COALFIRE

Date: March 7, 2022

From: Coalfire Systems

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

Subject: *Letter of Attestation – Adherence of Google Services with the MARS-E Framework*

During the period of 02/01/2022 and 03/04/2022, Coalfire, an A2LA accredited FedRAMP Third-Party Assessment Organization (3PAO), performed an annual FedRAMP High security assessment of the Google Services information system. The results of the assessment indicate that Google has effectively implemented security controls to maintain the security and privacy of the Google Services information system. The methodology used to conduct the security assessment of Google Services was based upon the Risk Management Framework outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems. The Google Services Security Control Assessment was performed in accordance with NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations.

The Minimum Acceptable Risk Standards for Exchanges (MARS-E), Volume 1: Harmonized Security and Privacy Framework, Version 2.2, is part of a suite of documents which addresses the mandates of the Patient Protection and Affordable Care Act of 2010. The documents define a risk-based security and privacy framework for use in the design and implementation of Exchange Information Technology (IT) systems. The MARS-E Document Suite presents the comprehensive body of Affordable Care Act security and privacy controls. The structure of the MARS-E is based on NIST SP 800-53 Rev 4 and uses the same control family numbering, descriptions, and control requirements.

Currently, there is no formal authorization and accreditation process for MARS-E. However, Google has requested that Coalfire, an independent third-party assessment organization, perform a comparison of the controls listed in the MARS-E Catalog of Security and Privacy controls and contrast it against the assessment activities performed in evaluating the FedRAMP standard.

Google Services is currently authorized at the FedRAMP High baseline by the Joint Authorization Board (JAB). In comparing the MARS-E control catalog against FedRAMP High's requirements, Coalfire concluded that there is a significant overlap between the MARS-E control standard and the NIST 800-53 Rev 4 controls that have been evaluated as part of the FedRAMP High security assessment.

All FedRAMP High baseline security controls, including overlapping controls required for MARS-E compliance, were tested during the system's initial FedRAMP assessment. Following FedRAMP High authorization on 11/22/2019, the system's control assessment schedule has been regulated by the FedRAMP Annual Assessment Guidance, version 2.0, dated 11/24/2017. Google adheres to the requirement that a 3PAO assess all FedRAMP core controls, historical control findings, and roughly one

third of the remaining NIST SP 800-53 rev. 4 Moderate baseline controls on an annual basis. This ensures that all controls are tested at least once during the three-year continuous monitoring cycle.

Coalfire attests that the controls noted for Google's FedRAMP High authorization provides significant coverage of the MARS-E requirements. Of the 255 controls included in MARS-E 2.2, FedRAMP High provides coverage for 206, leaving a delta of 49 differential controls. These 49 controls have not been historically part of the scope of Coalfire's FedRAMP evaluation of Google Services, and include the following:

Control Family	Control Listing
Access Control (AC)	AC-3 (9)
Configuration Management	CM-4 (2)
Maintenance (MA)	MA-4 (1)
Physical and Environmental Protection (PE)	PE-2 (1)
System and Services Acquisition (SA)	SA-22
System and Communications Protection (SC)	SC-8(2), SC-32, SC-ACA-1, SC-ACA-2
Program Management (PM)	PM-1, PM-2, PM-3, PM-4, PM-5, PM-6, PM-7, PM-8, PM-9, PM-10, PM-11, PM-12, PM-13, PM-14, PM-15, PM-16
Privacy: Authority and Purpose (AP)	AP-1, AP-2
Privacy: Accountability, Audit, and Risk Management (AR)	AR-1, AR-2, AR-3, AR-4, AR-5, AR-6, AR-7, AR-8
Privacy: Data Quality and Integrity (DI)	DI-1 (1), DI-1 (2),
Privacy: Data Minimization and Retention (DM)	DM-1, DM-2, DM-3 (1)
Privacy: Individual Participation and Redress (IP)	IP-1, IP-2, IP-3, IP-4(1)
Privacy: Security (SE)	SE-1, SE-2
Privacy: Transparency (TR)	TR-3
Privacy: Use Limitation (UL)	UL-1, UL-2

Based on the thorough evaluation of the information system, Coalfire concludes that Google Services is in compliance with the MARS-E 2.2 standard based on the most recent FedRAMP Security Assessment Report as well as the testing of the additional controls listed above.

All statements in this attestation are valid as of the date of this letter.

Sincerely,

Timothy P. O'Brien

Tim O'Brien

Senior Manager, FedRAMP & Assessment Services
Coalfire Systems