Leak Questions Begin To Center Around A Cell Phone

APRIL 10TH, 2023 BY DAVID ARISOTO | 0 COMMENTS

CIPHER BRIEF REPORTING – A wall of small lockers, replete with keys and combination locks, stands just inside the Pentagon – one of many where, upon entering, cell phones are often deposited. Employees are required to leave their phones behind before entering more secure areas.

The reasons for that might seem obvious. But this week, as Pentagon officials scrambled to root out a major security leak and reassure affected U.S. allies, they also began reviewing existing security procedures that purportedly led to a trove of intelligence slides being photographed and shared on social media.

"If you go into a SCIF, or any kind of facility that has classified information, then your phone does not go with you," explained Lieutenant General Robert Ashley (Ret.), who served as director of the Defense Intelligence Agency (DIA).

SCIF is an acronym for a *Sensitive Compartmented Information Facility*, a secure location where classified information is accessed by those wielding clearances. DNI maintains precise technical standards for such locales, including construction designs, limitations on transmitters, and even biometric readers, with the intention of guarding against surveillance efforts by using – among other things – air-gapped networks, which physically separate computers from external Internet connections.

Devices that photograph and connect to an outside signal are therefore highly problematic. In fact, any electronic devices that can be used to snap images or take audio recordings are explicitly banned.

"It transmits. It has an active microphone," Lt. Gen. Ashley told The Cipher Brief. "Everything about [a phone] tells me it does not go in a SCIF."

Such facilities have been historically used to review some of the nation's most sensitive security information. And given the apparent markings on the leaked documents, a considerable number of those files may have been produced as part of a briefing book by the Joint Staff's intelligence arm, known as the J2 – which works in SCIFs.

"Those products only reside on top secret SCI [Sensitive Compartmented Information] computer systems," noted Javed Ali, a former senior U.S. counterterrorism official and Cipher Brief Expert, who explained the systems as part of a discussion on efforts to narrow the circle in identifying potential culprits. And yet those Joint Staff briefings, he added, are generated by "dozens, if not hundreds of people." Plus, once formally approved and disseminated, "we're talking thousands, if not tens of thousands of people who might be getting these on a daily basis." Still, Ali noted, "they had to have originated at some point within a SCIF."

He then posited the question, "Who had access to those briefing slides on that particular day?"

"This is a classic needle in haystack."

It's not just for the President anymore. Are you getting your daily national security briefing? Subscriber+ Members have exclusive access to the Open Source Collection Daily Brief, keeping you up to date on global events impacting national security.

It pays to be a Subscriber+Member.

Meanwhile, Milancy D. Harris, deputy undersecretary of defense for intelligence and security, has reportedly been tasked with leading the Pentagon internal review process, which includes members of legislative affairs, public affairs, policy, legal counsel, and the joint staff.

The mood now is one of "doubling-down," said Lt. Gen. Ashley. "All leaders are talking about this across the [intelligence community]."

More details are also coming to light about the documents themselves, including those purported to show creased folds that may have been smoothed out by the perpetrator before being photographed.

"To me, the creased and folded means they ripped it out of something, took it out of something, or printed it," said Beth Sanner, former Deputy Director for National Intelligence at ODNI and former briefer to President Trump. "In order to put them on the Internet, you would have to physically take a picture of them, or scan them."

The method, she noted, could be to "fold it up, stick in your jacket, [and] go to bathroom," for example, to photograph the documents.

"It would not be weird for someone to leave one of those offices with a briefing book full of classified information and walk to another office," she added. "It would be weird to walk out of the building with that. But lots of people do it," she said. "People aren't checking. Sometimes there are spot checks. But hardly ever. The system depends on culture."

Approximately 24,000 military and civilian employees, and some 3,000 non-defense support personnel, are employed at the Pentagon.

"Ultimately, this is about trust. You put a lot of procedures in place. None of them are going to be absolute," explained Lt. Gen. Ashley. "You can put electronic devices inside facilities that will recognize a phone trying to reach out to a cell tower ... But ultimately when you bring people into these jobs, it's based on a high degree of trust, until proven different."

"We've seen through the years, people with very high levels of clearance that have compromised and that have spied," he added. "Those are the anomalies."

And yet in the ongoing review, experts say there is an expectation for a closer look at legacy systems. Sanner has written about one in particular, regarding the intelligence community's reliance on physical paper. Classified electronic systems, she contends, create better forensic data trails and security measures, such as passwords and timed wipeout programs, which essentially set clocks for data to be removed from tablets, or other devices.

On the go? Listen to the Open Source Report Podcast for your rundown of the biggest national security stories of the day. Listen wherever you subscribe to podcasts.

The focus on the phone, meanwhile, has simultaneously resurfaced a broader conversation from 2018, when the Defense Department issued a memo that called for stricter adherence to practices that required phones be left outside secure areas. DOD authorities reportedly listed "laptops, tablets, cellular phones, smartwatches, and other devices" in a memo, emphasizing the importance of adhering to standards following revelations that seemingly innocuous devices, such as fitness trackers, could be used to track troop locations and other highly-sensitive information.

Taken together, a top Pentagon spokesman on Monday told reporters that the leak, and how the documents were ascertained, presents a "very serious risk to national security."

And yet, according to security experts, this was likely *not* a classic insider threat.

"If it was a hostile intelligence service ... you'd want to keep your insider in place for as long as possible," explained Nick Fishwick, former Senior Member of the British Foreign Office, who served as director general for international operations. "Your insider doesn't suddenly start putting things on the Internet so that the offended country knows it's got a problem."

"It's possible that the Russians might think that given the tremendous benefit of doing this, we'll take a risk in putting this out there. But that doesn't seem to me very likely."

On Tuesday, Britain's Ministry of Defence reported that "a serious level of inaccuracy" was also uncovered in the disclosures, something to which experts often consider hallmarks of foreign disinformation campaigns, including those conducted or aligned with Moscow.

"The way Russians do it is they will take a bunch of true facts, and then sprinkle in their propaganda," said Daniel Hoffman, former senior officer with the Central Intelligence Agency, where he served as a three-time station chief and a senior executive Clandestine Services officer.
One such example, he noted, occurred at the height of the Cold War, when a series of Soviet operations played into public distrust of U.S. institutions, as well as rumors of covert biological warfare programs – something Thomas Boghardt, a historian at the U.S. Army Center of Military History, described as "one of the most successful Soviet disinformation campaigns," falsely linking the AIDS virus to military research conducted at the Fort Detrick Laboratory.

Similar operations from foreign adversaries were launched during the more recent Covid-19 pandemic.

"In the past, this is how the Russians have done stuff," noted Hoffman. "Did they do that in this case? I don't know."

And yet the case is also markedly dissimilar from other recent high-profile insider leaks.

Unlike the cases of former Army intelligence analyst Chelsea Manning, or NSA systems contractor Edward Snowden, who sucked terabytes worth of documents off classified networks into portable devices – these images appear to be of hard copies of briefing slides, which began circulating across social media platforms, including Twitter, Telegram, and Discord, a popular gaming platform.

The scope, thus far, also appears to be considerably more narrow.

"With Snowden, we lost all sorts of sources and methods for NSA," said Sanner. "This is just a very small group of documents. And it's finished intelligence ... it's not an intercept. It is an analytic piece that includes information from all sorts of sources."

"The implications for this are much more tactical and narrow. It doesn't mean that it can't be profound in some ways, but it's not systemic. It's not like we have to go back and redo our algorithm some-how," she explained.

Sanner then paused, and added, "probably."

---

by Cipher Brief Deputy Managing Editor David Aristoto

Read more expert-driven national security insights, perspective and analysis in The Cipher Brief

CATEGORIZED AS: INTELLIGENCE | UKRAINE

TAGGED WITH: INTELLIGENCE | LEAKS | UKRAINE | WASHINGTON

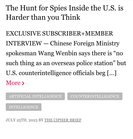
Related Articles

What the American Public Should Know about UFOs

CIPHER BRIEF REPORTING – A retired Air Force Intelligence Officer turned whistleblower testified before a House Oversight Committee on Wednesday that the U.S. government is not [...] More ›

INTELLIGENCE | SPACE | UNITED STATES

JULY 27TH, 2023 BY THE CIPHER BRIEF

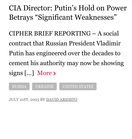


The Hunt for Spies Inside the U.S. is Harder than you Think

EXCLUSIVE:SUBSCRIBER+MEMBER INTERVIEW — Chinese Foreign Ministry spokesman Wang Wenbin says there is "no such thing as an overseas police station" but U.S. counterintelligence officials beg [...] More ›

COUNTER-INTELLIGENCE | COUNTERINTELLIGENCE | INTELLIGENCE

JULY 25TH, 2023 BY THE CIPHER BRIEF



CIA Director: Putin's Hold on Power Betrays "Significant Weaknesses"

CIPHER BRIEF REPORTING – A social contract that Russian President Vladimir Putin has engineered over the decades to cement his authority may now be showing signs [...] More ›

PUTIN | UKRAINE | UNITED STATES

JULY 20TH, 2023 BY DAVID ARISOTO

Featured Piece

Warning Signs of a More Dangerous Global Conflict

BOTTOM LINE UP FRONT — If President Joe Biden's recent remarks in Poland and President Vladimir Putin's in Moscow just a day later are any indication of the path forward, the February 24 anniversary of the Russian invasion of Ukraine may represent the beginning of a new and potentially much more dangerous phase of the conflict, which is increasingly looking like a conflict between NATO and the Russian Federation.

FEB 22, 2023, BY BOB DANNENBERG

About the Cipher Brief

National security is everyone's business. The Cipher Brief is committed to publishing trusted, non-partisan information that brings together the expertise of the public and private sectors.

READ MORE

Book Reviews

View all ›

Defiance: The Latest in The Bourne Series

BOOK REVIEW: Robert Ludlum's The Bourne Defiance By Brian Freeman / G.P. Putnam's Sons Reviewed by Elizabeth C. MacKenzie Biedell The Reviewer: Elizabeth MacKenzie Biedell [...] More ›

JULY 19TH, 2023 BY THE BOURNE DEFIANCE

What the Experts Say

> The Cipher Brief's Open Source Report is an extraordinary product and an important daily read for situational awareness on national security issues.

General John R. Allen (Ret.)
Former Commander of the NATO International Security Assistance Force in Afghanistan