OFFICE *of the*
INSPECTOR GENERAL
U.S. GOVERNMENT PUBLISHING OFFICE

OIG-25-050

Date

June 16, 2025

To

Director, U.S. Government Publishing Office

From

Inspector General

Subject

Management Implication Report 24-0014-I, GPO Government Cell Phone Applications

Case Summary

We investigated GPO-issued cell phones, comparing application data against GPO policy, particularly Section 7, Subsection C, paragraphs 6 and 14 of GPO Directive 825.29E on Internet and Email Policy:

- Paragraph 6: Prohibited uses of the Internet using GPO-owned devices include "[c]reating, downloading, viewing, storing, copying, or transmitting materials related to gambling."
- Paragraph 14: Prohibited uses of the Internet using GPO-owned devices includes "[i]nstalling or using any personal or non-GPO software or hardware directly on a GPO computer or directly on the GPO network that is not issued and/or authorized by the GPO including, but not limited to, iPods, Smart Phones, personal USB drives, other USB devices, other add-on devices, instant messaging (IM), peer-to-peer (P2P), freeware, shareware, video games and photo shops."

What We Found

We identified numerous downloads of non-GPO software onto GPO-issued mobile devices, most of which did not appear to serve any official government function. These unauthorized applications pose potential security risks, increase the agency's exposure to malware and data breaches, and contravene established IT policies. Our findings suggest a need for strengthened oversight, enhanced mobile device management protocols, and increased user awareness to ensure compliance with agency cybersecurity standards.[1]

The following table lists the most commonly downloaded unauthorized applications by category, with the corresponding number of download instances noted in parentheses.

[1] This proactive investigation generated several investigative leads, some of which remain under active examination. Further inquiry is ongoing to determine the extent of any potential violations of law, rule, or regulation.

Table 1: Most Frequently Downloaded Unauthorized Applications

Social media	Streaming	Gambling/Sports Betting	Shopping
Facebook (70)	Netflix (54)	FanDuel Sports Books (6)	Amazon (62)
Instagram (44)	Hulu (27)	BET MGM Sports (3)	Costco (14)
X (22)	Disney+ (17)	DraftKings (1)	Bath & Body Works (6)
Snapchat (9)	Tubi (12)		Bed Bath & Beyond (2)
Twitch (3)			

Source: OIG Analysis

Recommendations

As a result of our investigation, we have three recommendations.

Recommendation 1: Enroll all GPO-issued devices in a Mobile Device Management system capable of controlling application installations, limited to only approved applications, and enforcing policy compliance.

If unable to institute a Mobile Device Management system, conduct periodic audits of GPO-issued devices to detect unauthorized software and ensure policy adherence.

Recommendation 2: While the current annual GPO Cybersecurity Awareness Training highlights the risks of downloading mobile applications,[2] we recommend that the annual training include more information about or greater emphasis on the **prohibition** of downloading personal or non-GPO software on GPO-issued mobile devices.

Recommendation 3: We note that there may be legitimate business or reasonable personal use cases for the above applications (e.g. social media and streaming services). However, the current GPO IT policy strictly prohibits application downloads as stated above.

GPO should consider updating IT policies to more clearly define the scope of acceptable and prohibited uses, including establishing a "whitelist" of approved applications. The updated policy should better delineate reasonable personal use, use while off-duty, and the consequences for violations to include loss of network access or mobile phone use.

If you have any questions, please contact me or Assistant Inspector General for Investigations Robert Stachurski at 202-512-1944 or rstachurski@gpo.gov.

Digitally signed by Nathan Deahl
Date: 2025.06.16 11:18:41 -04'00'

NATHAN J. DEAHL
Inspector General

[2] FY25 GPO Cybersecurity Awareness Training "Lesson 4: Safeguarding Information & Portable Devices"