State of Florida

Agency for State Technology

Rick Scott, Governor

4050 Esplanade Way, Suite 115
Tallahassee, FL 32399-0950
Tel: 850-412-6050

Eric M. Larson
State CIO/Executive Director

LONG RANGE PROGRAM PLAN

Agency for State Technology
Tallahassee, Florida

October 1, 2018

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

Dear Directors:

Pursuant to Chapter 216, Florida Statutes, our Long Range Program Plan (LRPP) for the Agency for State Technology 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 2019-20 through Fiscal Year 2023-24. The internet website address that provides the link to the LRPP located on the Florida Fiscal Portal is http://ast.myflorida.com/publications. This submission has been approved by Eric M. Larson, Executive Director.

Sincerely,

Eric M. Larson
State CIO/Executive Director

Agency for State Technology

LONG RANGE PROGRAM PLAN

FISCAL YEARS 2019-2020

THROUGH 2023-2024

Eric M. Larson, Executive Director/
State Chief Information Officer
Agency for State Technology

Agency for State Technology

Long Range Program Plan

FY 2019-2020 through FY 2023-2024

Agency Mission and Goals

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 the authority of the State Data Center to AST. 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	Adding Value Wherever We Go Enterprise-wide Service Organization Standardized Self-Improving Process Get it Right the First Time Remove Single Points of Failure Optimize the Organization

Stakeholders 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 provide high availability services for the State Data Center customers.

Agency Objectives, 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: 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 2016-17)	FY 2019-20	FY 2020-21	FY 2021-22	FY 2022-23	FY 2023-24
2	4	6	6	6	6

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

Objective: 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 or Security Meetings with a Training Component for Agency Information Security Managers (ISMs) and Partners on Cyber Threats and Security Management Practices

Baseline Year (FY 2016-17)	FY 2019-20	FY 2020-21	FY 2021-22	FY 2022-23	FY 2023-24
10 trainings or meetings with training component	10 trainings or meetings with training component	10 trainings or meetings with training component	10 trainings or meetings with training component	10 trainings or meetings with training component	10 trainings or meetings with training component

Goal 3: To deliver high availability services for the State Data Center customers.

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: Provide operational management and oversight of the State Data Center.

Outcome 1: Data Center Facility Uptime Availability Percentage

Baseline Year (FY 2016-17)	FY 2019-20	FY 2020-21	FY 2021-22	FY 2022-23	FY 2023-24
99.85%	99. 9%	99.9%	99.9%	99.9%	99.9%

Outcome 2: Average percentage of Service Level Agreement (SLA) sub-measures at or above target goals

Baseline Year (FY 2016-17)	FY 2019-20	FY 2020-21	FY 2021-22	FY 2022-23	FY 2023-24
95%	95%	95%	95%	95%	95%

Agency for State Technology

Long Range Program Plan

FY 2019-20 through FY 2023-24

Linkage to Governor's Priorities

The Agency for State Technology's (AST) Long Range Program Plan (LRPP) builds on the Governor's priorities by providing efficient technology services to State Data Center (SDC) customer agencies. Technology services are a critical component in support of the goals of all agencies, and AST's LRPP strives to ensure that all Governor's agencies can leverage technology to enable a more innovative, efficient, and sustainable government. A key component in AST's plan is cybersecurity, critical to the health, welfare, and safety of State of Florida citizens through protection of citizen data and availability of technology essential to the delivery of services. The plan also builds on the Governor's priority of focusing on job growth and retention by striving to maintain 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, effective technology services will enable Florida's support of a safe and well-educated citizenry, creating a pro-business climate resulting in both business and job growth.

Trends and Conditions Statement

Technology continues to be a pervasive and driving force in virtually every facet of modern life. This is due, in part, to the broad range of accessible and 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 new technology products are developed, there will be increasing opportunities for the use of centralized, shared services provided by private entities commonly referred to as "cloud" services. These services sometimes offer an opportunity for the government to modernize service delivery while reducing some of the risk and cost of the traditional approach of creating custom applications.

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

Positive Trends

a. Security processes, services, and tools are improving rapidly to address the increased severity and sophistication of attackers. While a significant investment in people, process, and technology will be necessary to adequately address the security risk, it is possible to address security concerns if the efforts are prioritized appropriately.

b. The commoditization of applications and services in the marketplace continue to provide opportunities to increase the agility and improve efficiencies of operation. Unfortunately, the ability to customize traditional COTS (Commercial off the Shelf) applications often led to challenges upgrading and sustaining them. Cloud services and applications help overcome that challenge by limiting the options to customize the applications and hosting environment. While limiting application customization may require updated business processes that align with the cloud applications, adopting these highly commoditized, continuously improved services will result in a far more sustainable application that can significantly reduce or eliminates the cost and complexity of iterative application refreshes over the life of the application. As the cloud marketplace continues to mature, and the scope and maturity of commoditized cloud applications expands, more options to leverage these cloud services will occur.

c. Open standards that offer interoperability of common services are improving rapidly. Adopting industry standards for services and protocols used by identity management, service integration, data management, security, and many others will position the state to leverage commoditized services to the greatest extent possible.

d. 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.

e. The costs continue to fall for a vast array of computing devices: tablets, smartphones, servers, storage systems, networking equipment, and computer-embedded industrial products. A host of new technologies are becoming affordable enough to be integrated and applied to solve business problems.

f. 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.

g. Many IT services are now readily available on the open market "as-needed". The initial cost of services is quite reasonable, when compared with traditional procurements as 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.

h. Agile development methodologies have been used by industry and state agencies for decades. When properly executed, they are found to increase customer satisfaction and reduce the risk of project failures due to close and regular interactions with the customer and the frequent releases of working code (rather than waiting months or years to reveal the application). Moreover, agile methods promote self-organization of teams which contributes to improved team dynamics, performance and accountability. Some agencies have invested in agile methods' training (such as Scrum) to equip staff to apply these methods to development projects. AST will begin to incorporate these methods into the Project Management and Oversight Standards and coordinate training opportunities to educate state staff in the successful application of agile methods.

Negative trends

a. Security exploits with severe outcomes are continuing to occur at a troubling rate. The scope and severity of these exploits are driven by increased coordination between bad actors, often sponsored by well-funded organizations or nation-states. As successful exploits become more profitable and strategic, the tools available to identify and exploit vulnerabilities are becoming more capable and available to a broader audience, increasing the quantity and impact of bad actors.

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 necessarily based on an unwillingness to share the information. Instead, this is often the

result of isolation of data within applications, in addition to a lack of resources necessary to identify, catalog, manage, and coordinate the sharing of the information available.

c. The recruitment of highly technical positions required to support the information technology needs of state government is sometimes difficult within 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 legacy systems and creating even greater risks in developing strategies for their replacement.

d. Systems that support the operations of the State are implemented in isolation from one another, often with overlapping functionality, processes and data sets. Without a comprehensive view of process overlap and data dependencies across agencies, it will be challenging to create an enterprise view for application development efforts that includes the opportunities for data sharing and system component reuse. The necessary coordination will require extensive effort, but enhanced, enterprise-coordinated architectural designs can reduce potential duplication of costs and result in better collaboration across agency boundaries.

e. Many of the state's legacy systems are outside the scope of mainstream supportability and several major application redevelopment efforts to address them are occurring concurrently. These modernization efforts will have a high short-term cost, in addition to the growing costs to support the legacy systems during the development and implementation of their modernized replacement. While it is justifiable to offset development costs by attempting to recover operational costs from the legacy systems, underestimating the complexity, level of effort, expertise and cost to sustain the legacy applications not only introduces significant risk to State operations that still depend on them, issues that occur as a result will divert resources from modernization, potentially increasing costs by delaying implementation and the subsequent realization of returns on the investment.

f. The 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.

Cloud Services

Some analysis of existing and emerging technology trends related to cloud services in the marketplace has been undertaken, including evaluating technology advancements to determine their possible applicability in the delivery of services.

Cloud Service Brokering

The industry is continuing to see traditional on-premises data centers like the AST SDC evolve in becoming IT service brokers by integrating third party cloud services into their on-premises private cloud. IT service brokers can offer internal and external cloud services to their customers and move qualifying services between them in the most cost-effective manner. Qualifying applications can be mapped to the cloud environments based on 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 integrated hardware and software environment to run customer applications. The packaged (commoditized) nature of these environments limit the number of configuration and integration options; however, this predictability is necessary to optimize support, performance, and internal cloud readiness. 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 complexity.

Initiatives and specific technologies

The following is a focus on initiatives and specific technologies that will influence the services provided by 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. Software Defined Infrastructure
7. IT Service Management
8. Server Virtualization
9. 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 SDC customers own, operate, and support various applications themselves (even if hosted in the SDC). 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 third party providers.

Evaluation of SaaS

SaaS is a vendor-offered solution that is shared across many public and private 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 strict 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-premises 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 are 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 is undergoing development 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 expectations in management, budgeting, and termination of such agreements.

Strategies for SaaS

- Identify pilot candidates
- Canvas marketplace for potential opportunities and capabilities using requirements analysis
- Develop a process and procedure for adequate review, evaluation and ROI (Return on Investment)
- Pilot applications
- Develop contracting mechanisms to take advantage of the marketplace
- Ensure the development of an appropriate exit strategy

2. Infrastructure as a Service (IaaS)

IaaS refers to vendors offering pre-defined sets of standard 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. 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 SDC (operating as an IaaS provider to state customers). The SDC 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 pursuing IaaS services in the cloud using contracts administered by the SDC.

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 an eventual 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, dedicated network connectivity, electricity, infrastructure, and hardware refresh costs are considered in the cost/benefit estimation.

Recommendations for IaaS

IaaS 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 and security expectations are met, actual savings can be identified, and the elastic capacity utilization can be monitored for budget sufficiency, and state's interests are protected when such service agreements are terminated.

During the 2018 Legislative Session, AST was authorized by the 2018-19 General Appropriations Act (Line 2927) in proviso, to release a competitive solicitation to outsource all mainframe services to a cloud service. Upon completion of the competitive solicitation, a proposed plan is to be submitted to the chair of the Senate Appropriations Committee, the chair of the House of Representatives Appropriations Committee, and the Executive Office of the Governor's Office of Policy and Budget.

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), and Criminal Justice Information Services (CJIS) Policy, 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 (ISM) responsible for implementing the state's security framework, which includes the minimum standard for protecting state IT resources. Adoption of the security framework was a collaborative effort between AST, agency ISMs and members of the agency Inspectors General community. The framework identifies standard practices for detecting, reporting, and responding to IT security incidents, breaches, and threats. In addition, AST collaborated with the Florida Department of Law Enforcement (FDLE) Cybercrime Office, to develop and implement a process for reporting security incidents and breaches in compliance with statute.

Adoption of an IT security framework

An IT security framework is the foundation for an effective, enterprise-wide security program. It is a code of practice and principles that include 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 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.

An effective security posture also requires significant investment in the staff resources responsible for maintaining it. As a result, AST is continuously investigating opportunities to increase the knowledge and awareness of ISM staff as well as the general population. Through the AST partnership with University of West Florida, ISM training is being modeled after their Cybersecurity Degree program. By doing so, the frequency and quality of training improves.
Similarly, AST has facilitated providing security awareness training materials and tools to every agency that is an SDC customer. This approach ensures that the staff are properly trained to identify social engineering attacks that rely on human nature to compromise the security of state systems. As a result, there is now a consistent portfolio of training materials and real-world exercises that can prepare all customers of the SDC to do their part to protect the data managed by the State.

Strategies for Security

- Evaluate new and available security technologies for both strategic and operational initiatives.
- Invest in the training and exercises necessary to improve the quality of the security workforce as well as improving the awareness of end users to the risks they face when being provided access to state data.
- Partner AST with FDLE and other state agencies to work toward effective enterprise security solutions and programs.
- 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 continue 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. Software Defined Infrastructure

Software defined infrastructure is a broad term that includes the virtualization of equipment beyond the servers. Software Defined Networks, for example, include virtual network infrastructure such as switches, routers, load balancers, firewalls, and other network equipment that was historically shared by multiple customers and physically bound to a single location. Similarly, software defined storage provides flexibility for the location of files and data that historically were limited to a physical storage equipment within a single location. In general, limitations introduced by dependencies on specific physical equipment hinder

the ability of applications and services to migrate out of the primary physical data center into another location, such as the Cloud or secondary site such as a disaster recovery site. The ability to remove application dependencies on equipment that is physically located within the SDC will clear the path for implementing a Hybrid cloud data center that allows applications that can benefit from migration into the Cloud to do so while minimizing the impact on other applications that remain within the SDC. The work to attrition physical equipment in favor of virtual equipment that has the flexibility to migrate between physical sites was started during the physical consolidation of its two data center facilities in June 2016, when the resources housed in the former Northwood Shared Resource Center (NSRC) were migrated to the AST-South facility (formerly the Southwood Shared Resource Center, or SSRC). The series of projects to complete the logical consolidation and more fully integrate the technical operations of each has provided an opportunity to introduce and utilize software defined infrastructure. AST plans to continue the work that will facilitate not only the consolidation but ensure that applications that can benefit from Cloud are provided the best opportunity to take advantage of it with the least possible disruption to existing operations.

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, matured services are increasingly achieved through the rigor imposed by IT service management standards and best practices. By the application of modern, proven management techniques these practices ensure that customers of the SDC 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. Server Virtualization

Server virtualization refers to the creation of multiple 'virtual machines' on a single 'physical' machine. Each virtual machine acts like a physical computer with its own 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, cloud readiness), server virtualization is a prerequisite.

Current environment

Server virtualization has been a technology used to consolidate server workloads in the SDC for several years. Although hardly an emerging technology, virtualization efforts are not complete. Server virtualization continues to evolve and expand the capabilities offered and the efficiencies to be gained. The SDC has 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 SDC has a standardized virtualization platform and there is high confidence that this effort will continue to move forward and even accelerate the remaining logical consolidation work. Importantly, as a result of data center consolidation, the SDC continues to support multiple server virtualization platforms.

As internal cloud services providers, the SDC 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 SDC continually evaluates the emerging capabilities of server virtualization solutions to determine features needed to provide enhancements at the most cost-effective price.

In addition to internal cloud services, the SDC expects to expand into an IT service broker role. Virtualized IT assets can freely move between the on-premises and off-premises clouds, as required by changes in cost, risk, or performance. AST made great strides in Fiscal Year 2015-16 upgrading and consolidating virtualization environments positioning the SDC for a move into the IT service broker role.

Recommendations for Server Virtualization

Spurred by the physical data center consolidation efforts, now over 90% of the servers run in a virtual environment. Until this effort is complete, more work is necessary to continue virtualizing old physical servers (obtaining customer cooperation for testing support) and migrating from non-standard virtualization environments.

Strategies for Server Virtualization

- SDC server virtualization efforts must continue with as much urgency as available computing capacity will allow.
- Enable cloud and service brokering services to more flexibly manage cost, risk, and performance requirements.
- Increase virtualization density levels by maximizing and tuning underlying hardware performance.
- Increase automation within the virtualization environment to speed service delivery.

9. Disaster Recovery

Disaster Recovery (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 SDC inherited multiple DR vendor contracts and solutions from customer agencies over the course of data center consolidation. These solutions were often inadequate and unreliable and only covered a fraction of the applications in the data centers. The Florida Legislature provided funding in the 2014 General Appropriations Act (GAA) for the initial implementation of a disaster recovery service for a limited number of agency applications with “urgent” criticality, based on the results of an externally provided study completed in December 2013. In Fiscal Year 2015-16, additional agencies were allocated DR funding. Since that time the AST has continued to refine and expand the DR offering to include solutions that protect the most complex and critical customer agency applications. In addition to expanding the underlying technologies, AST has developed cost recovery models and capacity forecasting to provide truly functional, seamless disaster recovery offerings that support all landscapes, including legacy technologies not easily supported in third-party DR solutions.

Evaluation of Enhanced Disaster Recovery Capabilities

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

Customers are interested in leveraging 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 SDC should continue to develop and enhance current DR capabilities while considering alternative technologies in the context of the trends and conditions identified in this document. Particular attention should be given to solutions that will enhance SDC strategies and drive cost effectively. This will assist with agency expectations for business continuity by working closely with customer agencies to identify their actual DR needs.

Strategies for Disaster Recovery

- Refine and develop solutions that allow the SDC 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 enhance recovery performance.
- Evaluate the integration of cloud DR solutions with the AST DR environment to facilitate not only a transition to cloud where practical, but to create a functional bridge of cloud ready agency applications with legacy applications that are not cloud capable.
- Work with customer Agencies to expand Cloud based Disaster Recovery options where opportunities arise.
- Integrate DR solution options into the normal workflow of customer service provisioning.

Performance Measures and Standards (LRPP Exhibit II)

Agency for State Technology

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 2018-19 (Words)	Approved **Prior** Year Standard **FY 2017-18** (Numbers)	**Prior** Year Actual **FY 2017-18** (Numbers)	**Approved** Standards for **FY 2018-19** (Numbers)	**Requested FY 2019-20** Standard (Numbers)
Number of Security Guidance Artifacts Published	2	5	2	2
Number of Trainings or Security Meetings with a Training Component for Agency Information Security Managers (ISMs) and Partners on Cyber Threats and Security Management Practices	10	14	10	10

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 2018-19 (Words)	Approved **Prior** Year Standard **FY 2017-18** (Numbers)	**Prior** Year Actual **FY 2017-18** (Numbers)	**Approved** Standards for **FY 2018-19** (Numbers)	**Requested FY 2019-20** Standard (Numbers)
Data Center Facility Uptime Availability Percentage	99.9%	100.0%	99.9%	99.9%
Average Percentage of Service Level Agreement (SLA) Sub-measures at or Above Target	95.0%	97.35%	95.0%	95.0%

Assessment of Performance for Approved Performance Measures (LRPP Exhibit III)

Agency for State Technology

LRPP Exhibit III: PERFORMANCE MEASURE ASSESSMENT

Department: Agency for State Technology
Program: Executive Direction and Support Services
Service/Budget Entity: 72980100
Measure: Number of Security Guidance Artifacts Published

Action:

- ☐ Performance Assessment of Outcome Measure
- ☒ Performance Assessment of Output Measure
- ☐ Adjustment of GAA Performance Standards
- ☐ Revision of Measure
- ☐ Deletion of Measure

Approved Standard	Actual Performance Results	Difference (Over/Under)	Percentage Difference
2	5	3 (over)	150% (over standard)

Factors Accounting for the Difference:
Internal Factors (check all that apply):

- ☐ Personnel Factors
- ☐ Competing Priorities
- ☐ Previous Estimate Incorrect
- ☐ Staff Capacity
- ☐ Level of Training
- ☐ Other (Identify)

Explanation:
N/A

External Factors (check all that apply):

- ☐ Resources Unavailable
- ☐ Legal/Legislative Change
- ☐ Target Population Change
- ☐ This Program/Service Cannot Fix the Problem
- ☐ Current Laws Are Working Against the Agency Mission
- ☐ Technological Problems
- ☐ Natural Disaster
- ☐ Other (Identify)

Explanation:
N/A

Management Efforts to Address Differences/Problems (check all that apply):

- ☐ Training
- ☐ Personnel
- ☐ Technology
- ☒ Other (Identify)

Recommendations:
AST will measure the appropriateness of this metric over the coming measurement periods to assess potential for increase in the standard.

LRPP Exhibit III: PERFORMANCE MEASURE ASSESSMENT

Department: Agency for State Technology
Program: Executive Direction and Support Services
Service/Budget Entity: 72980100
Measure: Number of Trainings or Security Meetings with a Security Component for Agency Information Security Managers (ISMs) and Partners on Cyber Threats and Security Management Practices

Action:
☐ Performance Assessment of Outcome Measure ☐ Revision of Measure
☒ Performance Assessment of Output Measure ☐ Deletion of Measure
☐ Adjustment of GAA Performance Standards

Approved Standard	Actual Performance Results	Difference (Over/Under)	Percentage Difference
Ten trainings or meetings with training component	14	4 (over)	40% (over standard)

Factors Accounting for the Difference:
Internal Factors (check all that apply):
☐ Personnel Factors ☐ Staff Capacity
☐ Competing Priorities ☐ Level of Training
☐ Previous Estimate Incorrect ☐ Other (Identify)
Explanation:
N/A

External Factors (check all that apply):
☐ Resources Unavailable ☐ Technological Problems
☐ Legal/Legislative Change ☐ Natural Disaster
☐ Target Population Change ☐ Other (Identify)
☐ This Program/Service Cannot Fix the Problem
☐ Current Laws Are Working Against the Agency Mission
Explanation:
N/A

Management Efforts to Address Differences/Problems (check all that apply):
☐ Training ☐ Technology
☐ Personnel ☐ Other (Identify)
Recommendations:
N/A

LRPP Exhibit III: PERFORMANCE MEASURE ASSESSMENT

Department: Agency for State Technology
Program: State Data Center
Service/Budget Entity: 72980500
Measure: Data Center Facility Uptime Availability Percentage

Action:
☐ Performance Assessment of Outcome Measure ☐ Revision of Measure
☒ Performance Assessment of Output Measure ☐ Deletion of Measure
☐ Adjustment of GAA Performance Standards

Approved Standard	Actual Performance Results	Difference (Over/Under)	Percentage Difference
99.9%	100 %	Over	0.1%

Factors Accounting for the Difference:
Internal Factors (check all that apply):
☒ Personnel Factors ☐ Staff Capacity
☐ Competing Priorities ☒ Level of Training
☐ Previous Estimate Incorrect ☐ Other (Identify)
Explanation:

External Factors (check all that apply):
☐ Resources Unavailable ☐ Technological Problems
☐ Legal/Legislative Change ☐ Natural Disaster
☐ Target Population Change ☒ Other (Identify)
☐ This Program/Service Cannot Fix the Problem
☐ Current Laws Are Working Against the Agency Mission
Explanation: None

Management Efforts to Address Differences/Problems (check all that apply):
☒ Training ☐ Technology
☒ Personnel ☐ Other (Identify)
Recommendations:
N/A

Office of Policy and Budget – June 2018

LRPP Exhibit III: PERFORMANCE MEASURE ASSESSMENT

Department: Agency for State Technology
Program: State Data Center
Service/Budget Entity: 72980500
Measure: Percentage of Service Level Agreement (SLA) Sub-Measures at or Above Target Goals

Action:

- ☐ Performance Assessment of Outcome Measure
- ☒ Performance Assessment of Output Measure
- ☐ Adjustment of GAA Performance Standards
- ☐ Revision of Measure
- ☐ Deletion of Measure

Approved Standard	Actual Performance Results	Difference (Over/Under)	Percentage Difference
95.0%	97.35	Over	2.22%

Factors Accounting for the Difference:
Internal Factors (check all that apply):

- ☒ Personnel Factors
- ☐ Competing Priorities
- ☐ Previous Estimate Incorrect
- ☐ Staff Capacity
- ☒ Level of Training
- ☐ Other (Identify)

Explanation:

External Factors (check all that apply):

- ☐ Resources Unavailable
- ☐ Legal/Legislative Change
- ☐ Target Population Change
- ☐ This Program/Service Cannot Fix the Problem
- ☐ Current Laws Are Working Against the Agency Mission
- ☐ Technological Problems
- ☐ Natural Disaster
- ☐ Other (Identify)

Explanation:

Management Efforts to Address Differences/Problems (check all that apply):

- ☐ Training
- ☐ Personnel
- ☐ Technology
- ☐ Other (Identify)

Recommendations:
N/A

Office of Policy and Budget – June 2018

Performance Measure Validity and Reliability (LRPP Exhibit IV)

Agency for State Technology

LRPP EXHIBIT IV: Performance Measure Validity and Reliability

The agency is not proposing any changes to its performance measures.

Associated Activities Contributing to Performance Measures (LRPP Exhibit V)

Agency for State Technology

LRPP Exhibit V: Identification of Associated Activity Contributing to Performance Measures - Executive Direction and Support			
Measure Number	**Approved Performance Measures for FY 2017-18**		**Associated Activities Title**
1	Number of Security Guidance Artifacts Published		Information Technology – Executive Direction and Support Services
2	Number of Trainings or Security Meetings with a Training Component for Agency Information Security Managers (ISMs) and Partners on Cyber Threats and Security Management Practices		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 2017-18**		**Associated Activities Title**
3	Data Center Facility Uptime Availability Percentage		Information Technology – Data Center Administration Information Technology – Computer Operations
4	Percentage of Service Level Agreement (SLA) sub-measures at or above target goals		Information Technology - Data Center Administration Information Technology – Computer Operations

AGENCY FOR STATE TECHNOLOGY

SECTION I: BUDGET	OPERATING	FIXED CAPITAL OUTLAY
TOTAL ALL FUNDS GENERAL APPROPRIATIONS ACT	66,661,637	
ADJUSTMENTS TO GENERAL APPROPRIATIONS ACT (Supplementals, Vetoes, Budget Amendments, etc.)	(86,696)	
FINAL BUDGET FOR AGENCY	66,574,941	

FISCAL YEAR 2017-18

SECTION II: ACTIVITIES * MEASURES	Number of Units	(1) Unit Cost	(2) Expenditures (Allocated)	(3) FCO
Executive Direction			3,413,309	
Central Services				
CICS Processing	By LPAR		$771,323	
DB2 Processing	By LPAR		$42,683	
DCF DB2 Processing	By LPAR		$984,374	
DCF IMS Processing	By LPAR		$3,701,142	
DCF Storage	By LPAR		$83,896	
DCF z\OS Processing	By LPAR		$6,696,734	
EDI Translation	9,362,128	0.0065	$61,080	
Linux\Unix Capacity Unit	46,620	22.83	$1,064,347	
Linux\Unix Managed Server	4,948	191.77	$948,882	
Mainframe Backup/Virtual Storage	36,665,898	0.0034	$126,014	
Mainframe Storage	142,782	0.7349	$105,002	
Oracle Storage	1,095,042	0.2609	$285,679	
Oracle Services	2,724	1,670.32	$4,549,949	
UDB Service	16,800	53.33	$896,026	
Web\App\File\Transfer Services	5,322	59.32	$315,674	
Z\OS Processing	By LPAR		$4,366,278	
Core Services				
Data Protection Services	271,323,097	0.0137	$3,707,452	
Data Archival Service	10,284,742	0.1969	$2,025,516	
Load Balancing	21,924	16.24	$356,014	
Network Unit	36,794	82.46	$3,033,976	
Object Storage Services	3,426,564	0.2950	$1,010,969	
Block Storage Services	18,704,109	0.1499	$2,803,178	
Distributed Services by Agency Direct			$9,751,497	
Infrastructure and Facilities				
Additional Electrical Circuits	2,728	29.610	$80,777	
Floor Tiles	2,840	275.51	$782,441	
Rack Mounts	2,395	100.35	$240,334	
Scheduling Services	46,688	22.11	$1,032,061	
Windows Platform				
Azure	12	19,928.56	$239,149	
Citrix	21,190	32.91	$697,362	
Hosted Messaging Archival	12,036	10.57	$127,161	
Enterprise Vault Cloud Service	529,896	1.57	$829,652	
SQL Services	7,140	136.72	$976,171	
SQL Capacity Unit	238,542	4.33	$1,033,363	
Windows Capacity Units	557,102	6.98	$3,889,504	
Windows Managed Server	26,447	153.83	$4,068,245	
TOTAL			65,097,214	0

SECTION III: RECONCILIATION TO BUDGET			
PASS THROUGHS			
TRANSFER - STATE AGENCIES			
AID TO LOCAL GOVERNMENTS			
PAYMENT OF PENSIONS, BENEFITS AND CLAIMS			
OTHER		(6)	
REVERSIONS		1,477,733	
TOTAL BUDGET FOR AGENCY *(Total Activities + Pass Throughs + Reversions) - Should equal Section I above. (4)*		66,574,941	

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 (AST): 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.

Artifact: A document, spreadsheet, presentation, diagram, chart, brochure, poster, graphic, or any other material, generally for the purpose of documentation, training and/or awareness.

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 Services.

Cloud: The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.

COBIT: Control Objectives for Information and Related Technology.

COSO: Committee of Sponsoring Organizations of the Treadway Committee.

Customer: An 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.

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 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.

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.

Input: See Performance Measure.

IOE: Itemization of Expenditure.

ISO: International Organization for Standardization.

IT: Information Technology.

LAN: Local Area Network.

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

Legislative Budget Commission (LBC): 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.

Legislative Budget Request (LBR): 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.

Long Range Program Plan (LRPP): 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 fiscal year in which it is appropriated.

On-premise: Software that is installed and runs on computers on the premises (in the building) of the person or organization using the software, rather than at a remote facility such as a server farm or cloud.

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. Prior to June 2016, the State Data Center had two locations, Northwood and Southwood. Effective July 1, 2016, Southwood is the only State Data Center location.

Project: A temporary endeavor that has 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 (SLA): 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.

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

State Data Center (SDC): Established within the AST to provide data center services as an enterprise information technology service. Prior to July 1, 2016, the State Data Center had two locations, Northwood and Southwood; however, the SDC is now located only in the Southwood location.

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

Uptime: Measure of the time a machine, typically a computer, has been working and available.

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.