TRUST: IN BID FOR STAY, DOJ LIKENED TRUMP TO CATASTROPHIC INTELLIGENCE COMPROMISE

There's a detail in DOJ's request for a stay of Judge Aileen Cannon's injunction on using stolen Trump documents to investigate Trump that hasn't gotten enough attention.

A footnote modifying a discussion about the damage assessment the Intelligence Community is currently doing referenced a letter then-NSA Director Mike Rogers wrote in support of Nghia Pho's sentencing in 2018. [This letter remains sealed in the docket but Josh Gerstein liberated it at the time.]

> [I]n order to assess the full scope of potential harms to national security resulting from the improper retention of the classified records, the government must assess the likelihood that improperly stored classified information may have been accessed by others and compromised. 4
>
> 4 Departments and agencies in the IC would then consider this information to determine whether they need to treat certain sources and methods as compromised. See, e.g., Exhibit A to Sentencing Memorandum, United States v. Pho, No. 1:17-cr-631 (D. Md. Sept. 18, 2018), D.E. 20-1 (letter from Adm. Michael S. Rogers, Director, National Security Agency) ("Once the government loses positive control over classified material, the government must often treat the material as compromised and take remedial actions as dictated by the

> particular circumstances.”).

Even on its face, the comment suggests the possibility that the Intelligence Community is *shutting down collection programs* because Trump took documents home.

But the analogy DOJ made between Trump and Pho, by invoking the letter, is even worse.

I’ve written about Pho, who with Hal Martin, is believed to be the source of the files leaked by Shadow Brokers and, with them, two devastating global malware attacks, WannaCry and NotPetya.

Over a month ago, I suggested that the IC likely had Pho and Martin in mind as they considered the damage Trump may have done by doing the same thing; taking highly classified files home from work.

> [T]he lesson Pho and Martin offer about how catastrophic it can be when someone brings classified files home and stores them insecurely, no matter their motives — are the background against which career espionage prosecutors at DOJ will be looking at Trump’s actions.

But with the footnote, I’m no longer the only one to make such an analogy. DOJ did so too, in an unsuccessful effort to get Judge Cannon to understand the magnitude of the breach she was coddling.

As you read this letter, replace Pho’s name with Trump’s. It reads almost seamlessly.

That’s the analogy DOJ made between Trump and someone his own DOJ prosecuted aggressively.

> Pho retained classified information outside of properly secured spaces and by doing so caused very significant and long-lasting harm to the NSA, and consequently to the national security of the United States.

> [snip]
>
> [T]he exposure of the United States' classified information outside of secure spaces may result in the destruction of intelligence-gathering efforts used to protect this nation. Mr. Pho, who voluntarily assumed this responsibility, ignored his oath to his country and the NSA by taking classified information outside of secure spaces, thereby placing that information in significant jeopardy.
>
> [snip]
>
> Mr. Pho's conduct in improperly and unlawfully retaining national defense information, which included highly classified information, outside of secure space had significant negative impacts on the NSA mission.
>
> [snip]
>
> Techniques of the kind Mr. Pho was entrusted to protect, yet removed from secure space, are force multipliers, allowing for intelligence collection in a multitude of environments around the globe and spanning a wide range of national security topics. Compromise of one technique can place many opportunities for intelligence collection and national security at risk.
>
> By removing such highly classified materials outside of secure space, Mr. Pho subjected those materials to compromise. It is a fundamental mandate in the Intelligence Community that classified material must be handled and stored in very specific and controlled ways. If classified material is not handled or stored according to strict rules, then the government cannot be certain that it remains secret. Once the government loses positive control over

> classified material, the government must often treat the material as compromised and take remedial actions as dictated by the particular circumstances. Depending on the type and volume of compromised classified material, such reactions can be costly, time consuming and cause a shift in or abandonment of programs. In this case, the fact that such a tremendous volume of highly classified, sophisticated collection tools was removed from secure space and left unprotected, especially in digital form on devices connected to the Internet, left the NSA with no choice but to abandon certain important initiatives, at great economic and operational cost.
>
> In addition, NSA was faced with the crucial and arduous task of accounting for all of the exposed classified materials, including TOP SECRET information, the unauthorized disclosure of which, by definition, reasonably could be expected to cause exceptionally grave damage to the national security. Accounting for all of the exposed classified material was necessary so that NSA could attempt to assess the damage that resulted from the classified and diverted critical resources away from NSA's intelligence-gathering mission.
>
> The detrimental impacts of Mr. Pho's activities are also felt in other less tangible ways, including a loss of trust among colleagues and essential partners who count on NSA to conduct its mission.
>
> [snip]
>
> Trust is an essential component of all of the work that is done by NSA employees. It is affirmed by our sworn oath to uphold and defend the Constitution, sealed by our signed obligations to protect national defense

> information.
>
> [snip]
>
> This trust extends to a circle with other U.S. intelligence agencies, who share valuable intelligence insights; military personnel, who share details of their operational plans; and international partners, who share their sovereign secrets with us, all for common objectives.
>
> [snip]
>
> Future decisions about sharing will be weighted with considerations of the breach of trust by one party.

There's little that distinguishes Pho's compromise from Trump's. While Trump didn't load all this stuff online like Pho did, he brought it to a thinly-protected country club aggressively targeted by foreign intelligence services — a more obvious target than Pho's desktop computer.

And whether the IC knows about the extent of the compromise right now, or whether something he made available will shut down shipping and hospitals and drug manufacturing in two years time, as Pho's compromises did, the IC has to act as if these files have already been compromised.

That's what the footnote says.

As I said, Trump's own DOJ ratcheted up prosecutions in the wake of the Pho and Martin compromises. And now Trump — along with a judge he appointed — are trying to make sure he evades the same justice that his own DOJ demanded of others.

Update: Clarified that Martin and Pho are believed to be the source of the files leaked by Shadow Brokers, but not the leakers themselves.

Go to emptywheel resource page on Trump

Espionage Investigation.