COALFIRE

Date: December 1, 2023

From: Coalfire Systems

To: Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Subject: *Google Services NIST SP 800-171 Rev 2 Compliance*

The purpose of this letter is to provide Google customers with an independent perspective on Google's implementation of NIST SP 800-171 requirements within the Google Services information system for the 2022 – 2023 reporting period. This evaluation is limited to the infrastructure and products that are part of the Google Services FedRAMP Authorization boundary as outlined on the FedRAMP Marketplace.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services. As an accredited FedRAMP Third Party Assessment Organization (3PAO), Coalfire Systems (Coalfire) performs independent security assessments for cloud service provider offerings such as Google Services. As a 3PAO, Coalfire is required to meet strict accreditation requirements that ensure assessment independence and integrity. FedRAMP is recognized within the industry as one of the most comprehensive risk assessment programs for commercial or government agency cloud environments.

From September 12, 2022, to March 10, 2023, Coalfire performed a FedRAMP High baseline annual assessment of Google Services. The assessment included security control analysis, vulnerability scanning, and penetration testing, the results of which are documented in the Google Workspace FedRAMP Security Assessment Report (SAR), dated March 28, 2023.

Following the FedRAMP Assessment, Coalfire performed comparative analysis of the FedRAMP baseline against the NIST SP 800-171 requirements and determined that requirements were tested as part of FedRAMP assessment activities. Through an evaluation of Appendix D of NIST SP 800-171 Rev 2, assessors noted that each of the NIST 800-53 controls correlated to CUI controls were evaluated during the standard Google Services annual assessment cycle.

Through the evaluation of NIST 800-171, Coalfire observed the following deviation from control requirements:

- **NIST SP-800-171 controls: 3.11.3** – Remediate vulnerabilities in accordance with risk assessments (mapped and associated NIST SP 800-53 rev4 controls: RA-5).
  Coalfire noted a single moderate vulnerability recorded on the system's POA&M that had exceeded a remediation time period of 90 days.
- **NIST SP-800-171 control: 3.5.6** – Disable identifiers after a defined period of inactivity.
- **NIST SP-800-171 control: 3.5.7/3.5.8** – Enforce a minimum password complexity and change of characters when new passwords are created, Prohibit password reuse for a specified number of generations (mapped and associated NIST SP 800-53 rev4 controls: IA-5(1)).

The deviations described present a risk that is exceptionally low due to compensating controls. As a result, and noting the deviation above, Coalfire concludes that Google has implemented the required NIST SP 800-171 controls for its Google Services cloud service offering.

Coalfire is a leading FedRAMP 3PAO and has built a reputation on the comprehensiveness of the assessments that we provide to our clients on behalf of the US Government. We stand behind all the work we perform and put forth unbiased deliverables outlining the results of assessment activities.

Sincerely,

Adam Smith

Director, FedRAMP & Assessment Services
Coalfire Systems