Florida Board of Governors General Office
2018-2019 Legislative Budget Request

Funding of $9.16 million is needed to support the 65 authorized positions and associated operating expense for the Board Office. The operating expense covers the costs associated with data collection and management, Board meeting expenses, travel expenses, office supplies and other Board initiatives.

Last year, the Board requested four new information technology positions and funds to implement critical cyber security initiatives, disaster recovery and backup, and modernization of existing databases. The Board received two of the four positions, but no additional operating resources to implement these initiatives. Consistent with last year's request, information technology and security funding of $877,519 is requested for technical services, application support/modernization and disaster recovery. Additional details are attached.

2018-2019 Legislative Budget Request		
		Total
1	2017-18 Budget (65 positions plus operating expenses)	$8,285,673
2		
3	20181-19 New Issue:	
4	Information Technology & Security Needs	$877,519
5		
6	Total Budget Request	$9,163,192
7	% Increase	10.5%

Board of Governors Office
Information Technology and Security Needs
2018-19 LBR Overview

The 2017 Legislature and Governor recognized the importance of having secure data systems and appropriated two new information technology security positions to assist the Board in ensuring data is properly secured and to ward off cybersecurity attacks on the system databases. The operating funds to go with these positions to implement some much needed initiatives was not provided. This request seeks recurring and nonrecurring resources to implement these projects.

Challenges

- The Board faces an ever increasing risk of information security failures due to the current escalating risk from cyber intrusions worldwide. There projects are also needed to bring the Boards IT system in compliance with the Agency for State Technology's Identity Management regulation (74-5.003).
- The very nature of the Boards' information gathering and data usage has drastically changed since its formation. The bulk of the research data being collected by the Board is now being used for funding considerations. Performance funding alone currently has half of a billion dollars associated with the metrics created from the Board's data warehouse. Although the Board has modernized its physical Information Technology infrastructure, the data collection applications are still structured after the Board of Regents legacy flat file data system.
- Board technical staff do not have the capacity to fully support the data analytic system. Finding and hiring high-level technical expertise to support these critical applications is necessary to improve data modernization.
- The Board has limited disaster recovery in place for its primary data systems located at Northwest Regional Data Center (NWRDC).

Proposed Solutions

- Implement multiple critical cybersecurity IT projects.
- Implement a data collection application modernization project.
- Move the Boards' analytics applications onto a hosted cloud infrastructure.
- Identify needs and initiate disaster recovery capability.

2018-19 Florida Board of Governors Information Technology and Security LBR request

	Cost		
Category	Reoccurring	One-time	Total
Common Technical Services*	$424,785	$0	$424,785
IT Security	$141,395	$156,830	$298,225
Application Support/Modernization	$128,509	$6,000	$134,509
Disaster Recovery	$0	$20,000	$20,000
	$694,689	$182,830	$877,519

*These Technical Services are common to all projects. They will be used over the life of all projects across multiple years.

Board of Governors Office
Information Technology and Security Needs
2018-19 LBR Subject Detail

Background

As the Board of Governors has matured as an agency, the Information Technology and Security (ITS) unit's areas of responsibility have continually increased. As areas of responsibility have increased and the technology security landscape has evolved, the ability to adequately limit the Board's information technology security risk, ensure business continuity, promote innovation, and efficiently deliver data to Board staff with its current information technology resources has proven to be challenging.

The areas that are most critically affected are Information Security, Application Support/Modernization, and Disaster Recovery.

When the Board office was formed, no information technology security positions were allocated for the Board. During the initial first five years of the Boards existence, no remote backup and recovery services existed for the Boards' primary data systems. It was during this five year period that the Board's primary data collection system, State University Data System (SUDS), was migrated from a mainframe platform to a client server platform modernizing the infrastructure.

Current Situation

a. Information Technology (IT) Security - Current heightened cybersecurity threats worldwide have placed the Board at a risk for a security breach or other types of security failures. In 2014, the Board engaged the IT security and identity experts from the University of Florida to produce an IT roadmap for the Boards' IT systems. The ITS office lacked the expertise and funding to enact all of the identified projects in the roadmap. In 2017-18 the Board office was allocated an Information Security Officer position and an IT Security Analyst position. With qualified personnel available to oversee these projects the Board only lacks funding to initiate these projects. These projects are also needed to bring the Boards IT system in compliance with the Agency for State Technology's Identity Management regulation (74-5.003).
b. Application Support/Modernization
    1. The migration of the State University Data System (SUDS) to a client/server platform modernized the infrastructure. However, resources to modernize and update the application itself was not available during infrastructure migration. The current data collection system is based largely upon criteria and parameters defined and implemented by the Board of Regents. The university business environments and their data systems have drastically changed since the system was designed. Some of this was highlighted in the OPPAGA University Personnel presentation to the House during the 2017 legislative session. The advent of performance-based Funding has also elevated the need for higher quality information to improve accountability.
    2. With the assistance of the Federal SLEDS grant, the Board expanded its Data Analytics Application. This expansion has been key in allowing the Board office to perform the performance-based funding analysis. Currently, the ITS has no staff with the technical expertise to manage this system, thus contracted staff have been utilized. Due to funding constraints and the high cost associated with the expertise related to this IT function, the Boards' ability to fully staff these needs has been limited.
c. Disaster Recovery - In 2011, the Board had no Disaster Recovery or Backup process in place for its enterprise systems at NWRDC. ITS has initiated full 'Backup as a Service' (BaaS) from NWRDC. Thanks to legislative support during the 2016-17 fiscal year, both on and offsite BaaS services will be

completely functional in 2017-18. Disaster recovery for the Board's critical systems is still non-existent. This continually puts the Board at risk for data loss and disruption of business operations.

Elevated Risk

a. IT Security and Access Management - The majority of ITS's data collections are personally identifiable information which include social security numbers. The inability to initiate targeted IT security projects increase the risk of a data security incident.
b. Application Support/Modernization
    1. State University Data System (SUDS) Data Quality and Accountability – A legacy application that houses data based on outdated criteria, makes verifying information more time consuming and labor intensive. This situation also increases the margin of error within the data. These factors put the accountability processes at risk. This situation also increases the data validation workload of both Board and university staff creating duplicative efforts and creating inefficiencies.
    2. Board Analytic Data Systems - Lack of support for the Board's analytic system puts the system at risk for failure. This could lead the inability to complete the performance-based funding calculations in a timely manner, thus impacting the university budgeting process.
c. Disaster Recovery – In the event of a catastrophic data center failure, due to a natural disaster or other unforeseeable occurrences, the Board does not have the capability to restore system operations within any reasonable time frame.

Recommended Actions

ITS is proposing the following solutions to address the issues describe in this document.

a. Security Projects – Implementation of cybersecurity related projects (details can be provided upon request in a separate document or meeting)
b. Application Support/Modernization
    1. ITS recommends a multi-year SUDS application modernization project be implemented. The first year of this project will be devoted to scoping the project, identifying Board needs, evaluating university business processes, gathering requirements, and designing a plan for the redesign. The second and third years will be dedicated to building, testing, and implementing the new systems.
    2. Board's Data Analytic Application – secure recurring funds to procure cloud-based Software as a Service (SaaS) to house the Data Analytic Application. Additionally one time funds are also needed to assist in the migration of the applications to the Cloud.
c. Disaster Recovery – ITS recommends having a 3rd party disaster recovery evaluation performed on its current primary IT systems. Based upon the evaluation, implement the recommended actions using NWRDC services.

Return on Investment

a. Security Projects - The primary justification for initiating these security projects is to lower or avoid the risk associated with a possible data breach. Although a 100 percent guarantee of preventing such an incident is not feasible, lowering the risk associated is desirable. Quantifying the avoidance of cost associated with the repercussion if a breach occurred would be dependent upon the detail of the event. However, an estimate of the cost of data monitoring alone for a single years' worth of student and staff data being compromised would be approximately $5 million dollars. If multiple years were breached the cost would grow dramatically depending upon the depth of the breach. This figure does not include forensic investigation, technology repair, legal fees, or possible civil judgments.
b. Application Modernization - The Boards data warehouse application is built on a business model that ceased to existence more than 17 years ago. There are three facets to the return on investment for

modernizing these applications. Improved data processing times, improved data quality, and a decreased level of personnel effort across the system.

Currently, the processing load for the legacy application has been optimized by improving the underlying hardware. No further data processing time improvements can be realized by adding infrastructure. Current benchmarks show excess headroom for processing that cannot be realized due to the legacy design. Although housed in a relational database, the legacy application does not use a normalized data model for data storage and retrieval. Based on current benchmarks, we believe a 30 percent efficiency can be achieved by improving the application design.

The return on investment for data quality are harder to quantify. However, currently the Board uses the legacy applications and data, to distribute $520 million in performance-based funding appropriations. This creates a higher level of confidence then the legacy data can easily provide. Challenges are also encountered when attempting to meet information requested by the legislature or Governor's office. This was recently validated by OPPAGA's analysis of the Board's legacy personnel data.

The level of staff effort system wide to transform, load, and validate university data based on the legacy definitions is monumental. By redesigning this application, workload across the SUS can be reduced. The Board office is also at risk in this area due to a lack of redundant staff that manage this system. Also, due to the nature of the legacy system and data, new staff take an inordinate amount of time to become experts over their assigned areas.

c. Disaster Recovery - Having disaster recovery is a key industry standard for critical information technology systems. The primary return on investment for implementing disaster recovery is risk avoidance. In the event of a disaster that cripples these systems the time and cost to restore the systems could be extravagant. Also there could be a potential loss of data that would have to be recollected impacting the workload of every university. Without a disaster recovery system in place the Board is in jeopardy of not meeting its state, federal, and constitutional obligations.