

Date: February 14, 2025
From: Coalfire Systems
To: Google LLC
 1600 Amphitheatre Parkway
 Mountain View, CA 94043
Subject: *FedRAMP High (NIST 800-53r5) Compliance of Google Maps Platform*

The purpose of this letter is to provide Google Maps Platform customers assurance that the listed service offerings are operating in compliance with the requirements of the FedRAMP High* Authorization for the 2024-2025 reporting period. The FedRAMP High baseline is a set of 411 NIST SP 800-53 revision 5 controls and additional requirements (including vulnerability scanning, penetration testing, and continuous monitoring) to be assessed to determine adequacy of security of a High impact system (loss of confidentiality, integrity, and availability would result in serious adverse effects on customer operations, assets, or individuals).

Google Maps Platform Offerings*		
Air Quality API	Maps Static API	Consumer SDK for Android
Pollen API	Street View Static API	Consumer SDK for iOS
Solar API	Address Validation API	Driver SDK for Android
Advanced Markers	Geocoding API	Driver SDK for iOS
Aerial View API	Geolocation API	Fleet Engine API
Data Driven Styling (DDS) for Datasets	Places API	JavaScript Journey Sharing Library
Elevation API	Places SDK for Android	Location Selection API
Map Tiles API	Places SDK for iOS	Navigation SDK for Android
Map Tiles API (2D Tiles)	Time Zone API	Navigation SDK for iOS
Map Tiles API (3D Tiles)	Directions API	Route Optimization API
Maps Datasets API	Distance Matrix API	Route Overview API
Maps Embed API	Roads API	SearchVehicles API
Maps JavaScript API	Routes API	Shipment Tracking
Maps SDK for Android	Routes Preferred API	Trip and Order Progress
Maps SDK for iOS		

Table 1 – GMP products submitted for FedRAMP Authorization

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) conducts independent security assessments for cloud service provider offerings such as Google Services and Google Maps Platform.. 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. Services that are denoted with an asterisk (*) may not be restricted to US location for data storage

or processing as documented within the SA-9(5) requirement. Please review the JAB P-ATO letter for more information.

From August 26, 2024 to January 31, 2025, Coalfire performed a FedRAMP High baseline annual assessment of Google Services to include the Google Maps Platform offerings. The assessment included security control analysis, vulnerability scanning, and penetration testing.

As a result of assessment activities, Coalfire concludes that Google has implemented NIST SP 800-53 Revision 5 security controls in compliance with the FedRAMP High baseline and that all deviations from the baseline are being tracked and remediated in accordance with FedRAMP guidance.

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 on the results of our review and presented to the US Federal Government for their authorization determination.

Let us know if you have any questions or concerns.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Timothy O'Brien", with a long, sweeping underline.

Timothy O'Brien - Director, FedRAMP & Assurance Services - Coalfire Systems