Date: May 27, 2022

From: Coalfire Systems

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

Subject: *Letter of Attestation – Google Services NIST 800-171 Compliance*

The purpose of this letter is to provide Google Services (Google Cloud Platform (GCP) and Google Workspace) customers assurance that Google Services is operating in compliance with the requirements of NIST SP 800-171 (CUI) for the 2021 – 2022 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 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 13, 2021 to May 20, 2022, 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 Services FedRAMP Security Assessment Report (SAR), dated May 20, 2022.

Following the FedRAMP Assessment, Coalfire performed comparative analysis of the Google Services FedRAMP Package against the NIST SP 800-171 requirements and determined that requirements were tested as part of FedRAMP assessment activities. Coalfire observed the following deviations from NIST SP 800-171 requirements:

1. NIST SP-800-171 controls: 3.1.9 – Provide privacy and security notices consistent with applicable CUI rules (mapped and associated NIST SP 800-53 rev4 controls: AC-8)
2. NIST SP-800-171 controls: 3.1.10 - Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity (mapped and associated NIST SP 800-53 rev4 controls: AC-11)
3. NIST SP-800-171 controls: 3.5.6 – Disable identifiers after a defined period of inactivity (mapped and associated NIST SP 800-53 rev4 controls: AC-2 (3) and IA-4)
4. NIST SP-800-171 controls: 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))

It should be noted that all of these vulnerabilities present risks that are exceptionally low due to compensating controls. As a result, Coalfire concludes that Google has implemented the required NIST SP 800-171 controls with all deviations noted above.

Coalfire is the leading 3PAO of the FedRAMP program, having performed the most assessments to-date. Our reputation has been built on the comprehensiveness of our assessments that we provide to our clients and the overall thoroughness of our reviews 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. Any recommendations for authorization are based off the results of our review and presented to the US Federal Government for their authorization determination.

Sincerely,

Adam Smith

Director, FedRAMP & Assessment Services
Coalfire Systems