Encrypted, But Exposed: Why Signal Falls Short for Classified Communications

Despite its strengths in personal privacy, Signal falls short for classified use due to infrastructure, certification, metadata, and personal device risks.

COLUMBUS, OH, UNITED STATES, March 31, 2025 /EINPresswire.com/ -- By Matt Santill, CISSP, Cyber Security Services

Signal is one of the best tools for personal privacy and secure communications. Its open-source encryption protocol, minimal data collection, and transparent model make it a favorite for journalists, activists, and privacy-conscious users worldwide.

But… when it comes to government or classified use, a few limitations are worth discussing.

1. Startup-Sized Budget (~$20M/year)
Signal runs a global communication platform on a budget more typical of a tech startup. Budget doesn't always equal security—but when you're dealing with high-stakes, national-security-level risk, lack of resources becomes a real concern.

"In cybersecurity, resilience and redundancy often require investment," said Matt Santill, founder of Cyber Security Services. "When your infrastructure is underfunded, you may not even know when it's under attack."

2. Tens of Millions of Users on Shared Infrastructure
A small team is supporting tens of millions of users on the same infrastructure, including potentially sensitive communications. That infrastructure isn't segmented, prioritized, or isolated.

"If you're a government agency relying on the same cloud queues as everyone else," Santill noted, "you're accepting a risk profile you don't control."

3. No Government Differentiation
There's no segmentation or enhanced controls for official users. No advanced logging. No optional hardening. No tiered authentication. Whether you're a local journalist or an intelligence officer, you get the same protections—and the same vulnerabilities.

4. No NSA or DoD Certification
Signal is not approved under the NSA's Commercial Solutions for Classified (CSfC) program or listed on the Department of Defense Approved Products List (APL). That disqualifies it for classified communications outright.

"No matter how secure it seems, if it hasn't been vetted and approved, it doesn't belong in a classified environment," Santill emphasized.

5. Metadata Still Exists
Edward Snowden showed us: metadata is surveillance gold.

Despite Signal's strong encryption and privacy-forward stance, important metadata risks remain, many of which are acknowledged directly in their own privacy policy:

- Phone numbers are required for account creation, tying identity to communication activity.
- "Our third-party providers send a verification code…"
Providers like Twilio introduce upstream/downstream dependencies and risk. Not all third parties are disclosed.
- "Signal can optionally discover which contacts in your address book are Signal users…"
Even hashed contact data, when uploaded for matching, can be exploited to reveal networks or associations—a valuable target for nation-state adversaries.
- Message timing may reveal user behavior, even if message content is encrypted.
- "Signal queues encrypted messages for offline delivery"
This introduces in-transit metadata exposure—such as who messaged whom, and when.

6. Personal Devices Are Still a Major Risk
Even if the app is encrypted, Signal is usually run on personal mobile devices—devices that lack government-grade hardening, secure boot processes, and controlled app ecosystems. These endpoints are susceptible to spyware, malware, and zero-click nation-state exploits. The app may be secure—but the device is still vulnerable.

"A nation-state adversary doesn't need to break Signal—they just need to compromise your phone," said Santill. "Far too many senior government officials rely on personal devices, assuming Signal alone makes their communications secure. That assumption is dangerously flawed—and it puts our national security at risk."

Bottom Line
The real vulnerability often isn't the app—it's the device itself. Yet many government officials continue to use personal, unhardened mobile devices, mistakenly believing that Signal alone ensures secure communication. That assumption leaves critical operations dangerously exposed. A nation-state adversary may not be prioritizing the message content alone—communication patterns can reveal networks, relationships, and mission priorities.

“Make no mistake—Signal is a target. And if it wasn’t before, it is now.”

In a world of advanced threats and digital espionage, encryption isn’t the end of the story—it’s just the beginning.

About the Author
Matt Santill, CISSP, is the founder of Cyber Security Services, a cybersecurity firm based in Westerville, Ohio. He has served as a CISO for public and private institutions and provides cybersecurity guidance, virtual CISO services, and secure communication assessments for clients in regulated and high-risk industries.

Matt Santill
Cyber Security Services
+1 786-266-7388
email us here
Visit us on social media:
Facebook
LinkedIn
