Prioritization of Cybersecurity and Legacy Modernization Projects Report to the Legislative Budget Board

October 1, 2016

PUBLIC REPORT

Texas Department of Information Resources

1. Public Report

1.1. Overview

HB 1 (84R), Article IX, Section 9.10 (the General Appropriations Act) required the Department of Information Resources (DIR) to submit to the Legislative Budget Board by October 1, 2016, a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems (PCLS report) to be considered for funding. To be included in this prioritization, agencies were required to submit information about their cybersecurity and legacy systems modernization projects to DIR through the Statewide Portal for Enterprise Cybersecurity Threats, Risks, and Incident Management (SPECTRIM).

The 2014 Legacy System Study was produced by DIR at the direction of the 83rd Legislature (House Bill 2738) to evaluate the composition of the state's current information technology (IT) landscape and determine how best to approach and make decisions about an aging infrastructure. A legacy system is defined in statute as a computer system or application program that is operated with obsolete or inefficient hardware or software technology.

Much like the physical infrastructure of public bridges and roads, IT infrastructure must be maintained to ensure continuity of service to the public. A legacy system operates with old, obsolete, unsecured, or inefficient hardware or software. Legacy systems are more difficult and costly to maintain, less resilient, and carry a higher degree of security risk. Often, they cannot be easily replaced because many core, mission-related functions rely on them and budgets cannot always keep up with changes in technology.

Agencies are obliged to provide secure and reliable information and services to both the citizens they serve and the workforce they support. As the need to provide citizens access to information grows, the public sector continues to be an active target for cybersecurity attacks.

The 2016 PCLS report contains information about 82 projects from 29 agencies totaling an estimated funding request of $379 million. The data is represented in four categories of combined cybersecurity risk and legacy modernization risk as follows:

Table 1 - Prioritization Overview

Cybersecurity risk	Legacy risk	Number of projects
Higher	Higher	9
Higher	Lower	18
Lower	Higher	15
Lower	Lower	40

1.2. Methodology

DIR's Enterprise Solutions Services (ESS) and Office of the Chief Information Security Officer (OCISO) teams worked collaboratively with the Legislative Budget Board (LBB) and affected state agencies throughout the process to carry out this prioritization in the following four phases:

1. Strategize— Evaluate HB 1 (84R), Article IX, Section 9.10, then formulate a plan to collect data and report to state leadership
2. Gather—Develop a data entry mechanism and train agencies to populate the data
3. Analyze—Validate and analyze the data submissions, then formulate recommendations
4. Report—Produce a prioritization report for the LBB and state leadership

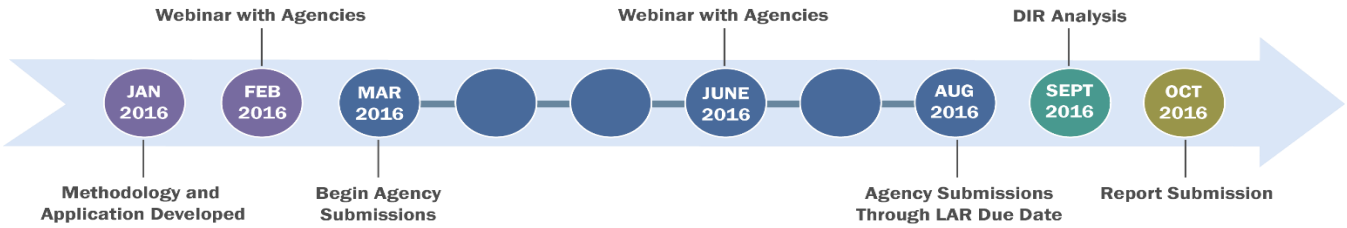

Figure 1 - Timeline

Agencies provided information about each project that addressed the purpose, approach, desired outcome, and value of their projects. Agencies identified whether the requested project will be funded as an exceptional item or through their existing appropriations, and whether there are federal or grant funds tied to the project.

Projects were classified by agencies as either Cybersecurity, Legacy Systems Modernization, or a combination of both, and were submitted at the same time as their Legislative Appropriations Request (LAR). Agencies were asked to identify their project by a name reference that would be used consistently in their LAR and the Prioritization of Cybersecurity and Legacy Systems report. DIR did not assess the methodology, architecture, or solutions for the projects.

Metrics were obtained from a weighted scoring of:

- Assessment of the status of legacy systems
- Extent of remediation to legacy environments
- Effective implementation of recommendations from the Legacy Systems Study
- A self-assessment of the probability and impact of cybersecurity failure
- Residual risk of their overall cybersecurity program

1.3. Approach

To provide consistent data collection with strong security controls, DIR leveraged the Texas Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) for:

- Data input by agencies
- Integration with Legacy System Study metrics
- Score calculation

The prioritization (score) of each Cybersecurity project was based on a ranking of the agency's self-assessment of the risk of cybersecurity failure. Agencies answered security assessment questions which provided a consistent characterization of failure probability and resultant impact for their systems, relative to industry standards.
Probability is the likelihood or frequency that harm will come to the agency or the state because of weakness or exposure. This was determined by identifying how easily this weakness can be exploited, what incentive someone might have to gain access or cause damage to the agency or state's information assets, and the safeguards currently in place to protect the assets. The Impact was determined based on the costs to the agency or the state, both tangible (e.g. human safety or monetary losses) and intangible (e.g. damage to reputation, brand name, or trust).

The prioritization (score) of each Legacy Systems modernization project was based on the agency's projection of cost vs. benefit, the breadth of the environment being addressed, and the relevance of the project to business applications' findings from the legacy systems study performed in 2014. Agencies were instructed to describe metrics they will use for tracking Return on Investment (ROI) and an explanation of the methodology used to identify the benefit and cost values. The set of instructions to agencies provided a standard comparison of projects.

The analysis method groups all projects into four (4) main quadrants across a distribution of legacy remediation scoring and cybersecurity risk.

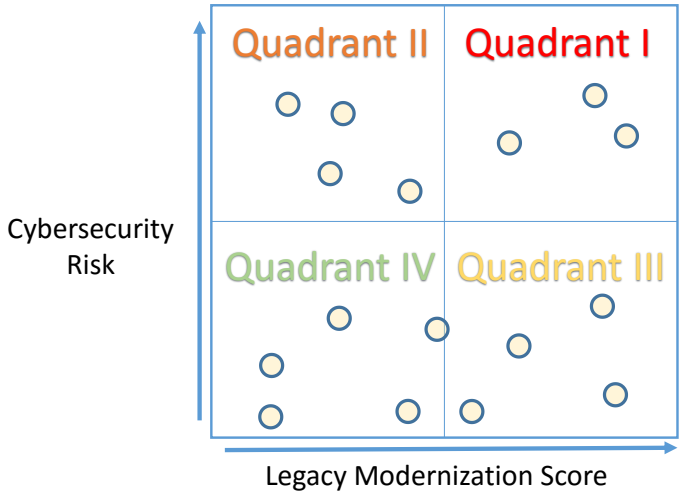

Figure 2 - Example Cybersecurity & Legacy Quadrant Chart

The chart indicates groupings ordered numerically from one to four, with quadrant one being the highest focus and quadrant two being the second, and so on.
The quadrants are then effectively associated with the following risk categorization:

Table 2 - Risk Categorization by Quadrant

Cybersecurity risk	Legacy risk	Number of projects	Quadrant
Higher	Higher	9	I
Higher	Lower	18	II
Lower	Higher	15	III
Lower	Lower	40	IV