Date: November 9, 2023

From: Coalfire Systems

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

Subject: *Google Workspace 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 Workspace information system for the 2022 – 2023 reporting period.

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 Workspace. 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 April 21, 2023, Coalfire performed a FedRAMP High baseline annual assessment of Google Workspace. 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 April 21, 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. During the assessment, it was noted that Google Workspace is built to leverage the Google Services system, with many control requirements being directly inherited from this infrastructure. Additionally, it was noted during testing that Workspace is highly customizable and that customers carry a degree of responsibility for implementing NIST 800-171 requirements in alignment with their organizational objectives.

For requirements that are not inherited from Google Services, Coalfire observed the following deviation from NIST SP 800-171 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 low vulnerability recorded on the system's POA&M that had exceeded a remediation time period of 180 days.

The deviation described presents 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 Workspace cloud service offering.

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

Sincerely,

Adam Smith

Director, FedRAMP & Assessment Services
Coalfire Systems