# Defense Secretary Pete Hegseth’s use of Signal app exposes flaws in US government communication security



Defense Secretary Pete Hegseth has drawn scrutiny for his use of the Signal messaging app to send highly sensitive targeting information to colleagues, friends, and family members. This incident, dubbed "Signalgate," highlights widespread issues with the security measures and technology currently employed by the US government for handling classified information. These shortcomings often compel military and intelligence officers to resort to insecure alternatives to communicate swiftly and effectively.

The core challenge lies in the government's reliance on sensitive compartmented information facilities, or SCIFs, where classified communications must occur. SCIFs are typically confined, windowless rooms designed to safeguard classified data, but they significantly restrict the use of the internet and modern digital tools that are crucial for rapid decision-making and operations. Aaron Brown, a former CIA officer and Army Ranger with two decades of experience, describes these facilities as "an outmoded security practice for more than 20 years." He notes, "The SCIF was built for a bygone era in the 1970s and 80s when communications were easy to control, and the speed of business didn't require persistent access to the internet."

Hegseth reportedly used Signal to disseminate information about planned military actions in Yemen during the Trump administration. He communicated with a Signal chat group set up by national security adviser Michael Waltz, called “Houthi PC small group,” to update senior officials on targeting and timing. In addition, he shared similar information through another Signal chat that included his wife and personal lawyer. Multiple former military and intelligence officers have criticised these actions as reckless, stating they would usually warrant disciplinary measures.

This situation is not unique to Hegseth. Thousands of military and intelligence personnel encounter similar dilemmas. CIA officers, for example, require rapid internet access to execute their missions effectively. However, when confined to SCIFs, whether overseas or at headquarters such as Langley, access to the internet requires special permission. Some officers reportedly resort to leaving SCIFs to use mobile phones or bring phones inside, both of which violate regulations. Brown explains that officers face an impossible choice: either comply with restrictive rules and risk mission failure or breach those rules to maintain operational speed.

The restrictive SCIF environment also limits the use of emerging technologies such as advanced artificial intelligence (AI) tools that are transforming national security capabilities. Brown reveals he waited 18 months—and ultimately abandoned efforts—to gain approval to use Google in a classified setting. While the Pentagon and intelligence community have some access to earlier AI models, they are barred from widespread use of the latest ones, including OpenAI’s ChatGPT-4o, Google’s Gemini 2.5, and Anthropic’s Claude 3.7. Brown asserts, "It is not an exaggeration to say that SCIFs are in very large part to blame for the IC’s technology deficits."

Despite the existence of technologies that could resolve these issues, government adoption has been slow. One example is Cape, a mobile phone company founded by former Special Operations sergeant John Doyle. Cape has developed a virtual mobile network that operates outside the conventional cellular network and is purportedly nearly impossible to hack or trace. Doyle emphasised in an email: "Modern mobile is how we all communicate—from teenagers glued to Snapchat to soldiers on the frontline in Ukraine to our nation’s elected officials. It’s a national imperative to make secure commercial mobile work for everyone’s needs, including defense and intelligence professionals."

Government security officials, however, remain entrenched in legacy systems that inhibit progress. Brown points out that despite demand for new systems, "innovation is blocked by outdated security practices, overly rigid counterintelligence policies, and inefficient acquisition processes."

Additionally, mobile SCIFs—prefabricated units intended to provide secure environments in homes or unclassified spaces—exist but are scarce and slow to be approved, often taking up to a year.

This situation underscores the tension between maintaining stringent security protocols and enabling the rapid, modern communication essential for effective military and intelligence operations. The Washington Post is reporting on this issue in the context of the Hegseth controversy, shedding light on broader systemic challenges faced by the US government in securing classified information while adapting to technological advancements.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://apnews.com/article/6a64707f10ca553eb905e5a70e10bd9d> - This article reports that Defense Secretary Pete Hegseth set up an unsecured internet line in his Pentagon office to use the Signal messaging app on a personal computer, bypassing Pentagon cybersecurity protocols.
2. <https://www.ft.com/content/e69c96f0-e0ed-4f4e-824b-24a06ea3dd62> - This piece discusses the controversies surrounding Pete Hegseth's appointment as U.S. Secretary of Defense, including his mishandling of sensitive military information and the destabilization of the Pentagon.
3. <https://www.ibtimes.com/nobody-was-texting-war-plans-hegseth-denies-mishandling-classified-data-amid-leaked-signal-chat-3767503> - This article covers Defense Secretary Pete Hegseth's denial of mishandling classified information, despite reports of sharing sensitive military plans via the Signal app.
4. <https://www.koat.com/article/trump-signal-app-controversy/64306368> - This report details the fallout from revelations that top national security officials discussed sensitive attack plans over the Signal messaging app, with a journalist inadvertently added to the chain.
5. <https://www.nationalmemo.com/hegseth-signal-leak> - This article discusses the leak of a Signal chat involving Secretary of Defense Hegseth, revealing classified information about military operations and the subsequent controversy.
6. <https://www.the-independent.com/news/world/americas/us-politics/signal-texts-read-classified-documents-trump-hegseth-b2721905.html> - This piece reports on the publication of Signal chat messages detailing sensitive military operations, contradicting claims that no classified information was shared.
7. <https://www.washingtonpost.com/opinions/2025/04/29/hegseth-signal-scif-classified-information/> - Please view link - unable to able to access data