Coordinated Privacy Disclosure, Final Report

Official WhiteHouse.gov Android App (gov.whitehouse.app)

Executive Office of the President of the United States

DELIVERY PERMANENTLY FAILED ON BOTH ADDRESSES · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, 90 DAYS AFTER INITIAL DISCLOSURE

Target	The official White House Android application
Package	gov.whitehouse.app, version 47.4.7
Operator	Executive Office of the President of the United States
Initial Disclosure	2026-06-27
Stated Embargo	No literal date was stated in either message; the campaign-wide 90-day default from initial disclosure applies, landing on 2026-09-25.
Report Published	2026-09-25, on the 90-day default date
Regulators	Austrian DSB
Total Outbound Messages	2, on 2026-06-27 and 2026-07-24, to webmaster@whitehouse.gov and privacy@whitehouse.gov.
Inbound Replies	0. Both messages permanently failed delivery: Gmail's own delivery report confirms a final SMTP timeout (Action: failed, Status 4.4.1) on both webmaster@whitehouse.gov and privacy@whitehouse.gov, for both the initial disclosure and the follow-up.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed that the official White House Android app ships a German-language locale package, meaning GDPR Art. 3(2) applies directly to its EU users, and that FirebaseInitProvider initializes at app launch, before any consent screen is shown, meaning Firebase Analytics begins collecting behavioral data the moment a citizen opens the app, with no valid legal basis under Art. 7. This computes to MEDIUM/6.9 under CVSS v4.0.

A second finding, also MEDIUM: the app requests ACCESS_ADSERVICES_AD_ID and ACCESS_ADSERVICES_ATTRIBUTION, permissions designed to attribute app installs to advertising campaigns. Citizens who download the official government app of the United States are, by this mechanism, treated as advertising-conversion events. A third finding, also MEDIUM: a Firebase API key is hardcoded in plaintext in the production resources, permitting unauthenticated calls against the project's quota.

Two further findings correct to LOW. OneSignal, a US-based push-notification provider embedded with 567 compiled classes, includes a full location-tracking stack, LocationModule, LocationController, and nine location-permission sub-classes; a build plugin strips the explicit location permission from the manifest, so the capability is compiled and linked but not exposed at runtime in this build. Separately, the app requests RECORD_AUDIO with no privacy notice disclosing why a government news app needs microphone access beyond media playback. Genuine positives are worth naming and were named directly in the original disclosure: certificate pinning on whitehouse.gov with SHA-256 pins is implemented correctly, cleartext traffic is blocked for all production domains, Firebase App Check with Play Integrity is active, and OTA updates are disabled. These are the habits of a technically capable team; the privacy-compliance layer did not receive the same attention.

Two messages were sent, on 27 June 2026 and again on 24 July 2026, to webmaster@whitehouse.gov and privacy@whitehouse.gov, with the Austrian DSB copied from the second message onward. Delivery itself permanently failed: Gmail's own delivery report confirms a final SMTP timeout (Action: failed, Status 4.4.1) on both addresses for both sends, meaning no byte of either message is confirmed to have reached the target's mail infrastructure at all. The second message explicitly noted the earlier delivery uncertainty to the recipient, before that uncertainty resolved into confirmed permanent failure. No acknowledgment of receipt, automated or human, was ever received on either address. No literal embargo date was stated to the target in either message; the campaign-wide 90-day default from initial disclosure applies, landing on the date of this report's publication.

Scope: Root-level static analysis of the production official White House Android application (gov.whitehouse.app, version 47.4.7), pulled from Google Play and reviewed on 27 June 2026 by an Austrian researcher. No account was created and no interaction with Firebase's or OneSignal's backend infrastructure was performed.

Disposition

Five findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. Pre-consent Firebase auto-initialization, advertising-attribution tracking in a government app, and a hardcoded Firebase API key all correct to MEDIUM. A compiled but disabled location-tracking stack inside a bundled push SDK, and an undocumented microphone permission, both correct to LOW. Two messages were sent, on the day of disclosure and again 27 days later. Both permanently failed delivery on both addresses, confirmed by a final SMTP timeout in Gmail's own delivery report, and no reply of any kind was ever received.

ID	Severity	Title
C1	MEDIUM	Pre-Consent Firebase Auto-Initialization
C2	MEDIUM	Advertising-Attribution Tracking in a Government App
H1	MEDIUM	Firebase API Key Hardcoded in Plaintext
H2	LOW	Compiled Location-Tracking Stack Inside a Bundled Push SDK
M1	LOW	Undocumented Microphone Permission

What the WhiteHouse.gov App Got Right

Certificate pinning on whitehouse.gov, with SHA-256 pins valid until 2027-06-01, is implemented correctly. Cleartext traffic is blocked for all production domains. Firebase App Check with Play Integrity is active. Over-the-air updates are disabled. These are the habits of a technically capable engineering team; the privacy-compliance layer did not receive the same level of attention.

Two Messages, Delivery Never Confirmed, No Reply Ever Received

Two messages were sent, on 27 June 2026 and again on 24 July 2026, to webmaster@whitehouse.gov and privacy@whitehouse.gov, with the Austrian DSB copied from the second message onward. Both permanently failed delivery on both addresses: Gmail's own delivery report confirms a final SMTP timeout (Action: failed, Status 4.4.1) on each. No byte of either message is confirmed to have reached the target's mail infrastructure at all. No acknowledgment of any kind, automated or human, was ever received on either address.

Findings

C1: Pre-Consent Firebase Auto-Initialization

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9.

FirebaseInitProvider (initOrder=100, directBootAware=true) fires at app launch, before any consent screen is shown. Firebase Analytics begins collecting behavioral data the moment a citizen opens the app, with no valid legal basis under Art. 7.

Impact: Behavioral data collection begins before the app's user has had any opportunity to consent or decline, in an application operated by a government executive office.

Fix: Gate Firebase initialization behind a consent mechanism. No confirmation that this has occurred was ever received.

C2: Advertising-Attribution Tracking in a Government App

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9.

The app requests ACCESS_ADSERVICES_AD_ID and ACCESS_ADSERVICES_ATTRIBUTION, permissions designed to attribute app installs to advertising campaigns.

Impact: Citizens who download the official government app are, through this mechanism, treated as advertising-conversion events, a data-minimisation mismatch for an app with no advertising business model.

Fix: Remove the advertising-attribution permissions unless a specific, disclosed purpose requires them. No confirmation that this has occurred was ever received.

H1: Firebase API Key Hardcoded in Plaintext

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N, 6.9.

A Firebase API key is extracted from res/values/strings.xml. This key permits unauthenticated calls against the Firebase project's quota, and misconfigured Firebase Security Rules would allow unauthenticated read or write access to Firestore or Storage.

```
google_api_key: AIzaSyCSeWRGlA-P4_TVdibML1it4BUiL83lcdI
firebase_project: project-cf0140be-fd49-41d2-a5b
```

Impact: Any party can exhaust the project's API quota anonymously, and a security-rules misconfiguration would expose backend data with no additional access barrier.

Fix: Restrict the API key by package name and certificate. No confirmation that this has occurred was ever received.

H2: Compiled Location-Tracking Stack Inside a Bundled Push SDK

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4.

OneSignal, a US-based push-notification provider, is embedded with 567 compiled classes, including a full location-tracking stack (LocationModule, LocationController, nine location-permission sub-classes). A build plugin strips the explicit location permission from the manifest, so the capability is compiled and linked but not exposed in this build's runtime permissions.

Impact: The location-tracking capability exists in the compiled binary even though the current build does not request the runtime permission that would activate it, a latent capability, not an active one.

Fix: Remove the unused location module from the OneSignal integration entirely, instead of relying on a build-time permission strip. No confirmation that this has occurred was ever received.

M1: Undocumented Microphone Permission

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.4.

The app requests RECORD_AUDIO. The expo-audio plugin present in the app covers media playback, but RECORD_AUDIO goes beyond playback. No privacy notice discloses why a government news app needs microphone access.

Impact: Users have no documented explanation for why a news and media application requests microphone recording capability.

Fix: Document the specific purpose for RECORD_AUDIO, or remove the permission if unused. No confirmation that this has occurred was ever received.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 7	C1	Pre-consent Firebase auto-initialization.
Art. 5(1)(b)	C2	Advertising-attribution tracking in a government app.
Art. 32	H1	Firebase API key hard-coded in plaintext.
Art. 46, Chapter V	H2	Compiled location-tracking stack inside a bundled push SDK.
Art. 13	M1	Undocumented microphone permission.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own. In this report, C1, C2, and H1 correct to MEDIUM, and H2 and M1 correct to LOW, all on their own computed bands, with no escalation applied. Disclosure conducted under ISO/IEC 29147 and GDPR Art. 3(2)'s extraterritorial scope for the app's German-language EU-targeted release. REF REF: WHITEHOUSE-2026.