COLORADO
Governor's Office of Information Technology

# 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 not answered in this FAQ, contact Jeff Blitstein at jeffrey.blitstein@state.co.us.

## General Information

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

   The OIT Salesforce team has initiated a security remediation project for all affected Salesforce applications. All Salesforce applications were scanned for code vulnerabilities in mid-2022. Vulnerabilities are ranked high, medium and low. Some remediation will be covered separately or through other projects. 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 APIs and security settings if needed. Priority will be given to those applications with the highest and medium vulnerabilities taking availability into account.

3. **Who is affected?**

   Practically every agency, in some way.
   - Departments with high and medium security vulnerabilities include **CDHS, CDLE, CDOT, CDPS, DNR, DOLA, DOR, GOV, and HCPF.**
   - Remediation work by the OIT team will need to be coordinated with any ongoing development in the affected Salesforce application. The project team will coordinate with agencies to determine a window where remediation can be performed. 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 to dedicate to 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, and is estimated to take 46 weeks. The project will be completed in two-week sprints (two-week periods of work). The project is expected to be completed by the end of June 2023.

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

   - Focused effort on several agencies at the same time, 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 at once).
   - Next Steps
     - 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.