Congress of the United States

Washington, DC 20515

August 21, 2026

Orice Williams Brown
Acting Comptroller General of the United States
Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Acting Comptroller Brown:

We write to request that the Government Accountability Office (GAO) conduct a comprehensive review of federal law enforcement agencies' hacking of Americans' electronic devices.

While federal law enforcement agencies have used hacking and spyware as an investigative tool for more than 25 years, there exists little public information regarding its scope, frequency, or operational safeguards. Unlike traditional surveillance authorities, such as wiretaps or pen registers, the government does not publish annual reports for hacking operations. Furthermore, while the Department of Justice (DOJ) and Department of Homeland Security (DHS) have established public policies governing their use of surveillance technologies like cell-site simulators ("Stingrays"), no comparable public policies exist that govern federal hacking. Moreover, DOJ and the Federal Bureau of Investigation (FBI) have repeatedly ignored congressional requests for greater transparency across multiple administrations.

To enable informed public debate, ensure appropriate operational safeguards, and assist Congress in crafting future legislation, we request that the GAO conduct a review of federal law enforcement hacking and publish an unclassified report detailing its findings and recommendations, accompanied by a classified annex if necessary to address sensitive operational details. We request that you review the practices and policies of federal law enforcement agencies, including the FBI, Drug Enforcement Administration, Secret Service, and Homeland Security Investigations in three areas:

1. Internal Misuse, Audit Protocols, and Safeguards Against Abuse: Spyware and other hacking tools grant expansive access to personal devices, including webcams, location data, stored files, and encrypted communications. Unrestricted access to such invasive surveillance capabilities invites abuse by rogue agency personnel. Indeed, there are countless documented examples of government employees abusing other sensitive surveillance databases and tools for unauthorized personal purposes. We request that GAO review:

- Any documented instances in which federal law enforcement personnel misused agency hacking capabilities for unauthorized or personal purposes.
- The technical logging, auditing, and access controls implemented by agencies to monitor the deployment and operational use of hacking tools and whether existing internal oversight mechanisms and administrative penalties are sufficient to deter, detect, and discipline employees abusing hacking tools.

2. Cybersecurity Risks, Vulnerability Management, and Tool Proliferation: The government's acquisition and use of sophisticated hacking capabilities create inherent collateral risks to national security and civilian infrastructure. These hacking tools can fall into criminal and foreign adversary hands through multiple vectors: targets discovering and reverse-engineering government software exploits, adversaries compromising government or contractor networks, or malicious insiders leaking or selling government hacking tools. These

risks are far from theoretical. Notably, a former senior official at defense contractor L3Harris was sentenced earlier this year for stealing and reselling sensitive hacking tools—which were originally developed for U.S. intelligence agencies—to a Russian broker. We request that GAO review:

- How federal law enforcement agencies acquire, store, and secure hacking tools and the adequacy of cybersecurity requirements imposed on contractors that supply hacking tools to the government.
- The procedures agencies use to assess and reduce the risk that hacking technology may be intercepted, reverse-engineered, or repurposed by targets or third parties.
- Whether vulnerabilities exploited by law enforcement hacking tools are regularly submitted to the interagency Vulnerabilities Equities Process, including after such hacking tools have fallen into the wrong hands.

3. Judicial Candor, Authorization Transparency, and Risk Disclosure: Federal courts rely heavily on the government's candor when evaluating search warrant applications under Rule 41 of the Federal Rules of Criminal Procedure. Given the invasiveness of this method of surveillance, and the serious collateral risks to third parties described above, courts must be provided sufficient information in order to properly evaluate applications for government hacking operations. We request that GAO review:

- How federal law enforcement agencies present hacking requests to courts, and whether warrant applications sufficiently disclose specific operational risks, including potential system instability, data corruption, exposure of non-target data, or the potential for third parties to detect and re-use government hacking tools.
- Whether agencies adequately inform judges when they are seeking permission to conduct a hacking operation involving unknown targets, bulk hacking, or operations that may inadvertently sweep up innocent bystanders.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Greg Casar
Ranking Member
Subcommittee on Federal Law Enforcement