Salesforce Security Vulnerabilities Remediation FAQ

This FAQ is a living document and will continue to be updated as more information becomes available. If you have a question that needs to be answered in this FAQ, contact Jeff Blitstein at jeffrey.blitstein@state.co.us.

General Information

1. **What is the Salesforce Security Vulnerabilities Remediation Project?**

   Security vulnerabilities within Salesforce applications have been identified as a priority in our work to reduce technical debt for the state. Salesforce applications were scanned for code vulnerabilities in May 2022 and ranked high, medium and low. The Salesforce Security Vulnerabilities Remediation project will identify and remediate each application's high and medium vulnerabilities at no cost to the agency. Other projects will cover some remediation that isn't within this project's scope. Scans will be re-run to ensure accuracy before beginning work.

2. **Why has OIT made this project a priority?**

   As part of our ongoing process of shoring up technical debt for the State, the primary goal of this project is to identify and remediate the high and medium vulnerabilities for each application at no cost to the agency. Additionally, we will update retiring application interfaces (APIs) that are no longer needed and security settings if needed. APIs are the connections between two applications that allow applications to "talk to each other" and work together. Priority will be given to those applications with the highest and medium vulnerabilities taking availability into account.

3. **Who is affected?**

   The state agencies with high and medium security vulnerabilities include the **Colorado Department of Human Services (CDHS), Colorado Department of Labor and Employment (CDLE), Colorado Department of Transportation (CDOT), Colorado Department of Public Safety (CDPS), Department of Natural Resources (DNR), Department of Local Affairs (DOLA), Department of Revenue (DOR), the Governor's Office (GOV), and Health Care Policy & Financing (HCPF).**

The OIT team will need to coordinate remediation work with any ongoing development in the affected Salesforce application. The project team will coordinate with agencies to determine a window for remediation. Once determined and high and medium vulnerabilities are remediated in a sandbox environment, the Salesforce applications must be tested. To ensure that the repairs are working as intended with no impact on the application, one or two subject matter experts (SMEs) will be needed to test the application. If an agency has insufficient time or resources for testing, the project team will provide internal OIT testers. The project team will need input from those with experience with the individual applications.

4. **When will this happen?**

   The project kicked off the week of July 25, 2022. The project will be completed in two-week sprints (two-week work periods). The project is expected to be completed by November 2023.

5. **How will it be completed?**

   There will be a focused effort on several agencies simultaneously, which will minimize confusion, maximize output and deliver quick wins.

   Remediation and testing are application-driven, meaning that work will be done not by agency but by application (which may mean multiple agencies are involved simultaneously). The Salesforce Remediation Project team will alert agencies of the vulnerabilities remediation affecting their business and determine if SMEs are necessary for the agency to test and verify that the solutions are working for their applications.