



TECHNICAL BRIEF · BASED ON OIG-26-06 · DHS

76% OF APPS ON DHS I&A MOBILE DEVICES POSED RISKS

76%

OF APPS INSTALLED ON DHS I&A MOBILE DEVICES POSED SECURITY RISKS, WERE PROHIBITED, OR ALLOWED PROHIBITED ACTIVITIES (DHS OIG, NON-GAO)

In April 2026, DHS OIG reported that 76 percent of apps installed on DHS Office of Intelligence and Analysis mobile devices posed security risks, were prohibited, or allowed prohibited activities. DHS concurred with all 11 recommendations, and Oversight.gov listed them as open.

THE FINDING

On April 30, 2026, the DHS Office of Inspector General published [Deficiencies in I&A Mobile Device Security Create Vulnerabilities, Place Information at Increased Risk](#) (OIG-26-06). This is a non-GAO source. DHS OIG audited how the department's Office of Intelligence and Analysis (I&A) and its Office of the Chief Information Officer (OCIO) manage and secure I&A mobile devices, and found they "did not effectively manage and secure" them.

The figure that travelled: 76 percent of apps installed on I&A mobile devices posed security risks, were prohibited, or allowed prohibited activities. [FedScoop](#) reported that the OIG reviewed 650 apps, over an audit period of December 2023 through March 2025. Two I&A-developed apps used to share intelligence with law enforcement and first responders carried three vulnerabilities that I&A knew about and had not fixed.

DHS OIG made 11 recommendations, seven to OCIO and four to I&A's Directorate of Technology and Data Services. Three go to apps: control the vulnerabilities in custom-developed apps, set policies and procedures so component custom-developed apps are evaluated, and make sure user-installed apps are evaluated for security risk. DHS concurred with all 11.

WHY IT KEEPS HAPPENING

The recommendations split the work. The fix for the custom apps' vulnerabilities goes to I&A's directorate, while the policy that says how a custom app gets evaluated goes to OCIO. A vulnerability list can sit with one office while the procedure that would force a fix sits with another.

The device layer adds a second gap. Reporting on the audit says employees could download high-risk apps, including some the department had approved, and that DHS did not prevent installation of unapproved ones. Recommendations 9 through 11 ask for defined inventory ownership, enrollment of OCIO-issued devices in mobile device management (MDM), and unenrollment of devices with no business need.

DHS told reporters it had already made some changes and that unmanaged apps "do not have access to DHS data and services," according to [GV Wire](#). The OIG's recommendations stand regardless, and FedScoop reports that some are resolved but remain open until OIG reviews a closeout letter.

WHY IT MATTERS TO YOUR BID

Mobile security work at DHS shows up in three kinds of requirements: custom app development and sustainment, MDM and mobile threat defense operations, and mobile security assessment. Evaluators scoring an "understanding of the requirement" will have read an OIG report that names unvetted apps in its first paragraph.

The wording matters. Recommendation 3 speaks of "component" custom-developed apps, not only I&A's, so a proposal for another DHS component's app can expect the same question: what evidence shows this app was tested before it reached a government device? An offeror that names the test method, the standard behind the evidence package, and who reviews it answers directly.

Closeout runs on paper too. FedScoop reports that resolved recommendations stay open until the OIG reviews a closeout letter, so DHS needs test reports and vetting packages it can attach.

A separate mobile duty applies to public-facing services. GAO's [Digital Experience: Agency Compliance with Statutory Requirements](#) (GAO-24-106764) listed "mobile-friendly" among eight 21st Century IDEA requirements. That concerns websites and digital services for the public, not workforce devices.

TECHNICAL APPROACH

The method below comes from Avalon's [Mobile Development](#) service. It covers custom-developed apps on unclassified networks and describes how the work is done, at the methodology level.

- 1. Fix the scope on paper.** For each custom-developed app, record the platforms, the device baseline, the distribution path through the agency's MDM (Intune, Workspace ONE, or Ivanti), the integrations, and who owns the Apple Developer and Google Play accounts. Findings without a named device baseline cannot be reproduced later.
- 2. Test statically and dynamically.** Run MobSF, an open-source mobile security framework, in an agency-approved environment and log findings by [OWASP MASVS](#) control group: storage, cryptography, authentication and authorization, network communication, platform interaction, and code quality. This is verification against a standard, not a penetration test.
- 3. Assemble the vetting evidence.** Format the test results, a mapping to the agency's own app security requirements, and a machine-readable software bill of materials as the evidence package for the agency's vetting process, which [NIST SP 800-163 Rev. 1](#), Vetting the Security of Mobile Applications, lays out. Add an evidence map to NIST SP 800-53 Rev. 5 controls SA-11 (developer testing) and SA-15 (development process) for the ISSO.
- 4. Check deployment fit.** Compare the app's distribution and permissions with the agency's device policies under [NIST SP 800-124 Rev. 2](#). Confirm that push payloads carry no sensitive data through Apple or Google services, and that any commercial cloud service the app calls holds a FedRAMP authorization or sits inside the agency boundary.
- 5. Hand over a backlog.** Load the findings into the agency's tracker, ordered by severity, with the agency product owner deciding what gets fixed and when.

The agency's reviewers approve the vetting package and own authorization. Several recommendations sit outside this method: removing prohibited apps and enrolling devices (4, 8, 10, 11), credentialed scanning (6), foreign travel procedures (7), and inventory roles (9). MDM operation is a separate service, and an independent penetration test is a separate Vulnerability Assessment task.

WHAT "FIXED" LOOKS LIKE

DHS OIG decides when a recommendation closes, and its public page lists no closure evidence for these 11. What follows are targets a program could set against recommendations 2 and 3, not results anyone has reported.

- Every custom-developed app in the portfolio has a current test report logged by MASVS control group, dated against a named build.
- The three known vulnerabilities in the two I&A-developed apps each trace to a backlog item with an owner and a retest result.
- A written procedure names who evaluates a custom-developed app before release, what evidence the evaluation needs, and who accepts it. Policy authorship stays with the agency.
- Each test and vetting package can be handed to the OIG as a closeout attachment without rework.

STATUS CHECK

OPEN Oversight.gov listed all 11 OIG-26-06 recommendations as open when read on October 8, 2026. FedScoop reported in May 2026 that some are resolved and stay open until the OIG reviews a formal closeout letter. The page shows no DHS OIG last-update date. GAO-24-106764 is background only, and its reporting requirement sunset in December 2023.

TEAMING FIT

NAICS	541511, 541512
AVALON'S SUB ROLE	Static and dynamic testing of custom-developed mobile apps by MASVS control group, a NIST SP 800-163 Rev. 1 vetting evidence package, an SA-11 and SA-15 evidence map, and a deployment-fit check against the agency's MDM posture, under the prime's mobile or application task
SMALL-BUSINESS STATUS	Small business; HUBZone (in progress)
LIKELY VEHICLES	GSA MAS (SIN 54151S IT Professional Services); GSA Alliant 3

If a DHS component's mobile app, MDM, or mobile security task is in your capture plan, Avalon teams as the sub that tests custom-developed apps by MASVS control group and assembles the SP 800-163 vetting evidence the agency's reviewers and the OIG will ask to see.

BRANDON IRELAND, FOUNDER · CONTACT@AVALONTECHSERVICES.COM · AVALONTECHSERVICES.COM

This brief analyzes publicly released oversight reports. It does not describe work Avalon performed for any agency named.