ 0.8	$ 1.3	
TAPM Replacement Asset Portfolio		$ 0.5	$ 1.5	$ 0.5	
Cascade Upgrade				$ 1.0	$ 2.0
TCIS Netcracker		$ 0.8	$ 1.8		
Replace EOL Systems		TBD	TBD	TBD	
Anticipated New Projects		$ 5.0	$ 6.0	$ 8.0	
Business Information Systems		$ 5.0	$ 10.0	$ 12.0	$ 12.0
Commercial Operations		TBD	TBD	TBD	TBD
Total Capital Request		**$ 35.70**	**$ 60.12**	**$ 49.61**	

Appendix C: Refresh Rates

Infrastructure Category	Refresh Rate
Servers	5 years
Storage (SANs and Fabric)	5 years
Desktop	5 years
Laptop	5 years
Thin Clients	7-10 years
Tablets	3 years
Network Printers	5 years[1]
Network devices	7 years
Wireless devices	
Cable Plant	14 years

Table C.1: Refresh Rates

[1]We have transitioned to managed print services. Under this arrangement we will lease the printers and the printers will be refreshed as part of the managed services

Financial Disclosure

This information was made publicly available on June 10, 2016 and contains information not sourced directly form BPA financial statements.