Florida
Agency for State Technology

4050 Esplanade Way
Tallahassee, FL 32399-0950
Tel: 850-412-6050

Rick Scott, *Governor*

Jason M. Allison, State CIO and *Executive Director*

Agency for State Technology

September 30, 2015

Cynthia Kelly, Director
Office of Policy and Budget
Executive Office of the Governor
1701 Capitol
Tallahassee, Florida 32399-0001

JoAnne Leznoff, Staff Director
House Appropriations Committee
221 Capitol
Tallahassee, Florida 32399-1300

Cindy Kynoch, Staff Director
Senate Committee on Appropriations
201 Capitol
Tallahassee, Florida 32399-1300

Directors:

Pursuant to Chapter 216, Florida Statutes, the Agency for State Technology's (AST) Long Range Program Plan (LRPP) is submitted in the format prescribed in the budget instructions. The information provided electronically and contained herein is a true and accurate presentation of our mission, goals, objectives and measures for the Fiscal Year 2016-17 through Fiscal Year 2020-21. This submission has been approved by Jason M. Allison, Executive Director and Chief Information Officer (CIO) for the State of Florida. The LRPP is published at: http://ast.myflorida.com.

Sincerely,

Jason M. Allison, CIO/Executive Director
Agency for State Technology

Agency for State Technology

LONG RANGE PROGRAM PLAN

FISCAL YEARS 2016-2017

THROUGH 2020-2021

Jason M. Allison, Executive Director/
Chief Information Officer
Agency for State Technology

Mission

Achieving Success through Technology.

Agency for State Technology

Long Range Program Plan

FY 2016-17 through FY 2020-2021

Agency Mission, Goals and Linkage to the Governor's Priorities

The Agency for State Technology (AST) was established July 1, 2014 by Chapter 2014-211, Laws of Florida. The law created a state Chief Information Officer (CIO) within the executive branch, established an enterprise information technology governance structure, and transferred two of the state's primary data centers (Northwood and Southwood) into the State Data Center under the authority of the state CIO. AST is directed to:

- Develop and implement information technology (IT) architecture standards,
- Establish IT project management and project oversight standards,
- Perform project oversight on IT projects with total costs of $10 million or more for executive agencies,
- Perform project oversight on any cabinet agency IT project that impacts another agency and has a total project cost of $25 million or more,
- Collaborate with the Department of Management Services on IT procurements,
- Provide operational management and oversight of the State Data Center,
- Identify opportunities for standardization and consolidation of IT services that support common business functions, and
- Recommend additional consolidations of agency data centers or computing facilities.

The AST Long-Range Program Plan (LRPP) is performance-based, with a five year planning outlook, to establish agency priorities and achieve its goals. All current and ongoing activities and performance have been reviewed and evaluated related to the AST's statutorily mandated mission. AST provides data center services, strategic guidance to state agencies related to their IT systems, project assurance oversight, and enterprise security protocol direction.

Mission	Achieving Success through Technology
Vision	To be the national leader in government technology
Guiding Principles	Deliver SERVICE that is: Strategic. Enterprise focused. Reliable. Value-adding. Innovative. Collaborative. Efficient.
Values	Enterprise-wide Service Organization Standardized Self Improving Process Get it Right the First Time Remove Single Points of Failure Optimize the Organization

Stakeholder and Customers	
The Governor and staff	Technology Advisory Council
Elected members of the Legislature and staff	Vendors of the State of Florida
State employees	State agencies and eligible entities
Citizens of the State of Florida	

AST Goals

Goal 1: To protect at the highest level the confidentiality, integrity, and availability of state IT resources by adopting a standardized cybersecurity framework and creating guidance artifacts.

Goal 2: To develop and deliver strategies that improve situational awareness for information technology threats and risk.

Goal 3: To deliver and assist state agencies with project management and oversight standards to increase success in agency IT projects.

Goal 4: To deliver high uptime availability for the State Data Center

Agency Service Outcomes

And Performance Projection Tables

Goal 1: To protect at the highest level the confidentiality, integrity, and availability of state IT resources by adopting a standardized cybersecurity framework and creating guidance artifacts.

Objective A: Develop risk-based rules, standards, and guidance for IT security by promoting standardization and consolidation of technology services that support state agencies. Security guidance may include: interpretation of certain parts of the security rule; template policies, procedures or guidelines; standards; or other more detailed guidance publications.

Outcome: Number of security guidance artifacts published

Baseline Year (FY 2015-16)	FY 2016-17	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21
TBD	2	4	6	6	6

Goal 2: To develop and deliver strategies that improve situational awareness for information technology threats and risk.

Objective A: Embed continual improvement into situational awareness campaigns so that the workforce supporting the State's mission is informed and more resilient to cyberattacks.

Outcome: Number of trainings for agency Information Security Managers (ISMs) and partners on cyber threats and security management practices.

Baseline Year (FY 2015-16)	FY 2016-17	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21
TBD	10 ISM meetings & 1 Special Workshop	10 ISM meetings & 1 Special Workshop	10 ISM meetings & 2 Special Workshops	10 ISM meetings & 2 Special Workshops	10 ISM meetings & 2 Special Workshops

Goal 3: To deliver and assist state agencies with project management and oversight standards to increase success in agency IT projects.

Objective A: Offer training to agencies through discussions at regularly held meetings (Chief Planning Officer (CPO)/Project Management Office (PMO) Roundtable).

Outcome: Number of project management trainings

Baseline Year	FY 2016-17	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21

(FY 2015-16)					
TBD	4	5	5	5	5

Goal 4: To deliver high uptime availability for the State Data Center

Provide efficient and reliable infrastructure and services. The state will use a reliable technology infrastructure and efficiently provide shared services in the State Data Center. These services are essential to support the state's data securely. AST, on an ongoing basis, will monitor the services for sustainability and cost reductions, whenever possible.

Objective A: Provide operation management and oversight of the State Data Center.

Outcome 1: Data Center Facility Uptime Availability

Baseline Year (FY 2015-16)	FY 2016-17	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21
99.8%	99.85%	99.9%	99.9%	99.9%	99.9%

Outcome 2: Percent of established Service Level Agreement (SLA) goals at or above target

Baseline Year (FY 2015-16)	FY 2016-17	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21
78%	89%	92%	95%	98%	100%

Agency for State Technology

Long Range Program Plan

FY 2016-17 through FY 2020-2021

Linkage to Governor's Priorities

AST's LRPP builds on the Governor's priorities of accountability budgeting and reduction of government spending by leveraging technology to enable a more innovative, efficient, and sustainable government. The plan also builds on the Governor's priority of focusing on job growth and retention by concentrating on the objective of maintaining an information technology workforce that is skilled, capable, and agile to ensure the state can deliver effective government technology services and solutions now and into the future. Additionally, a well-run state will lead to Florida creating a pro-business climate resulting in both business and job growth.

Trends and Conditions Statement

Technology is rapidly becoming more accessible and useful in every facet of modern life. This is due in large part to the broad access to powerful applications provided through elegant interfaces on inexpensive devices. This modernization of technology has created an environment where citizens are accustomed to instant, convenient access to the information and services that they need.

As government attempts to keep pace with the expectations of its constituents, it is often faced with challenges that slow the improvement of existing approaches for delivering services. Many of these challenges are due to the persistent desire to increase the efficiency and lower the cost of providing government services. Other challenges include ensuring that the information entrusted to the stewardship of the state is protected from increasingly sophisticated and persistent security threats.

As technology products mature, they have become increasingly dependent on centralized, shared services provided by private entities commonly referred to as “cloud” services. These services provide opportunities for the government to modernize service delivery while minimizing the risk and cost of the traditional approach of creating custom applications.

This section focuses on trends in both the market and in technology advancements that have the potential to provide long term cost reduction through efficiencies. It also highlights some risks associated with emerging trends.

Negative trends

a. Risk aversion and limited budgets have slowed the pace of application modernization within state agencies. While it is acceptable for a privately owned business entity to attempt service development or modernization only to be met with failure, typically government entities are more reluctant to assume risk, which paradoxically increases the cost of implementing new services.

b. The information held by the state has tremendous value both publicly as well as across agency boundaries. Unfortunately, much of this data is currently not freely accessible by other state agencies or the public, limiting the utility and opportunities to leverage the information. This is not based on an unwillingness to share the information that is public. Instead, this is often the result of a lack of information necessary to catalog and manage the information available.

c. The recruitment of highly technical positions required to support the information technology needs of state government is sometimes difficult within the confines of state salaries and benefits packages. Further, the retirement of staff with institutional knowledge leaves severe gaps in application support areas, making it more difficult to operate existing systems and creating even greater risks in developing strategies for replacement. To be successful, organizations must have the flexibility to attract and retain skilled workers.

d. The product life of many of the state's legacy systems has been forced to be extended and major application redevelopment efforts are starting to queue up. These efforts will have high cost and the complexity of the efforts is exacerbated by a lack of internal knowledge resources.

e. The state needs a comprehensive plan that contains an enterprise view for application development efforts that includes the opportunities for data sharing and system component reuse. Better planning can reduce potential duplication of hardware/software and can result in lower costs.

f. Complexity of data center operations demands greater documentation and policies/procedures that focus on best practices. Due to the age of many of the critical legacy components in the environment and their highly prioritized requirements for nonstandard support, it is difficult to develop process maturity, which endangers operational efficiency and continuous performance improvements.

g. How government approaches outsourcing should be in direct correlation with how much risk can be tolerated. Long-term commitments with uninterrupted renewal periods, the expectation of reduced costs, and running managed services beyond their supported life cycles, all increase exposure to risk and does little to mitigate the eventual financial impact. It is vitally important for the state to explore these opportunities. However, the state has a need for clear entrance criteria and an exit strategy to ensure the long-range protection of operations.

Positive Trends

a. The consolidation of platforms and services in the marketplace is driven by cost containment/reduction and efficiencies in operation. Florida began its approach with data center consolidation. Today, as the marketplace continues to expand into the cloud, it will be necessary to examine appropriate use cases and governance for leveraging these resources.

b. Standardization of hardware and software will lower the overall cost of ownership and create consistency in service levels. AST must set architecture standards in order to achieve the greatest advances in savings. This is a long and iterative process that begins with new projects and runs concurrent with hardware and software reinvestment cycles.

c. Tough competition in the vendor communities for the fewer, often larger state IT acquisitions and projects results in better competition and better pricing for the provision of goods and services.

d. Continuous advances in technology provide opportunities for greater versatility, flexibility, productivity, and customer service.

e. Modern equipment is more energy and space efficient which reduces operating and cooling costs and increases scalability of the State Data Center by providing efficient use of expensive raised floor data center facilities.

f. Storage space is becoming exponentially less expensive, which accommodates the continuously increasing demand for data storage within existing spending levels.

g. Significant effort has been made in the area of security programs with solid security protocols and software that allow for protection of the state data systems. These programs provide the greatest defense, containment, and mitigation strategies.

h. The computer industry now produces a vast array of devices: tablets, smart phones, servers, storage systems, networking equipment, and computer-embedded industrial products. A host of new technologies can be integrated and applied to solve business problems.

i. Data analysis tools are maturing, which will provide opportunities for the state to manage data as an asset through identifying common identity and data elements across disparate systems, creating federated data models for reporting and analysis, and laying the foundation for shared repositories of common data elements. Strong governance is needed to effectively manage data as an asset, and a diverse group of stakeholders must be involved in decision-making processes to ensure data will not be compromised. This can be achieved through clear data sharing and privacy agreements.

j. Technologies now allow for new ways to address common business needs across organizations. State entities with similar needs can work together in a collaborative environment to identify, analyze, and apply common tactics to solve common problems. When employed, the result has been effective organizational business practices and sharing of appropriate technology to solve issues at an enterprise level.

k. IT services are now readily available on the open market "as-needed". The cost of services are quite reasonable, when compared with traditional procurements, with payments correlated directly to consumption. The dynamic nature of these services allows customers to rapidly provision or change services based on business requirements. Additionally, customers benefit from "trying before buying" since large, up-front, capital investments are no longer needed. As marketplace offerings develop through the shared services model, the AST can facilitate the ability of organizations to take advantage of mature and stable enterprise IT solutions.

Cloud

To assist in planning, some analysis of existing and emerging technology trends in the marketplace has been undertaken, including evaluating technology advancements to determine their possible applicability to the delivery of services.

Hybrid Clouds & Service Brokering

The industry is continuing to see traditional on premises data centers like the AST SDC evolve to becoming IT service brokers by integrating third party cloud services into their on-premises' private cloud, becoming a hybrid cloud. IT service brokers offer hybrid cloud services to their customers. In a hybrid cloud service, a qualifying customer application may be run within an on premises private cloud,

or an off premises cloud provided by a third party. The IT assets can freely move between the on premises and off premises clouds as requirements change. Qualifying applications are mapped to the cloud environments based upon considerations of cost, risk, and performance.

Converged Infrastructure

Converged infrastructure combines IT infrastructure that traditionally was offered as stand-alone products. That is, data centers typically purchased storage, compute and network components from various hardware vendors and then integrated the components into solutions capable of running customer applications. Converged infrastructure offerings provide pre-integrated solutions from a vendor and offer opportunities for cost savings and operational efficiencies through reduction in complexity. It is anticipated that these offerings will continue to mature and become more mainstream over the coming years.

Converged infrastructure represents the cooperation between multiple vendors (or multiple business units of a single vendor) to develop a tested, predictable, and supportable hardware and software environment to run customer applications. The packaged nature of these environments limit the number of configuration and integration options; however, this predictability is necessary to optimize support and performance. Although procurement costs are similar to the costs of purchasing the individual components, operational efficiencies are possible provided that the converged infrastructure represents a large enough proportion of the total environment. Otherwise, it too must be integrated with the rest of the systems, adding to the variety.

Initiatives and specific technologies

The following is a focus on initiatives and specific technologies that will influence the services provided by the AST and are included in the examination for opportunities for change or expansion. This list is not all encompassing, but instead is made up of some of the lead technologies meriting continued or additional attention:

1. Software as a Service (SaaS)
2. Infrastructure as a Service (IaaS)
3. Platform as a Service (PaaS)
4. IT Security Frameworks
5. Data Center Security
6. Consolidation of AST North and AST South Data Center locations
7. IT Service Management
8. Data Center Interconnect (DCI)
9. Server Virtualization
10. Disaster Recovery

1. Software as a Service (SaaS)

SaaS is a broad term used in today's computing environments where technology advances have enabled the remote operation and support of various vendor-offered application solutions that generally

operate in the cloud. These solutions promise to provide business functionality and support on a broad spectrum of offerings, including flexibility of the hardware environments usually through the acquisition of a service.

Current Environment

At present, most data center customers own, operate, and support their various support applications themselves (even if hosted in the State Data Center). They provide for ongoing support and maintenance of those applications through individual application development work units and network support staff. In some cases, these are supported in part or in whole by consultant/contractor resources. In other cases, certain applications are outsourced for operation by vendor services through individual contracts with cloud vendors.

Evaluation of SaaS

SaaS is a vendor-offered solution that is shared across many customers (multi-tenant), thus reducing the overall operating costs and returning this value back to the customer. SaaS solutions often provide more options, respond to market forces quicker, and provide faster development than the traditional sustaining engineering process. Any candidate application for replacement by a SaaS solution must be independently evaluated for "fit for purpose" on a strictly case by case basis to ensure its appropriateness.

SaaS solutions fundamentally concentrate on standardized business best practices and typically are simpler applications of the general business rules. Generally, SaaS is much less expensive than building a custom solution or on premise implementation. Since the products are built 'generically' to satisfy the needs of many customers, sometimes they do not meet the particular needs of every customer. While offerings do allow for "some" customization to individual requirements, it is important to maintain a balance, as over-customization of SaaS products presents a hazard potentially excluding the product from automatic upgrades and releases which is an important contributing factor to the reduced cost over the product lifecycle (without the flexibility of upgrades, the value of the product will diminish faster over the product lifecycle).

Recommendations for SaaS

A framework for decision making needs to be developed to objectively determine what is in the best interests of the state. SaaS solutions should be pursued wherever their fit for purpose can be deemed appropriate while ensuring that due diligence is taken to safeguard expectation management and budgeting.

Strategies for SaaS

- Identify pilot candidates for replacement
- Canvas marketplace for potential opportunities and capabilities
- Develop a process and procedure for adequate evaluation and ROI (Return on Investment)
- Pilot applications
- Develop contracting mechanisms to take advantage of the marketplace in this space

2. Infrastructure as a Service (IaaS)

IaaS refers to vendors offering solutions through pre-defined sets of hardware components utilizing the Internet for connectivity. Generally speaking, these services (primarily compute and storage services) are developed specifically with the idea of providing these services through an Internet connection where the end-user has no responsibility for any maintenance of the hardware or operating systems and only requires an Internet connection with sufficient bandwidth to address their particular application and data needs. These solutions provide infrastructure functionality and support on a broad spectrum of offerings. As with SaaS, IaaS custom components can be expensive and often may reduce their value over time, but standard environments can be cost-effective.

Current Environment

At present, most agencies obtain their infrastructure support from the State Data Center (operating as an IaaS provider to state customers). The State Data Center provides ongoing support and maintenance of those hardware components through platform work units and network support staff, and in some cases, augmented by consultant/contractor resources. Several state customers are pursing IaaS services in the cloud using contracts administered by the State Data Center.

Evaluation of IaaS

Cloud computing provides a scalable online environment that makes it possible to handle an increased volume of work without additional impacts to performance. There is often no hardware or software installation required, and there is a reduction in the manpower and skill support requirements of in-house infrastructure.

Cloud deployments are built on a robust architecture providing resiliency and redundancy, and they can be accessed via nearly any electronic device that connects to the Internet. There are additional cost offsets when cloud-based storage, electricity, infrastructure, and five year hardware refresh costs are considered in the cost/benefit estimation.

Recommendations for IaaS

IaaS solutions should be pursued when their value as a more efficient and effective solution can be objectively determined. Careful analysis and due diligence must be taken to ensure that business expectations are met and sufficient ongoing budget is identified.

3. Platform as a Service (PaaS)

PaaS refers to a vendor hosted application framework within which custom applications can be developed and deployed. This type of cloud service has the potential to reduce the cost and risk associated with custom application design and development by providing modern, tested, and reliable software modules that have the flexibility found in traditional development frameworks without the complexity and cost of creating and hosting them manually.

Current Environment

At present, most agencies elect to leverage local development environments and tools. This approach offers the most flexibility with application design, but it requires a high level of diligence to ensure that the final product is secure, stable and meets the stated requirements.

Evaluation of PaaS

Evaluating a potential PaaS development environment is typically driven by the available skill set within the agencies and associated contractors. This, in combination with the application design requirements will help determine if the PaaS environment being evaluated is a good fit. The need to support integrations with related applications or the ability to leverage existing developed code should also be a factor in the decision

4. IT Security Frameworks

Information technology security planning is the responsibility of every organization in state government and running an effective information security program is challenging. Mandatory compliance with the numerous regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Criminal Justice Information Services (CJIS) policy, and Sarbanes-Oxley (SOX), just to name a few, requires careful consideration and dialogue in all government program areas.

Current environment

Each agency has a designated Information Security Manager and there are compliance requirements established by the former Agency for Enterprise Information Technology for agencies to follow that provide minimum assessments of IT security status and risk. In collaboration with the Department of Law Enforcement (FDLE), the AST is responsible for developing and implementing a process for detecting, reporting, and responding to information technology security incidents, breaches, and threats.

Evaluation of IT security frameworks

An IT security framework is the foundation for an effective, enterprise-wide security program. It is a code of practice and principles that includes process, policy, and procedures used to protect and govern information security. The framework is a method of establishing, implementing, reviewing, maintaining, and improving the security programs throughout state government.

Some IT security standards lack specific technical detail and guidance, but provide an overall program structure and the security management guidance that is necessary to implement and maintain an effective security program. Assessing, executing, monitoring, and auditing security programs using existing, proven security frameworks can strengthen security posture and support compliance with multiple regulations. Common security frameworks include International Organization for Standardization (ISO), Control Objectives for Information and Related Technology (COBIT), Committee of Sponsoring Organizations of the Treadway Committee (COSO), National Institute of Standards and Technology (NIST), and Health Information Trust Alliance Common Security Framework (HITRUST CSF).

Recommendations for Security

There are no “silver bullet” (simple) solutions for today’s complex environments. Layered security defenses include a series of different defenses each used to cover the gaps in the others' protective capabilities. Through the application of firewalls, intrusion detection systems, malware scanners, integrity auditing procedures, and local storage encryption tools, a layered security model can serve to protect information technology resources in ways that others cannot.

Strategies for Security

- Evaluate new and available security technologies
- Review and address security enhancements to new and ongoing IT initiatives
- Partner the State Data Center with FDLE and other state agencies to work toward effective enterprise security solutions
- Employ software tools to enable cyber hardening and to provide for the assessment, detection, control and remediation of security threats

5. Data Center Security

Securing IT assets continues to be a top priority of data centers worldwide. Attacks targeting valuable IT systems and their data continue to proliferate and the sophistication of these attacks continues to increase. Data centers work to deploy counter-measures to thwart these increasingly complex attacks. Traditional IT security tools do not provide adequate protection for emerging threats. Hacktivists, malware, zero-day exploits, and a proliferation of blended threats are using multiple attack vectors that are not detectable by existing security toolsets. The shortcomings inherent to traditional cyber-security tools creates a significant risk to Florida's ability to protect the confidentiality, integrity, and availability of information technology resources. As a result, state agencies cannot properly protect IT resources without implementing adaptive threat monitoring and response tools and services. These tools and services must be capable of detecting advanced threats used by cyber-criminals and address the increasing number of sophisticated attacks by well-trained state-sponsored hackers from adversarial nations and highly motivated hacktivist groups.

6. Consolidation of AST North and AST South Data Center Locations

The AST State Data Center (SDC) currently operates in two locations, AST North (formerly the Northwood Shared Resource Center, or NSRC) and AST South (formerly the Southwood Shared Resource Center, or SSRC). In 2015, the AST SDC will launch a series of projects to begin transferring people and technical assets from the AST North to the AST South. The AST SDC will work with the customer agencies during this transition to ensure that service levels are met. It is expected that this transition will be completed by the spring of 2018.

7. IT Service Management

As IT products become increasingly commoditized, it is imperative that data centers differentiate themselves by offering consistent, effective and efficient services. The creation and supply of these holistic services is increasingly being achieved through IT service management standards and best practices. By the application of modern, proven management techniques these practices ensure that customers of the data center receive high quality IT services at the lowest possible cost. Additionally, these practices help to mitigate risks associated with the provision of IT services.

8. Data Center Interconnect (DCI)

DCI technology is used to extend LAN (Local Area Network) and SAN (Storage Area Network) connectivity and provide accelerated, highly secure data replication, server clustering, and workload mobility between geographically dispersed data centers. This technology is also used to merge local infrastructure with third party IaaS platforms to facilitate building "hybrid" cloud environments, which reduces costs by migrating non-critical workloads to less expensive service tiers.

Current Environment

The existing connections between the Northwood and Southwood, State Data Center locations are routed (layer 3), not dedicated to data center interconnection. This prevents the State Data Center from migrating services between its locations, which would provide enhanced redundancy and disaster recovery capabilities as well as improving service provisioning through the ability to transparently provide services to any customer from either State Data Center location based on available capacity. The AST has ordered the equipment necessary to establish connectivity between the Data Centers, additionally, work is underway to establish the physical fiber connection between the Data Centers.

1) Path Forward

Work will continue on both the physical plant modifications, as well as the installation and configuration of the network equipment necessary to complete the interconnect. This will be followed by testing and tuning to ensure high reliability and throughput.

2) Utilization

The State Data Centers begin migration efforts of the virtual infrastructure from the North facility to the South facility as well as cross pollination of compute and storage at both facilities to reduce the overall operational costs.

9. Server Virtualization

Server virtualization refers to the creation of a virtual machine that acts like a physical computer with an operating system. Software executed on these virtual machines is separate from the underlying hardware resources, creating flexibility and mobility in its provisioning. In order to facilitate other important efforts (i.e., data center interconnect, disaster recovery), server virtualization is a prerequisite.

Current environment

Server virtualization has been a technology used to consolidate server workloads in the State Data Centers for several years. Although hardly an emerging technology, virtualization efforts are not complete. Server virtualization continues to evolve and expand on the capabilities offered and the efficiencies to be gained. The State Data Centers have made good progress with virtualization. To continue making progress, further customer agency support is required to expedite virtualization activities and to test virtualization conversions.

Evaluation of Server Virtualization

The State Data Centers have a standardized virtualization platform and there is high confidence that this effort will continue to move forward and even accelerate the migration as funding is made available. Importantly, as a result of data center consolidation, the data centers have been forced to support multiple server virtualization platforms. Again, customer agency support is needed to ease and expedite the migration from non-standard virtualization platforms to the State Data Center solution.

As internal cloud services providers, the State Data Centers will continue to expand server virtualization service offerings to partner agencies. These enhancements include more efficient use of resources through dense server consolidation farms and high-availability clusters with eventual self-service portals allowing partner agencies to provision virtual servers on an as-needed basis and to bill based only on pure usage of service and capacity. The State Data Center continually evaluates the emerging capabilities of server virtualization solutions to find the one that offers the features needed to provide these enhancements at the most cost-effective price.

In addition to internal cloud services, the State Data Center expects to expand into an IT service broker role. Service brokers offer hybrid cloud services to their customers. Hybrid cloud services offer the ability for an application to run on an on premise private cloud or an off premise cloud provided by a third party. Virtualized IT assets can freely move between the on premise and off premise clouds as required by changes in cost, risk, or performance.

Recommendations for Server Virtualization

While the data centers are heavy users of server virtualization (currently having over 85% of servers running in a virtual environment), there is still extensive work to be done in both virtualizing old physical servers (and obtaining customer cooperation for testing support), migrating from non-standard virtualization environments and, most importantly, acquiring the capacity necessary to support continued virtualization in order to accumulate the accompanying efficiency and cost-effective benefits.

Strategies for Server Virtualization

- State Data Center server virtualization efforts must continue with as much urgency as available computing capacity will allow.
- Enable hybrid cloud and service brokering services in order to more flexibly manage cost, risk, and performance requirements.

- Increase virtualization density levels by maximizing and tuning underlying hardware performance.
- Continue State Data Center organizational and geographic consolidation to reduce virtualization environment complexity.

10. Disaster Recovery (DR)

DR involves a set of policies, procedures, and technologies to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Current Environment

The State Data Center inherited multiple DR vendor contracts and solutions through consolidation. The Legislature further provided funding in the 2014 General Appropriations Act (GAA) for the initial implementation of a standard state-wide disaster recovery service for certain agency applications with "urgent" criticality, based on the results of an externally provided study completed December 2013. While DR is offered to all State Data Center customers, not all make use of the services offered. In Fiscal Year 2015-16 four additional agencies were allocated DR funding. Work continues to refine and expand the AST offering, including the underlying technologies, cost recovery model, and supporting staff. The end result is customers focus on their most critical applications due to the high cost of recovery services and the limitation of services offered.

Evaluation of Enhanced Disaster Recovery Capabilities

The State Data Center realizes that utilization of tape backup solutions represent a single point of failure and that the recovery time objective (RTO) under this approach affects business continuity. Consequently, the State Data Center is working with recovery service providers to implement enhanced solutions leveraging disk-based technologies, data de-duplication, and data replication. This includes offsite backup, offsite storage, and other managed services.

Customers want to leverage advancements in DR solutions to provide faster, more cost effective, and more comprehensive DR services. Solutions that provide seamless or near-seamless system failover and replication allow businesses and government to abandon legacy labor intensive tape recovery and complex disaster recovery plans in favor of cloud recovery services, faster replication, and backup to disk, both on and off site.

While many options are now available in the marketplace, the cost associated with the levels of service vary. The state must review current business applications and surrounding processes to determine the best fit and what services are truly required. AST will help the agencies evaluate technology needs to maintain essential state functions against the urgency of continued operations. Time frames for recovery are often directly proportional to the cost of such services. Business dependency on automated systems will direct these recovery requirements, and a balanced approach will provide the best combination of services against overall cost.

Recommendations for Disaster Recovery

The State Data Center should continue to develop and enhance current DR capabilities, while considering alternative technologies in the context of the trends and conditions identified here. Particular attention should be given to solutions that will enhance data center strategies and drive cost effectively. This will assist with agency expectations for business continuity by working closely with customer agencies to identify their true DR needs.

Strategies for Disaster Recovery

- Refine and develop solutions that allow the State Data Center to offer the highest level of availability to customer agencies for their most critical applications, and a scaled availability solution for their less critical applications.
- Evaluate emerging technologies and orchestration tools, assessing the potential value of each in the context of prior product investments, risk and maturity of alternative solutions, architectural requirements for use, and impact on established standard environments.
- Ensure that DR service offerings meet targeted recovery objectives and offer the capability for measuring ROI and enhancing recovery performance.
- Integrate DR solution options into the normal workflow of customer service provisioning.

LRPP Exhibit II - Performance Measures and Standards

Department: Agency for State Technology	Department No.: 7298

Program: Agency for State Technology	Code: 72980000
Service/Budget Entity: Executive Direction and Support Services	Code: 72980100

NOTE: Approved primary service outcomes must be listed first.

Approved Performance Measures for FY 2015-16 (Words)	Approved **Prior** Year Standard **FY 2014-15** (Numbers)	**Prior** Year Actual **FY 2014-15** (Numbers)	**Approved** Standards for **FY 2015-16** (Numbers)	**Requested FY 2016-17** Standard (Numbers)
Proposed new measure - Number of security guidance artifacts published	N/A	N/A	N/A	2
Proposed new measure - Number of trainings for agency Information Security Managers (ISMs) and partners on cyber threats and security management practices	N/A	N/A	N/A	10 ISM meetings and 1 Special Workshop
Proposed new measure - Number of project management trainings	N/A	N/A	N/A	4

NOTE: AST will submit a budget amendment to request approval of these proposed new measures in accordance with section 216.1827, F.S.

LRPP Exhibit II - Performance Measures and Standards

Department: Agency for State Technology	Department No.: 7298

Program: Agency for State Technology	Code: 72980000
Service/Budget Entity: State Data Center	Code: 72980500

NOTE: Approved primary service outcomes must be listed first.

Approved Performance Measures for FY 2015-16 (Words)	Approved **Prior** Year Standard **FY 2014-15** (Numbers)	**Prior** Year Actual **FY 2014-15** (Numbers)	**Approved** Standards for **FY 2015-16** (Numbers)	**Requested FY 2016-17** Standard (Numbers)
Proposed new measure - Data Center facility uptime availability	N/A	N/A	N/A	99.85%
Proposed new measure - Percent of established Service Level Agreement (SLA) goals at or above target	N/A	N/A	N/A	89%

NOTE: AST will submit a budget amendment to request approval of these proposed new measures in accordance with section 216.1827, F.S.

Performance Measure Validity and Reliability (LRPP Exhibit IV)

LRPP EXHIBIT IV: Performance Measure Validity and Reliability

Department: Agency for State Technology

Program: Executive Direction and Support Services

Service/Budget Entity: 72980100

Measure: Number of security guidance artifacts published.

Action (check one):

☐ Requesting revision to approved performance measure.

☐ Change in data sources or measurement methodologies.

☒ Requesting new measure.

☐ Backup for performance measure.

Data Sources and Methodology: The data source and methodology for this measure is a manual calculation of the number of training artifacts created to educate agency information security managers and partners.

Validity: This source and methodology is valid based on the tracking method, which is a manual calculation of the percentage of security guidance artifacts created to educate agency information security managers and partners.

Reliability: This source and methodology is reliable based on the tracking method, which is a manual calculation of the number of artifacts created. The artifacts shall be counted in the spreadsheet entitled “AST Information Security Training Artifacts.”

LRPP EXHIBIT IV: Performance Measure Validity and Reliability

Department: Agency for State Technology

Program: Executive Direction and Support Services

Service/Budget Entity: 72980100

Measure: Number of trainings for agency ISMs and partners on cyber threats and security management practices.

Action (check one):

☐ Requesting revision to approved performance measure.

☐ Change in data sources or measurement methodologies.

☒ Requesting new measure.

☐ Backup for performance measure.

Data Sources and Methodology: The data source and methodology for this measure will be a manual calculation of the number of trainings offered. The agenda for the meetings will be scanned and stored in a centralized location and summarized in a spreadsheet entitled "AST Information Security Trainings." The number of trainings offered will be counted.

Validity: This source and methodology is valid based on the tracking method, which is a manual calculation of the number of trainings held. The agenda for the meetings will be scanned and stored in a centralized location and summarized in a spreadsheet entitled "AST Security Trainings."

Reliability: This source and methodology is reliable based on the tracking method, which is a manual calculation of the number trainings held. The agenda for the meetings will be scanned and stored on in a centralized location and summarized in a spreadsheet entitled "AST Security Trainings."

LRPP EXHIBIT IV: Performance Measure Validity and Reliability

Department: Agency for State Technology

Program: Executive Direction and Support Services

Service/Budget Entity: 72980100

Measure: Number of trainings held on project management and oversight standards.

Action (check one):

☐ Requesting revision to approved performance measure.

☐ Change in data sources or measurement methodologies.

☒ Requesting new measure.

☐ Backup for performance measure.

Data Sources and Methodology: The data source and methodology for this measure will be a manual calculation of the number of trainings offered. The agenda for the meetings will be scanned and stored in a centralized location and summarized in a spreadsheet entitled "AST Project Management Trainings." The number of trainings offered will be counted.

Validity: This source and methodology is valid based on the tracking method, which is a manual calculation of the number of trainings held. The agenda for the meetings will be scanned and stored in a centralized location and summarized in a spreadsheet entitled "AST Project Management Trainings."

Reliability: This source and methodology is reliable based on the tracking method, which is a manual calculation of the number of trainings held. The agenda for the meetings will be scanned and stored in a centralized location and summarized in a spreadsheet entitled "AST Project Management Trainings."

LRPP EXHIBIT IV: Performance Measure Validity and Reliability

Department: Agency for State Technology

Program: State Data Center

Service/Budget Entity: 72980500

Measure: Data Center Uptime Availability

Action (check one):

☐ Requesting revision to approved performance measure.

☐ Change in data sources or measurement methodologies.

☒ Requesting new measure.

☐ Backup for performance measure.

Data Sources and Methodology: The data source for this measure is the Total Available Minutes (TAM), which equals the number of days in a month, multiplied times 24 hours multiplied times 60 minutes. Facility uptime for the period equals TAM, minus excessed/planned downtime, divided by total available uptime for the period. Scheduled outages will not be counted against uptime.

Validity: This source and methodology is valid based on the tracking method, which is a manual calculation from daily outage reports.

Reliability: This source and methodology is reliable based on the tracking method, which is a manual calculation from daily outage report.

LRPP EXHIBIT IV: Performance Measure Validity and Reliability

Department: Agency for State Technology

Program: State Data Center

Service/Budget Entity: 72980500

Measure: Percentage of SLA goals at or above target

Action (check one):

☐ Requesting revision to approved performance measure.

☐ Change in data sources or measurement methodologies.

☒ Requesting new measure.

☐ Backup for performance measure.

Data Sources and Methodology: The data source is based on AST's Cherwell system, which tracks a number of sub-measures that make up the data for this measure. These sub-measures are:

1. Percentage of incidents responded timely by Tier 1
2. Percentage of incidents responded timely by Tier 2
3. Percentage of incidents with timely customer updates
4. Percentage of service requests responded timely by Tier 1
5. Percentage of service requests responded timely by Tier 2
6. Percentage of service requests with timely customer updates
7. Availability of Windows servers
8. Percentage of servers at 95% or greater patch level
9. Percent of backups successful

Validity: This measure is valid as it represents the performance as dictated by service level agreements with SDC customers.

Reliability: This measure is reliable as the data is verifiable and captured by Cherwell.

Associated Activities Contributing to Performance Measures (LRPP Exhibit V)

LRPP Exhibit V: Identification of Associated Activity Contributing to Performance Measures - Executive Direction and Support			
Measure Number	**Approved Performance Measures for FY 2015-16 (Words)**		**Associated Activities Title**
1	New Measure: Number of security guidance artifacts published		Information Technology – Executive Direction and Support Services
2	New Measure: Number of trainings for agency ISMs and partners on cyber threats and security management practices.		Information Technology – Executive Direction and Support Services
3	New Measure: Number of project management trainings		Information Technology – Executive Direction and Support Services

LRPP Exhibit V: Identification of Associated Activity Contributing to Performance Measures – State Data Center			
Measure Number	**Approved Performance Measures for FY 2015-16 (Words)**		**Associated Activities Title**
1	New Measure - Data Center Uptime Availability.		Information Technology – Data Center Administration Information Technology – Computer Operations
2	New Measure - Percent of established SLA goals at or above target		Information Technology - Data Center Administration Information Technology – Computer Operations

AGENCY FOR STATE TECHNOLOGY-NORTHWOOD

FISCAL YEAR 2014-15

SECTION I: BUDGET	OPERATING	FIXED CAPITAL OUTLAY
TOTAL ALL FUNDS GENERAL APPROPRIATIONS ACT	31,753,894	
ADJUSTMENTS TO GENERAL APPROPRIATIONS ACT (Supplementals, Vetoes, Budget Amendments, etc.)	375,119	
FINAL BUDGET FOR AGENCY	32,129,013	

SECTION II: ACTIVITIES * MEASURES	Number of Units	(1) Unit Cost	(2) Expenditures (Allocated)	(3) FCO
Data Center NSRC Raised Floor Space - Colocation	10,888	3.39	36,939	
Data Base Managed Service - Oracle DB	2,036	1,073.38	2,185,409	
Data Base Managed Service - SQL DB	3,690	253.60	935,771	
Data Base Managed Service - UDB	510	467.14	238,242	
Mainframe				
IBM -- FLORIDA IMS Processing	2,696	1,528.09	4,119,477	
IBM -- FLORIDA/FSFN Batch Processing	8,357	489.49	4,090,890	
IBM -- FLORIDA/FSFN DB2 Processing	2,353	992.99	2,336,975	
IBM -- FLORIDA/FSFN TSO Processing	91	603.59	54,663	
IBM -- WIC Batch Processing	69	5,356.29	370,300	
IBM -- WIC CICS Processing	3	16,395.89	43,418	
IBM -- WIC DB2 Processing	37	4,728.31	173,217	
IBM -- WIC TSO Processing	11	3,457.30	38,818	
IBM Print Management (Dispatch)	2,856	21.09	60,247	
Mainframe Storage				
Backup Service - Mainframe	27,309,598	0.01	295,253	
Disk Storage - IBM Mainframe	1,813,133	0.21	377,597	
Offsite Tape Storage - Mainframe IBM	3,688	21.53	79,391	
Midrange				
Managed Server -- Windows- Capacity Units	258,888	5.77	1,493,676	
Managed Server -- Non Windows- Capacity Units	88,600	10.94	969,196	
Managed Server -- Non Windows- Server Units	2,436	349.20	850,652	
Managed Server -- Windows - Server Units	15,477	72.98	1,129,558	
Midrange Storage				
Backup Service - Midrange	25,953,767	0.05	1,370,302	
Disk Storage - Midrange	344,383,595	0.00	807,956	
Offsite Tape Storage - Midrange	19,660	32.49	638,726	
Network				
Application Load Balancing/Reverse Proxy	2,407	27.48	66,149	
Bandwidth	1,549,923	0.26	398,614	
Network Units	17,988	93.87	1,688,450	
Agency Direct Billed	1,942,456	1.10	2,143,361	
Professional Services - Direct Billed			881,858	
General Revenue - Disaster Recovery			1,337,495	
Unallowable Costs			850,909	
TOTAL			30,026,568	0

SECTION III: RECONCILIATION TO BUDGET			
PASS THROUGHS			
TRANSFER - STATE AGENCIES			
AID TO LOCAL GOVERNMENTS			
PAYMENT OF PENSIONS, BENEFITS AND CLAIMS			
OTHER			
REVERSIONS		2,102,445	
TOTAL BUDGET FOR AGENCY *(Total Activities + Pass Throughs + Reversions) - Should equal Section I above. (4)*		32,129,013	

SCHEDULE XI/EXHIBIT VI: AGENCY-LEVEL UNIT COST SUMMARY

AGENCY FOR STATE TECHNOLOGY-SOUTHWOOD

FISCAL YEAR 2014-15

SECTION I: BUDGET	OPERATING	FIXED CAPITAL OUTLAY
TOTAL ALL FUNDS GENERAL APPROPRIATIONS ACT	32,141,201	
ADJUSTMENTS TO GENERAL APPROPRIATIONS ACT (Supplementals, Vetoes, Budget Amendments, etc.)	65,379	
FINAL BUDGET FOR AGENCY	32,075,822	

SECTION II: ACTIVITIES * MEASURES	Number of Units	(1) Unit Cost	(2) Expenditures (Allocated)	(3) FCO
Data Center Management Subtotal				
Additional Electrical Circuit	3,138	20.43	64,110	
SRC Floor Tiles	2,692	222.14	598,000	
SRC Rack Mounts	1,688	109.65	185,089	
Scheduling Services	11,440	60.79	695,485	
Mainframe Services				
z/OS Processing	2,850	1,526.78	4,351,317	
CICS Processing	2,868	268.69	770,601	
DB2 Processing	2,763	52.61	145,365	
Mainframe Storage	128,133	1.56	199,413	
Mainframe Backup / Virtual Storage	17,579,294	0.01	117,318	
Open Systems Platform Subtotal				
Unix Managed Server Standard	159	171.77	27,311	
Unix Managed Server Premium	1,885	310.12	584,642	
Managed Server-Database Oracle Svcs	1,661	1,533.07	2,546,933	
Managed Server-Database SQL Svcs	3,089	113.16	349,543	
Unix Capacity Unit	2,430	194.32	472,255	
Net-Based Services	5,087	49.65	252,560	
EDI Translation	11,092,052	0.01	61,113	
Storage Management Subtotal				
Distributed Backup	143,342,541	0.02	2,882,764	
Distributed Storage (Unmirrored)	291,624,010	0.01	1,931,018	
Windows Platform Subtotal				
Windows Managed Server Premium	15,121	154.29	2,332,977	
Windows Capacity Unit	285,280	7.27	2,073,850	
Windows Applications Subtotal				
Transitional Service	614	84.92	52,103	
Citrix	16,666	38.33	638,885	
SSRC Email	17,656	19.78	349,299	
Enterprise Vault Cloud Archive	334,296	1.67	558,869	
			73,226	
Agency Directs			5,479,816	
General Revenue-Disaster Recovery			784,024	
Prior Year True-up Billing				
Unallowable Costs				
TOTAL			28,577,886	

SECTION III: RECONCILIATION TO BUDGET				
PASS THROUGHS				
TRANSFER - STATE AGENCIES				
AID TO LOCAL GOVERNMENTS				
PAYMENT OF PENSIONS, BENEFITS AND CLAIMS				
OTHER				
REVERSIONS			2,027,078	
TOTAL BUDGET FOR AGENCY *(Total Activities + Pass Throughs + Reversions) - Should equal Section I above. (4)*			30,604,964	

SCHEDULE XI/EXHIBIT VI: AGENCY-LEVEL UNIT COST SUMMARY

Glossary of Terms and Acronyms

Activity: A set of transactions within a budget entity that translates inputs into outputs using resources in response to a business requirement. Sequences of activities in logical combinations form services. Unit cost information is determined using the outputs of activities.

Agency for State Technology: A State of Florida agency charged with developing strategies for the design, delivery, and management of enterprise information technology services; monitoring delivery and management of those services; and establishing rules and policies for managing those services.

Appropriation Category: The lowest level line item of funding in the General Appropriations Act that represents a major expenditure classification of the budget entity. Within budget entities, these categories may include: Salaries and Benefits, Other Personal Services (OPS), Expenses, Operating Capital Outlay, Data Processing Services, Fixed Capital Outlay, etc. These categories are defined within this glossary under individual listings. For a complete listing of all appropriation categories, please refer to the ACTR section in the LAS/PBS User's Manual for instructions on ordering a report.

AST: Agency for State Technology.

AST-North: The State Data Center location in the Northwood mall, a leased facility.

AST-South: The State Data Center location located on the south side of Tallahassee; the facility is state-owned.

Baseline Data: Indicators of a state agency's current performance level, pursuant to guidelines established by the Executive Office of the Governor in consultation with legislative appropriations and appropriate substantive committees.

Budget Entity: A unit or function at the lowest level to which funds are specifically appropriated in the appropriations act. "Budget entity" and "service" have the same meaning.

CIO: Chief Information Officer.

CJIS: Criminal Justice Information System.

COBIT: Control Objectives for Information and Related Technology.

COSO: Committee of Sponsoring Organizations of the Treadway Committee.

Customer: The entity that receives services from the State of Florida Agency for State Technology (AST); the entity that agrees to the service level targets.

D3-A: A legislative budget request (LBR) exhibit which presents a narrative explanation and justification for each issue for the requested years.

Demand: The number of output units which are eligible to benefit from a service or activity.

EOG: Executive Office of the Governor.

Estimated Expenditures: Includes the amount estimated to be expended during the current fiscal year. These amounts will be computer-generated based on the current year appropriations adjusted for vetoes and special appropriations bills.

F.S.: Florida Statutes.

GAA: General Appropriations Act.

GR: General Revenue Fund.

HIPAA: Health Insurance Portability and Accountability Act.

HITRUSR CSF: Health Information Trust Alliance Common Security Framework.

Indicator: A single quantitative or qualitative statement that reports information about the nature of a condition, entity or activity. This term is used commonly as a synonym for the word "measure."

Information Technology Policy: A definite course or method of action selected from among one or two alternatives that guide and determine present and future decisions.

Information Technology Resources: Included data processing-related hardware, software, services, telecommunications, supplies, personnel, facility resources, maintenance, and training.

Information Technology Security: Protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of data, information, and information technology resources.

Input: See Performance Measure.

IOE: Itemization of Expenditure.

ISO: International Organization for Standardization

IT: Information Technology.

LAN: Local Area Network

LAS/PBS: Legislative Appropriation System/Planning and Budgeting Subsystem. The statewide appropriations and budgeting system owned and maintained by the Executive Office of the Governor.

LBC: Legislative Budget Commission.

Legislative Budget Commission: A standing joint committee of the Legislature. The Commission was created to: review and approve/disapprove agency requests to amend original approved budgets; review agency spending plans; issue instructions and reports concerning zero-based budgeting; and take other actions related to the fiscal matters of the state, as authorized in statute. It is composed of 14 members appointed by the President of the Senate and by the Speaker of the House of Representatives to two-year terms, running from the organization of one Legislature to the organization of the next Legislature.

LBR: Legislative Budget Request.

Legislative Budget Request: A request to the Legislature, filed pursuant to s. 216.023, Florida Statutes, or supplemental detailed requests filed with the Legislature, for the amounts of money an agency or branch of government believes will be needed to perform the functions that it is authorized, or which it is requesting authorization by law, to perform.

LMS: Learning Management System.

LRPP: Long-Range Program Plan.

Long-Range Program Plan: A plan developed on an annual basis by each state agency that is policy-based, priority-driven, accountable, and developed through careful examination and justification of all programs and their associated costs. Each plan is developed by examining the needs of agency customers and clients and proposing programs and associated costs to address those needs based on state priorities as established by law, the agency mission, and legislative authorization. The plan provides the framework and context for preparing the legislative budget request and includes performance indicators for evaluating the impact of programs and agency performance.

Narrative: Justification for each service and activity is required at the program component detail level. Explanation, in many instances, will be required to provide a full understanding of how the dollar requirements were computed.

NIST: National Institute of Standards and Technology.

Nonrecurring: Expenditure or revenue which is not expected to be needed or available after the current fiscal year.

OPB: Office of Policy and Budget, Executive Office of the Governor.

Outcome: See Performance Measure.

Output: See Performance Measure.

Outsourcing: Describes situations where the state retains responsibility for the service, but contracts outside of state government for its delivery. Outsourcing includes everything from contracting for minor administration tasks to contracting for major portions of activities or services that support the agency mission.

Pass Through: Dollars that flow through an agency's budget for which the agency has no discretion with respect to spending or performance. Examples of pass throughs include double budget for data centers, tax or license for local governments, WAGES contracting, etc.

PCI DSS: Payment Card Industry Data Security Standard.

Performance Measure: A quantitative or qualitative indicator used to assess state agency performance.

- Input means the quantities of resources used to produce goods or services and the demand for those goods and services.
- Outcome means an indicator of the actual impact or public benefit of a service.
- Output means the actual service or product delivered by a state agency.

Policy Area: A grouping of related activities to meet the needs of customers or clients that reflects major statewide

priorities. Policy areas summarize data at a statewide level by using the first two digits of the ten-digit LAS/PBS program component code. Data collection will sum across State agencies when using this statewide code.

Provider: The State Data Center established within the State of Florida Agency for State Technology. The State Data Center has two locations, AST-North and -AST-South.

Project: A temporary endeavor that has a defined beginning and end.

Project Oversight: An independent review and analysis of information technology projects providing insight into the project's scope, completion dates, budget, issues, and risks that might affect the successful and timely completion of the project.

Program: A set of activities undertaken in accordance with a plan of action organized to realize identifiable goals based on legislative authorization (a program can consist of single or multiple services). For purposes of budget development, programs are identified in the General Appropriations Act for Fiscal Year 2001-2002 by a title that begins with the word "Program." In some instances a program consists of several services, and in other cases the program has no services delineated within it; the service is the program in these cases. The LAS/PBS code is used for purposes of both program identification and service identification. "Service" is a "budget entity" for purposes of the LRPP.

Program Purpose Statement: A brief description of approved program responsibility and policy goals. The Purpose Statement relates directly to the agency mission and reflects essential services of the program needed to accomplish the agency's mission.

Program Component: An aggregation of generally related objectives which, because of their special character, related workload, and interrelated output, can logically be considered an entity for purposes of organization, management, accounting, reporting, and budgeting.

Reliability: The extent to which the measuring procedure yields the same results on repeated trials and data are complete and sufficiently error free for the intended use.

SAN: Storage Area Network

Service: See Budget Entity.

Service-Level Agreement: A formal document entered into by the State Data Center and a customer entity that outlines the service description, the service level targets, service costs, and the provider's and customer's responsibilities.

SLA: Service-Level Agreement

Standard: The level of performance of an outcome or output.

State Data Center: Established within the AST to provide data center services as an enterprise information technology service. The State Data Center has two locations, AST-North and AST-South.

TCS: Trends and Conditions Statement.

Unit Cost: The average total cost of producing a single unit of output – goods and services for a specific agency activity.

Validity: The appropriateness of the measuring instrument in relation to the purpose for which it is being used.

Virtualization: A software technique that allows one computer to run the workload of several systems on the same hardware by employing “virtual” systems.