COALFIRE

Coalfire Systems, Inc.
11000 Westmoor Circle, Suite 450
Westminster, CO 80021

December 22, 2017

To Whom It May Concern:

The purpose of this letter is to provide Google Services (Google Cloud Platform (GCP) and G Suite) customers assurance that Google Services is operating in compliance with requirements of NIST SP 800-171 (CUI) for the 2017 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 June 19, 2017 to October 15, 2017, Coalfire performed a FedRAMP Moderate baseline assessment of Google Services. The assessment included security control analysis, vulnerability scanning, and penetration testing. The results of assessment activities are documented in the Google Services FedRAMP Security Assessment Report (SAR), dated November 1, 2017. As of the date of this letter, Google's FedRAMP Package is being reviewed and Provisional ATO is expected on February 7, 2018.

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: 3.1.8 – Limit unsuccessful logon attempts (mapped and associated NIST SP 800-53 rev4 controls: AC-7)
2. 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)
3. 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))
4. NIST SP-800-171 controls: 3.8.4 – Mark media with necessary CUI marking and distribution limitations (mapped and associated NIST SP 800-53 rev4 controls: MP-3)

It should be noted that all of these risks are operationally required for continued operation of Google Services and that that the risks 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. Any questions regarding Coalfire's 2017 assessment of Google Services can be directed by email to Matthew.Houy@Coalfire.com.

Sincerely,

Matthew Houy

Matthew Houy

DIRECTOR | FEDRAMP ASSESSMENT SERVICES

COALFIRE | Coalfire.com | (C) 210.663.6825
22630 Davis Drive | Suite 225 | Sterling | Virginia 20164