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

October 1, 2018

Texas Department of Information Resources

PUBLIC REPORT

1. Public Report

1.1. Overview

SB 1 (85R), Article IX, Section 9.10 (General Appropriations Act) required the Department of Information Resources (DIR) to submit to the Legislative Budget Board a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems to be considered for funding. Texas Government Code, Section 2054.571 defines a legacy system as a computer system or application program that is operated with obsolete or inefficient hardware or software technology. To be included in this prioritization, 80 state agencies, excluding institutions of higher education, were provided the opportunity 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).

DIR was first tasked by the 84th Legislature, Regular Session, 2015, with conducting a prioritization of agency cybersecurity and legacy modernization projects. Building on the effort and methodology of the 2016 Prioritization of Cybersecurity and Legacy Modernization Projects, DIR has developed the 2018 report using improved data collection and methods, including agency self-assessments of applications for cybersecurity and legacy components.

Much like the physical infrastructure of public bridges and roads, IT infrastructure must be maintained to ensure continuity of service to the public. Legacy systems are more difficult and costly to maintain, less resilient, and typically carry more cybersecurity risk. However, they cannot be easily replaced because many core, mission-related functions rely on them and budgets cannot always keep up with changes in technology.

Additionally, 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.

This report contains information about 67 projects from 28 agencies totaling an estimated funding request of $482 million. The analysis of project submissions is represented in categories of cybersecurity risk and legacy modernization risk as follows:

Table 1 - Prioritization Overview by Risk

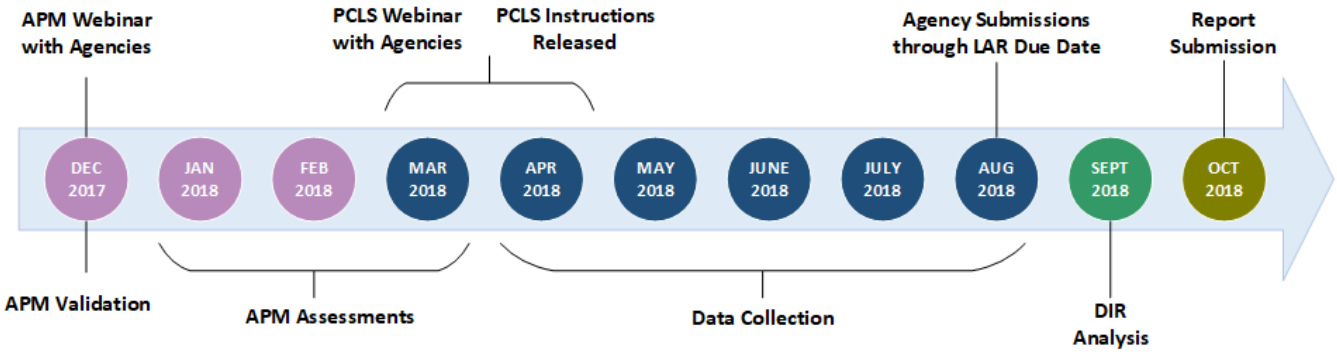
Cybersecurity risk	Legacy risk	Number of projects
High	High	6
High	Low	11
Low	High	22
Low	Low	28

1.2. Methodology Overview

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 state agencies throughout the process to carry out this prioritization in the following four phases:

1. Strategize— Evaluate SB 1 (85R), 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—Develop a prioritization report for the LBB and state leadership

Figure 1- Timeline



In January 2018, agencies were asked to inventory their business applications and perform Application Portfolio Management (APM) assessments on those applications. Each application had four sections with varying numbers of questions about the application: Technical, Financial, Architecture, and Business. Each of these sections were developed from the 2014 Legacy Systems Study methodology, and each response was assigned a value. The goal of the assessments was to enable agencies to determine the most appropriate actions for handling the future of those applications.

Agencies provided information about each project that addressed the purpose, approach, desired outcome, and value of their projects. Projects were classified by agencies as either Cybersecurity, Legacy Systems Modernization, or a combination of both. 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.

Project questionnaires were submitted at the same time as their Legislative Appropriations Request (LAR) and each project was assigned a unique PCLS Tracking Key for agencies to submit in their LAR and for tracking project funding requests throughout the budgeting process. 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 business applications
- Extent of remediation to legacy environments
- A self-assessment of the probability and potential impacts of a cybersecurity-related failures

- Residual risk of organizational cybersecurity

The analysis groups projects into one of four main quadrants across a distribution of legacy remediation and cybersecurity risk scores. The chart displays groupings ordered from one to four, with legacy modernization priority score displayed across the horizontal x-axis and cybersecurity risk displayed along the vertical y-axis. This classification generally results in combination projects with higher cybersecurity risk and higher legacy risk in quadrant one, higher cybersecurity risk projects with lower legacy risk in quadrant two, higher legacy priority and lower cybersecurity risk projects in quadrant three, and lower scores for both categories in quadrant four.

Figure 2- Example Cybersecurity and Legacy Quadrant Chart

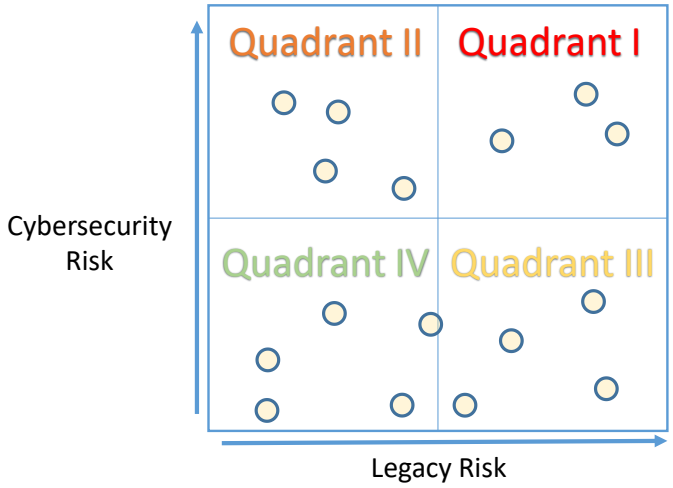


Table 2 - Risk Categorization by Quadrant

Cybersecurity risk	Legacy risk	Number of projects	Quadrant
High	High	6	I
High	Low	11	II
Low	High	22	III
Low	Low	28	IV