TLPCLEAR
PMSC Alpha Corp Joint Mission Analysis Team,
Compliance-Solutions.pro Intelligence Branch,
Cyber Warfare Center Pacific (CYWAR-CENPAC),
Liberty Station USNTC Point Loma CA USA
Release Date: March 24, 2024 22:54 Zulu

White House Signal Breach Secure Protocol Investigation

If high-ranking U.S. officials inadvertently included an unauthorized investigative journalist in a top-secret Signal chat, there are several plausible explanations for how this could have happened, and none of them are particularly good. At the most fundamental level, Signal is mistakenly associated with military-grade encryption and sophisticated security protocols,. While that may be good for their marketing campaigns and ROI, it doesn't translate to actuality. Signal is the "safest" publicly available messenger application in use today after Telegram. They both rate high on the secure communications gradient, but that does not mean that there are no issues that need to be resolved in order to actually be the "safest" platform to share sensitive information on.

If we can forget about the hype and just stick with the facts of the matter it would be clear that neither Signal or Telegram are sufficiently secure to discuss national security matters in group chats, private chats or direct messaging. So, when Defense Secretary Pete Hegseth, Vice-President J.D. Vance, White House National Security Advisor Mike Waltz and Secretary of State Mark Rubio, and 32 intelligence officers, executive security and Pentagon officials, used signal to discuss imminent military strikes against Yemeni targets, highly classified operational security and force protection details, including unit designations, deployment and staging areas, weapons systems and targeting and top secret maps and charts specific to mission objectives, they didn't notice, and Signal did not notify them, that an un-vetted guest with no security clearance was also in the chat with them.

That happened because Signal is not capable of the systems-level security posture required to secure top secret communications. It really defies logic as to why the leaders of the free world even considered using it when there are communications platforms that are purpose-built for top secret-level correspondence. The Joint Worldwide Intelligence Communications System (JWICS) is one of the most secure communications platforms in the world that allows global intelligence agencies to communicate freely with any other intelligence agency. The platform was secure-by-design to handle top secret and secret compartmentalized Information (SCI). JWICS should be the only U.S. government authorized platform for sharing top secret information. It's not new, every U.S. intelligence agency uses it, it's never be exploited or compromised. the first question that needs to be answered is how the executive branch concluded that it would be a good idea to use Signal for their battle sessions in the first place, the second question is why didn't the group chat moderator detect the uninvited guest.

As to the first question. There’s really no telling who is the responsible party that initially gave the green light to use Signal for secret information (CISA authorized it December 18, 2024), but the responsibility for it falls on the Assistant to the President and White House Director of Communications Steven Cheung, Principle Deputy Communications Director Alex Pfeiffer and Special Assistant to the President and War Room Director Ian Kelly. It's their responsibility to insure that all White House communications are secure and that only authorized devices and applications can be used for official business.

There are several secure communications policy guidelines that regulate the transmission of secret information, none of them include the use of Signal or Telegram for any official business. Signal is not secure-by-design, zero trust enabled or authentication pass key protected, it's end-to-end encryption does not encrypt everything, only the chat is encrypted. The security of the Vice President's communications and cell phone falls under multiple agencies and security protocols, designed for ensuring protection from espionage, cyber threats, and unauthorized access. The primary entities responsible include:

1. White House Communications Agency (WHCA)
The WHCA, a joint military unit under the Defense Information Systems Agency (DISA), provides secure voice, video, and data communications for the Vice President, the President, and other top officials. It ensures classified and unclassified communications are encrypted and protected from interception.

2. United States Secret Service (USSS)
The Secret Service’s Technical Security Division oversees the physical and cyber security of the Vice President’s communications devices. The Electronic Crimes Task Force (ECTF) works to prevent hacking, surveillance, and electronic eavesdropping. Signals intelligence (SIGINT) monitoring helps detect unauthorized attempts to access or intercept communications.

3. National Security Agency (NSA)
The NSA is responsible for securing classified communications through encrypted devices and hardened mobile phones for secure calls. NSA-approved secure devices, like Classified Secure Mobile Phones (CSMPs) or Secure Telephone Equipment (STE), are provided to the Vice President. The NSA’s Information Assurance Directorate (IAD) monitors potential cyber threats against government communication systems.

4. Defense Information Systems Agency (DISA)
DISA manages the Secure Mobile Environment (SME), providing Top Secret-level secure communications. It operates DoD Secure Voice Networks and ensures high-ranking officials are using NSA-approved encrypted channels for calls and messaging.

5. Federal Bureau of Investigation (FBI) – Counterintelligence & Cyber Divisions
The FBI's Counterintelligence Division investigates attempts by foreign adversaries to compromise the Vice President's communications. The FBI's Cyber Division handles any digital threats, including phone hacking, malware, and SIM-swapping attacks.

NSA-Hardened Devices: The Vice President is issued a highly secure, NSA-certified smartphone with end-to-end encryption. Commercial devices (iPhones, Androids, etc.) are not used for classified communications and are prohibited by specific policy restrictions..

Classified Communications Channels: Secure calls and messaging go through DOD-approved secure networks, like JWICS and the equally robust Classified Secret Internet Protocol Router Network (SIPRNet). Signal, WhatsApp, or regular mobile networks are NOT approved for classified discussions.

Strict Operational Security (OPSEC) Protocols: The Vice President's phone number is highly restricted, and unauthorized applications are not installed. Faraday bags (signal-blocking enclosures) are used to prevent remote exploitation of the device. Regular security sweeps are conducted to check for unauthorized access attempts.

If the Vice President and other top officials used an unsecured Signal chat for classified discussions, responsibility likely falls on: WHCA & NSA – For failing to enforce proper encrypted communications. Secret Service Technical Security Division – If a personal/unsecured phone was used. DISA – If secure mobile environments were not properly maintained. The Vice President's Staff – If OPSEC violations occurred due to negligence or unauthorized app usage. This represents a serious security breach, potentially violating U.S. national security laws like the Espionage Act (18 U.S.C. § 793) and Executive Order 13526 (which governs classified information handling). An immediate investigation has been launched. Bottom Line: The White House Communication Agency is the main entity responsible, but the rest of the oversight and enforcement failure is evenly spread out among the other responsible agencies, which typically indicates a systemic administration-wide failure to follow established policy and guidelines that are very clear and unambiguous.

1. Contact Syncing & Mistaken Identity
If one of the officials had the journalist's number saved in their contacts under a misleading or similar name (e.g., another official's name), they might have accidentally

added them to the chat. Signal allows users to invite contacts easily, and if a user is relying on auto-complete or contact suggestions, a misclick could lead to an unintended invitation.

2. Phishing or Spoofing Attack

An adversary (state-sponsored or independent) could have used a SIM swap attack or spoofed a legitimate official’s phone number to infiltrate the chat.

If the journalist’s number had been compromised in a recent data breach and was linked to an intelligence agency or military official in contact databases, Signal’s auto-suggestion could have included it mistakenly.

3. Insider Threat or Human Error

Someone in the group may have unknowingly shared an invitation link, believing it was only accessible to approved members. A rogue actor within the group could have deliberately added the journalist’s number for intelligence leaks or investigative purposes.

4. Exploitation of Signal’s Group Chat Features

Signal uses a "group link invite" system, where users can generate an invite link that can be forwarded. If this link was accidentally shared outside the intended recipients, an unauthorized user could have joined before being noticed. A poorly managed invite policy (e.g., allowing anyone with the link to join) may have enabled an unintended addition.

5. Database or Metadata Correlation Attack

Advanced threat actors could have exploited metadata analysis, correlating phone numbers of known intelligence officials and potential journalists, inserting the journalist’s number into the chat by manipulating network traffic or cached contacts.

6. Malicious Code or Exploit

If a vulnerability existed in the Signal app, an adversary could have injected a journalist’s number into a conversation at the network level. A compromised device within the chat may have been exploited to auto-add a non-cleared contact.

7. Psychological or Social Engineering Manipulation

A well-placed social engineering attack could have led someone in the group to believe the journalist was a vetted intelligence officer or staffer, leading them to be added manually.

8. Foreign Intelligence Manipulation

If a hostile intelligence service (e.g., Russia or China) had gained partial access to an official's phone or contacts list, they could have subtly altered the contacts database to include unauthorized numbers in messaging apps.

The simplest and most probable explanation is human error through mistaken identity or a misclick in contact selection, followed closely by a compromised invitation link or a SIM swap attack enabling number spoofing. However, given the high-profile nature of the officials involved, more sophisticated foreign intelligence interference cannot be ruled out. This incident necessitates an immediate forensic analysis of the Signal group logs, invite history, and device security of all participants to determine how the breach occurred. Signal is widely considered one of the most secure messaging apps due to its end-to-end encryption, but it is not immune to potential vulnerabilities. Here are some security concerns and past vulnerabilities associated with Signal:

1. Zero-Day Vulnerabilities and Exploits
While Signal has a strong security posture, state-sponsored attackers and advanced persistent threats (APTs) continuously look for zero-day vulnerabilities. There have been no major publicly disclosed zero-day exploits affecting Signal's encryption directly, but the possibility always exists.

2. Metadata Leakage Risks
Signal encrypts message content but does collect some metadata (e.g., phone numbers, registration timestamps, and IP addresses). In high-threat environments, adversaries could perform traffic analysis to infer user behavior, even if they cannot see the content of messages.

3. Cellebrite Exploitation Attempts
In 2021, Signal's founder demonstrated how Cellebrite, a forensic tool used by law enforcement, had significant security flaws. While Cellebrite claimed to extract some Signal data from compromised devices, Signal's security measures generally prevented unauthorized access.

4. Vulnerabilities in Desktop Client
In 2021, a WebRTC vulnerability (CVE-2021-32666) in Signal Desktop allowed an attacker to force a target to answer a call without user interaction. This issue was patched quickly, but it highlighted how flaws in auxiliary components (like WebRTC) could introduce risks.

5. Compromise of User Devices
If an attacker gains access to a user's unlocked phone (e.g., through spyware like Pegasus), Signal messages can be compromised. While Signal itself has strong security, it cannot protect against OS-level compromises.

6. Supply Chain Attacks & Dependency Risks

Signal relies on third-party infrastructure like Google Play or the Apple App Store for updates. If an adversary were to compromise these distribution channels, they could potentially inject malicious code.

7. Potential for Account Takeovers

Signal’s registration process relies on phone numbers, making users vulnerable to SIM swapping attacks. Although Signal has added registration lock PINs to mitigate this, an attacker with control of a victim’s phone number could still attempt to hijack accounts.

8. Abuse of Signal Group Links

Open group invite links can be exploited for social engineering, phishing, or infiltration of private groups.

9. Lawful Intercept & Court Orders

Signal has a policy of minimizing data collection, but if compelled by a court order, they might be forced to hand over what little metadata they do store. In 2016, Open Whisper Systems (Signal’s parent company) received a subpoena from the U.S. government but was only able to provide minimal information.

Mitigation’s and Best Practices

Use disappearing messages to limit retention of sensitive data. Enable registration lock PINs to protect against SIM swap attacks. Keep Signal updated to patch known vulnerabilities. Use a VPN or Tor to hide IP address metadata. Secure your device (e.g., prevent spyware infections and unauthorized access).

While Signal remains one of the best encrypted messaging platforms next to Telegram, its security is only as strong as the environment it operates in. A compromised device or OS will always be the weakest link. Signal, is commonly recognized for its robust security features, but it as had several Common Vulnerabilities and Exposures (CVEs) reported over the years. Notable vulnerabilities include:

CVE-2019-17191: In Signal for Android versions before 4.47.7, an attacker could force a call to be answered without user interaction, potentially opening an audio channel without the callee's consent.

CVE-2019-9970: Signal Desktop through version 1.23.1 and Signal for Android through version 4.35.3 were susceptible to an Internationalized Domain Name (IDN) homograph attack. This allowed URLs containing mixed-script characters to appear as legitimate links, posing phishing risks.

CVE-2018-3988: In Signal for Android version 4.24.8, using the photo feature within disappearing messages could leave images in the app's cache directory. These images were accessible to other applications, potentially exposing private information.
CVE-2022-28345: Prior to version 5.34 on iOS, Signal was vulnerable to URI spoofing via Right-to-Left Override (RTLO) injection. Attackers could craft links that appeared legitimate but directed users to malicious destinations.
CVE-2023-24069 (Disputed): Before version 6.2.0, Signal Desktop on Windows, Linux, and macOS stored message attachments in a directory that wasn't effectively cleared. This could allow an attacker with local file system access to retrieve potentially sensitive attachments. The relevance of this finding is disputed by the vendor, as the product isn't intended to protect against adversaries with local access.
CVE-2023-24068 (Disputed): Also before version 6.2.0, Signal Desktop allowed an attacker with local file system access to modify conversation attachments within the attachments directory. This could enable the insertion of malicious code into existing attachments. The vendor disputes the relevance of this finding for the same reasons as above.

It's important to note that Signal's development team actively addresses reported vulnerabilities, often releasing patches promptly to maintain the application's security integrity. However, the problem is that the Vice-President and Cabinet-level officials are not authorized to use the app for classified conversations, it's specifically prohibited for official government usage, period.

The use of the Signal messaging app by White House officials has been subject to varying policies across different administrations:

Biden Administration (2024): In 2024, the Cybersecurity and Infrastructure Security Agency (CISA) issued guidance encouraging highly targeted government officials to adopt free messaging applications that guarantee end-to-end encryption, such as Signal, as a best practice for secure communications.

Trump Administration (2025): Despite the earlier guidance, the Pentagon issued a warning to its staffers on March 18, 2025, advising against the use of Signal due to identified technical vulnerabilities that could potentially expose messages to unauthorized access.

Following this incident where top officials inadvertently included a journalist in a Signal group chat discussing sensitive military operations, President Trump indicated that the use of Signal might be limited in the future. It's important to note that while Signal offers robust end-to-end encryption, the handling of classified information is governed by strict protocols. Regardless of the communication platform's security features, discussing classified matters on unapproved channels is generally prohibited to prevent potential breaches and ensure compliance with federal records laws. Therefore, while specific policies regarding Signal have evolved, the overarching principle remains that classified information should only be communicated through officially sanctioned and secure channels.

The Cybersecurity and Infrastructure Security Agency (CISA) released the "Mobile Communications Best Practice Guidance" on December 18, 2024. This document does not have a specific release number but it was accessible on CISA's official website, it’s not now (we have a copy). On March 18, 2025, the Pentagon issued a department-wide advisory warning its staff against using the encrypted messaging application Signal, even for unclassified communications. The advisory highlighted a specific vulnerability in Signal that could be exploited by malicious actors, particularly Russian hacking groups, through phishing scams to access sensitive information. The advisory emphasized that the prevalence of Signal among surveillance targets made it a high-value target for interception efforts.

This warning was part of a broader effort to ensure the security of communications within the Department of Defense and to prevent potential breaches of sensitive information. Despite this warning, reports indicated that senior officials, including Defense Secretary Pete Hegseth and National Security Advisor Mike Waltz, used Signal for discussing sensitive military operations. This led to the inadvertent inclusion of a journalist in a group chat about military strikes, raising concerns about operational security and adherence to communication protocols.

The Pentagon's advisory served as a cautionary measure to prevent such security lapses and to encourage the use of more secure, approved communication channels for sensitive discussions. The Pentagon's advisory warning against the use of the Signal messaging app was issued department-wide on March 18, 2025. This advisory cautioned staff against using Signal, even for unclassified communications, due to identified vulnerabilities that could be exploited by malicious actors. The advisory was disseminated internally within the Department of Defense and is not publicly accessible. For more information or to request access to such advisories, you may visit the Department of Defense's official advisories page at:

defense.gov/News/Advisories

Please note that access to specific advisories may be restricted based on their classification and sensitivity.

So, apparently the National Coordinator for Critical Infrastructure and Resilience, America's Cyber Defense Agency, from the Cyber Security and Infrastructure Security

Agency (CISA) released a TLPClear Cell Phone Best Practices Guide that specifically recommends government officials, considered "high-risk of malign influence" on December 18, 2024 and the release date seems to point towards a politically motivated change in direction for CISA, who had previously specifically discouraged government officials from using Signal. This specific guidance has already been removed from CISA's website and can only be found using Google Advbanced Search and WayBack Machine. At that time, the Biden administration officials had already been using Signal and they used the CISA advisory as their justification for using it. The timing of such, one month prior to the Trump Administrations taking office is concerning, and apparently they continued using Signal in reliance on the guidance. The Pentagon has recently issued it's own internal guidance prohibiting Signals use. So there you have it, that's what happened.

Compliance-Solutions.pro is the intelligence branch of PMSC Alpha Corp which is subordinate to Intelligence Clouds, a global intelligence network. We support national security interests and conduct impartial, independent third party investigations and intelligence collections activities at the Cyber Warfare Center Pacific in Point Loma, California. We have no political affiliations, we unconditionally support the sitting U.S. President regardless of party affiliation.

END OF REPORT