carahsoft

From AI Policy to Mobile Protection: What Agencies Need to Know

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Lookout, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/LookoutResources

Join Events & Webinars:
carah.io/LookoutEvents

Discover Technology Solutions:
carah.io/Lookout

Learn About Procurement:
carah.io/LookoutContracts

Connect With Our Team:
Lookout@carahsoft.com
(844) 445-5688

From AI Policy to Mobile Protection: What Agencies Need to Know



Artificial intelligence continues to blaze a path of innovation — but also concern. Although the big story about risks associated with the technology focuses on the data that feeds it, other risks are emerging, including how AI is used in mobile devices.

Federal agencies are learning they need to figure that out quickly. A new executive order — "Promoting Advanced Artificial Intelligence Innovation and Security" — that the White House issued in June, gives them the green light to rapidly adopt AI. It also establishes a voluntary 30-day prerelease review process so agencies can use the technology responsibly.

To understand what this means for agencies, GovLoop asked David Richardson, Chief Technology Officer at Lookout, a leading cybersecurity company, during a recent webinar for his insights into AI's role in the mobile device space.

A Perilous Paradox

At its core, the new EO is about adopting AI quickly and using it to fulfill an agency's mission, Richardson said. It's also about doing all that securely after a 30-day review.

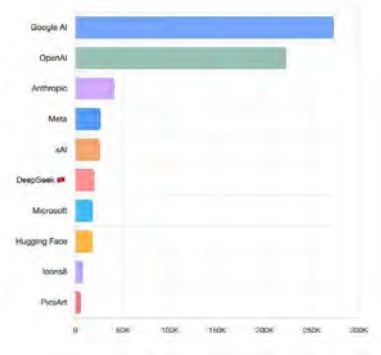
That sounds great, but it creates a paradox: "You have to adopt it as quickly as possible, but also make sure you follow this prerelease process," he said. "These things are competing for your attention all at once. It can be hard to sift through the noise and determine what is it that an organization should actually do."

What's more, many agencies lack visibility into what's happening on employees' government-issued mobile devices. Because they keep tight reins over what workers use on desktops and in the cloud, many workers download mobile apps instead.

"You've got native code running on these devices that are built by who knows who, and that traffic is completely encrypted," Richardson said. Agencies might have mobile device management in place, but all that tells them is what apps are installed, not what software development kits are included or what the apps are doing.

"This space is moving so quickly; so many new models and new applications are sprouting up every single day," he added. "This creates a significant blind spot when it comes to mobile."

Invisible AI SDKs embedded inside 600k+ mobile apps





That lack of visibility is especially concerning considering that:

50% or more of generative AI use happens on mobile devices

77% of employees say they paste agency data into AI tools

46% of organizations say they have had GenAI leaks already

Warning shot:

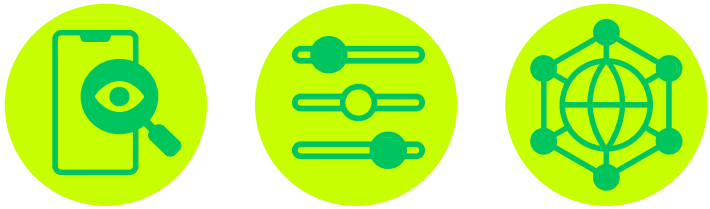
"Tons of different AI software development kits (SDKs) are being embedded inside of mobile applications...and not everyone is using the frontier models from Google, OpenAI or Anthropic," Richardson said. "Many developers are using much more cost-efficient models [from China] like DeepSeek, Baidu and ByteDance.... As an end user you have no idea whether that app that you downloaded to make you look like a cartoon character is using a local on-device model or a model from OpenAI or a model from DeepSeek."

Challenges of Agentic AI

The models rely on agentic AI, in which users give the AI capabilities of large language models the freedom to complete actions on their behalf. In other words, agentic AI can operate independently to achieve an objective. It determines each action dynamically, and rather than following an agency-defined script, it evaluates what it finds and decides what to do next to accomplish its objective. On mobile devices, agentic traffic is encrypted, allowing it to bypass inspection and standard security controls. Unsurprisingly, it's the No. 1 attack vector that chief information officers are worried about in 2026.

To defend against it, agencies need three things, Richardson said:

1. **Visibility** into what is on mobile devices
2. **Endpoint-level control** that dictates what applications may be installed based on the SDKs inside of them, the application programming interfaces they call out to and what data they're sharing with different models
3. **An understanding of network activity** at scale so they can monitor network and browser traffic



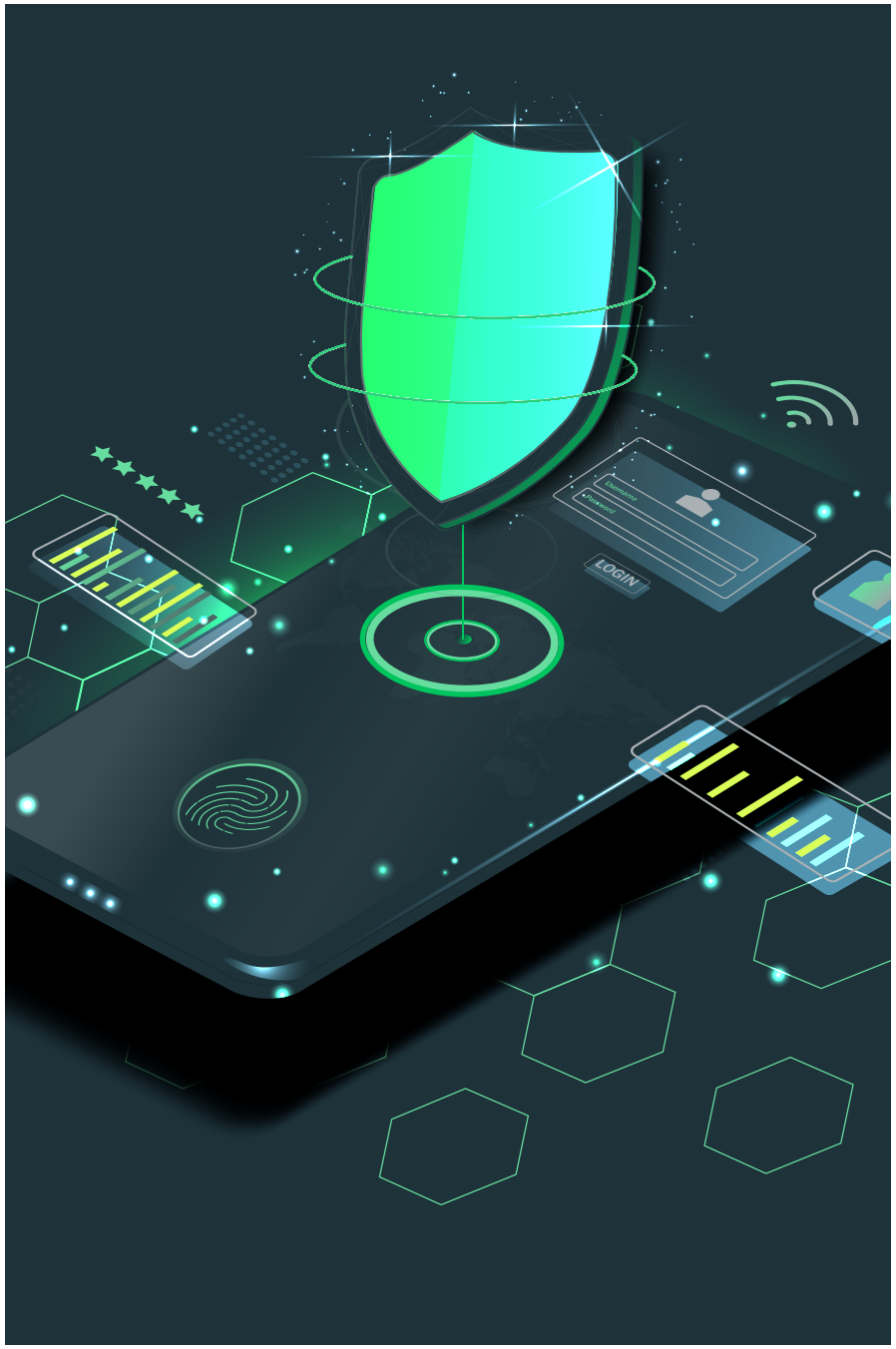
Understanding the risks of agentic AI: A case study

OpenClaw is a free, open source autonomous AI agent that can execute tasks via large language models. It can be helpful: reading and replying to email or doing research. But to do it, the agent circumvents an agency's IT and cybersecurity policies and controls. Richardson explained how:

> "Let's say you give your mobile device over to something like an OpenClaw, and you ask it to complete a simple task: 'I want to request a day off of work.' It wants to be helpful. It might run into a username and password field. It's going to hunt for your password. It's going to try to fill that in. Maybe there's multifactor authentication. It's going to open your multifactor authentication application, it's going to find that code, it's going to copy it to the clipboard, it's going to open the other app [and] it's going to paste it in there."

PromptSpy

PromptSpy is the first known Android malware to use GenAI in its execution flow. It takes a screenshot or reads the accessibility tree from your device. The attacker can then provide a command from its command-and-control server to the device. Next, the device sends the data associated with what's on the screen and the attacker's command to an AI model and asks it to complete the next step. All that happens unbeknownst to the user — and to the agency.



Steps to Security

The risk AI presents to agencies "isn't a hypothetical problem. This is a real problem that's here and now," Richardson said. To address it, many agencies need to overhaul their approach to AI governance.

Currently, it's largely seen as a documentation exercise: Agencies focus on creating policies, procedures and compliance paperwork to define acceptable AI usage. These activities are important, but "paperwork is not necessarily actually making you any more secure," he said.

Instead, organizations need to move toward operational security. That means developing visibility into what is happening on devices, implementing technical controls and establishing enforcement mechanisms that support policy objectives. Security programs require both governance and the technical capabilities needed to verify compliance.

"You need to move to a model of actually hardening, of actually understanding the capabilities and what's actually going on devices," he said.

New compliance frameworks, along with Android 16 and Apple iOS 26 Security Technical Implementation Guides requirements, are increasing expectations around mobile security. The argument is that mobile device management alone is no longer enough. Organizations must also implement mobile threat detection capabilities and gather endpoint telemetry if they want to meet audit requirements and maintain authorization to access sensitive federal data.

"It's not sufficient to just say, 'I manage the device. I know where my assets are,'" Richardson said.

How Lookout Helps

Lookout, which specializes in AI security for mobile, offers a cloud-based console that IT and security teams can use to manage cybersecurity across all an agency's devices. It provides visibility, collects telemetry from the devices and serves as a place for policy enforcement.

The console's AI usage capability shows data for thousands of devices and can show which AI providers are being used based on device DNS lookups, application inventories and the SDKs embedded within those applications. Users can manipulate the console to see more details about usage peaks and valleys and what's trending. That helps officials determine whether governance policies are working.

For example, using the console, an agency that implements policies to restrict OpenClaw could see that use dropped 98%.

"You can go a level deeper into the actual services themselves," Richardson said. "Is it the DeepSeek app or is it the DeepSeek API that's being used within this organization?"

Administrators also can determine whether activity is occurring through an API, a chat interface or another gateway. Additionally, they can identify which applications inside the organization are using specific AI providers or SDKs.

Once they identify problems, officials can take action through the console. For instance, they can:

- Block applications or domains
- Block communications between apps and DeepSeek or other AI companies
- Customize risk levels
- Adjust enforcement
- Apply policies based on the user or device

Ultimately, a combination of visibility, governance and enforcement are the key to protecting mobile devices from rogue AI agents. The Lookout console brings all those capabilities together in one dashboard so that agencies can easily comply with new AI review mandates and keep unapproved AI adoption out of their environments.

"Understand the reality of the situation today within your environment — not just what's on paper, but what's actually happening in the real world," Richardson said.



Conclusion

The gap between AI adoption requirements and security capabilities is widening for government agencies, especially when it comes to mobile devices. Many still focus on governance, but that's only part of a robust cyber approach. Agencies also need visibility into mobile AI usage, detection of agentic AI risks and technical controls that enforce policy rather than merely document it.

Watch the full webinar here

govloop