Prioritized Cybersecurity and Legacy Systems (PCLS) Study Report to the Legislative Budget Board (LBB)

Public Report - October 30, 2020

Contents

List of Figures

List of Tables

1. Prioritization Methodology and Approach

1.1. Overview

Section 2054.069 of the Government Code, requires the Texas Department of Information Resources (DIR) to submit to the Legislative Budget Board (LBB) a report that prioritizes state agency cybersecurity projects and projects to modernize or replace legacy systems to be considered for funding. Section 2054.571 of the Government Code defines a legacy system as a computer system or application program that is operated with obsolete or inefficient hardware or software technology. DIR submits this Prioritization of Cybersecurity and Legacy Systems Projects (PCLS) report to meet this requirement.

To be included in this prioritization, DIR provided the opportunity for 80 state agencies, excluding institutions of higher education, to submit information about their cybersecurity and legacy systems modernization projects through the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM).

DIR leverages information submitted by state agencies along with Legislative Appropriations Request (LAR) and the Biennial Operating Plan (BOP) to compile the PCLS report where projects are ranked and assessed.

For each legislative session's report, DIR evolves the analysis and scoring of the information submitted to best align with the changes in the technology and marketplace. This year's cybersecurity projects are evaluated as initiatives which purpose improves the overall organization's cybersecurity, enhances the organization's capability to identify, detect, protect, respond, or recover from cybersecurity threats and vulnerabilities, or will improve the organization's cyber maturity as measured in the biennial information security plan.

The 2020 report contains information about 59 projects from 27 agencies totaling an approximate funding request of $898.6 million. The analysis of project submissions is represented in categories of cybersecurity risk and legacy modernization risk and represented in quadrants.

Quadrants are defined by the statistically derived quartiles with slight modification through clustering of similarly rated prioritization scores across the distribution of all project scores.

Table 1 - Quadrant Distribution

Quadrant	Project Count
Quadrant I	12
Quadrant II	24
Quadrant III	15
Quadrant IV	8
Total	59

1.2. Methodology Overview

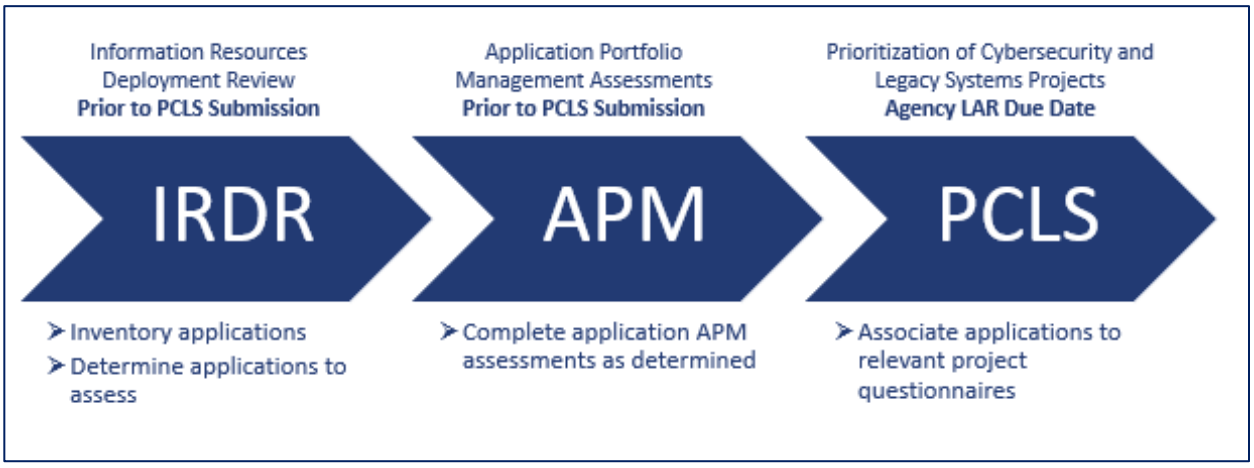
DIR's Enterprise Solutions Services (ESS) and Office of the Chief Information Security Officer (OCISO) teams worked collaboratively with the LBB and state agencies throughout the process to carry out this prioritization in the following four phases:

1. **Strategize**— Update the PCLS questionnaire, inform agencies about the changes, and formulate a plan to collect data, analyze, and report to state leadership.
2. **Gather**—Develop a data entry mechanism using the SPECTRIM tool and train agencies to populate the data. Instructions to submit the PCLS questionnaire was published on June 25, 2020.
3. **Analyze**—Validate and analyze the data submissions, then formulate recommendations.
4. **Report**—Develop a prioritized report for the LBB and state leadership. A preliminary report was submitted on October 1, 2020, followed by this supplemental report on October 30, 2020.

DIR determines project prioritization based on agencies' responses to the biennial Information Resources Deployment Review (IRDR), the PCLS project questionnaire, and the Application Portfolio Management (APM) assessment responses of the business applications associated with each project. The PCLS project questionnaire provides agencies with the opportunity to demonstrate the risks and potential impacts of not funding cybersecurity or legacy systems modernization projects.

DIR provided instructions to state agencies for completing questionnaires. Agencies used the DIR SPECTRIM portal to submit their PCLS project questionnaire responses. Only PCLS project questionnaires submitted through the SPECTRIM portal by the submission deadline were considered for prioritization.

Figure 1 - Legacy Systems Process Flow



1.3. Project Classification and Criteria

In prior PCLS reports, projects were classified as legacy modernization, cybersecurity, or a combination of both. For prioritization submitted before the 87th Legislature, DIR instructed agencies to select only one project type for improved standardization of project comparisons.

Cybersecurity projects must possess at least one of the following criteria:

- The project's primary purpose improves the organization's cybersecurity or enhances the organization's capability to identify, detect, protect, respond, or recover from cybersecurity threats and vulnerabilities.
- The project has clear objectives that will improve the organization's cyber maturity as measured in the biennial information security plan.

Legacy Modernization projects must possess at least one of the following criteria:

- The project's primary purpose modernizes the agency's legacy systems as defined in Section 2054.571 of the Government Code.
- The project primarily supports continued systems currency by monitoring the agency's application portfolio and information technology infrastructure.

1.4. Questionnaire Components

DIR provided the PCLS questionnaire to state agencies ahead of LAR deadlines. Table 2 provides an overview of the PCLS questionnaire components for the applicable project type.

Table 2 - PCLS Questionnaire Components

Section	Content	Project Type
Part 1: General information	Project narrative, project type, LAR/funding information and project characteristics	Cybersecurity Legacy modernization
Part 2: Associated business applications	Business application information – related applications and indirectly impacted applications	Cybersecurity Legacy modernization
Part 3: Cybersecurity issues and controls	Cybersecurity issues and cybersecurity controls	Cybersecurity
Part 4: Legacy issues	Modernization benefits, cost-benefit analysis and methodology, modernization scope (servers & software), system characteristics	Legacy modernization
Part 5: Probability determination	Incentive, control effectiveness, control reliability, threat event frequency, asset exposure	Cybersecurity
Part 6: Impact determination	Operational impacts, physical impacts, legal impacts, financial impacts	Cybersecurity

Agencies submitted responses to project questionnaires at the same time as their LAR. Each project is 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 agency projects.

DIR derived metrics 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

Contact: For more information on PCLS, please contact Krishna Edathil, Director of Enterprise Solution Services at krishnakumar.edathil@dir.texas.gov or (512) 475-4541