Tech Debt Portfolio Fact Sheet

Updated
Nov. 2022

COLORADO
Governor's Office of
Information Technology

Executive Summary

The Technical Debt Remediation Portfolio is a group of projects and programs that work together to build a foundation to support a modern state government with a growing number of online services. The projects focus on removing, updating or replacing older technology.

Key work includes: modernizing mainframe-based legacy applications and decommissioning the mainframe, moving from a leased data center (eFORT) to a state-owned data center or the Cloud & securing Salesforce application vulnerabilities.

Value

- Reduces costs associated with maintaining older technologies.

- Implements new, secure and supported technologies with plans for operations and maintenance to reduce future technical debt.

- Reduces the state's data center footprint and saves money by eliminating an expensive data center lease.

- Encourages cloud adoption and cloud modernization opportunities.

Major Business Impacts

- There will be occasional impacts to agencies as each project within the first phase of the Tech Debt Portfolio remediation work gets underway.

- Agencies can expect to be informed in advance of work that will or has the potential to interrupt business operations.

- Agencies can expect to be consulted about the timing of work that requires agency participation for testing.

Project Timeline

Projects within the tech debt portfolio will run concurrently beginning in July 2022. All work within the first phase of the tech debt remediation portfolio will be completed by June 30, 2024.

More Information

For more information, please contact your IT Director.

What is Tech Debt?

Technical debt is the cost of maintaining legacy technology - a challenge faced by both the public and private sectors. The state has an estimated $465 million in tech debt—the cost of equipment and staff time to keep unsupported and insecure older technology running to deliver services—stemming from aging infrastructure, end-of-life applications and systems with security vulnerabilities. When it isn't addressed, the consequences can be severe, and its impacts stretch across organizations.