DIR
Texas Department of Information Resources
Transforming How Texas Government Serves Texans

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

September 30, 2022

Contents

List of Figures

List of Tables

1. Prioritization Methodology and Approach

1.1. Overview

Section 2054.069 of the Texas Government Code requires the Texas Department of Information Resources (DIR) to submit to the Legislative Budget Board (LBB) a report that "prioritizes, for the purpose of funding, state agency cybersecurity projects and projects to modernize or replace legacy systems" by October 1 of each even numbered year. 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 the statutory 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 the responses to the PCLS project questionnaire, the biennial Information Resources Deployment Review (IRDR), and the Application Portfolio Management (APM) assessment of the business applications associated with each PCLS project to compile the PCLS report.

For each biennial report, DIR evolves the analysis and scoring of the information submitted to best align with the changes in the technology and marketplace. This year, DIR evaluated cybersecurity projects as initiatives that improve the organization's cybersecurity, enhance 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 2022 report contains information about 95 projects from 32 agencies totaling an approximate funding request of $927 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	27
Quadrant II	23
Quadrant III	23
Quadrant IV	22
Total	**95**

1.2. Methodology Overview

To assess and prioritize the projects for this report, DIR's Chief Technology Office (CTO) and the Office of the Chief Information Security Officer (OCISO) teams worked collaboratively with the LBB and state agencies in the following four phases:

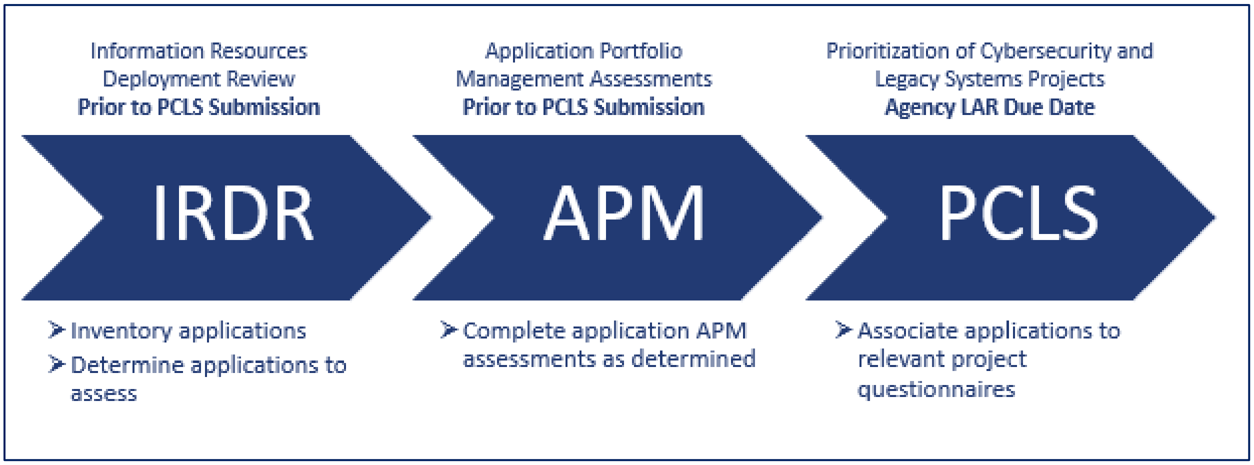
1. **Strategize** — Update the PCLS questionnaire, inform agencies about any changes from the prior PCLS questionnaire, and formulate a plan to collect data, analyze, and report to state leadership.
2. **Gather** — Develop a data entry mechanism using the SPECTRIM tool and train agencies to populate the data. DIR published the instructions on submitting the PCLS questionnaire in June 2022.
3. **Analyze** — Validate and analyze the data submissions, then formulate recommendations.
4. **Report** — Develop a prioritized report for the LBB and state leadership for submission on September 30, 2022.

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.

Responding to the PCLS project questionnaire provided agencies the opportunity to demonstrate the risks and potential impacts of not funding cybersecurity or legacy systems modernization projects.

DIR provided state agencies instructions for completing the PCLS questionnaires before the LAR deadlines. DIR only considered for prioritization those PCLS project questionnaires submitted through the SPECTRIM portal by the submission deadline.

Figure 1 - Legacy Systems Process Flow


Information Resources Deployment Review
Prior to PCLS Submission
IRDR
➢ Inventory applications
➢ Determine applications to assess
Application Portfolio Management Assessments
Prior to PCLS Submission
APM
➢ Complete application APM assessments as determined
Prioritization of Cybersecurity and Legacy Systems Projects
Agency LAR Due Date
PCLS
➢ Associate applications to relevant project questionnaires

1.3. Project Classification and Criteria

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

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 and software), and system characteristics	Legacy modernization
Part 5: Probability determination	Incentive, control effectiveness, control reliability, threat event frequency, and asset exposure	Cybersecurity
Part 6: Impact determination	Operational impacts, physical impacts, legal impacts, and financial impacts	Cybersecurity

Each project is assigned a unique PCLS Tracking Key for agencies to submit in their LAR and to track project funding requests throughout the budgeting process. DIR did not assess the methodology, architecture, or solutions of the 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; and
- Residual risk of organizational cybersecurity.

Contact: For more information on PCLS, please contact John Hoffman, CTO, Deputy State CIO at John.Hoffman@dir.texas.gov or (512) 936-2501