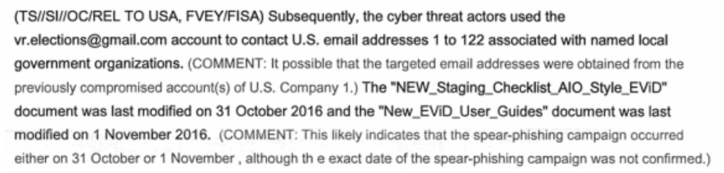
IF WE HAVE TO HAVE FISA, CAN WE AT LEAST NOT GIVE IT TO CONTRACTORS?

In very close succession today, the Intercept published a story on Russia's efforts to hack election-related officials and the government arrested the apparent source for that story, a woman named Reality Winner.

The story — which reports GRU attempted to phish some officials — is most interesting for the dates included in the leaked document accompanying the story. The document — dated May 5 but covering events from last fall — describes phishing attempts starting as early as a month before the election up to October 31 or November 1.



(TS//SI//OC/REL TO USA, FVEY/FISA) Subsequently, the cyber threat actors used the vr.elections@gmail.com account to contact U.S. email addresses 1 to 122 associated with named local government organizations. (COMMENT: It possible that the targeted email addresses were obtained from the previously compromised account(s) of U.S. Company 1.) The "NEW_Staging_Checklist_AIO_Style_EViD" document was last modified on 31 October 2016 and the "New_EViD_User_Guides" document was last modified on 1 November 2016. (COMMENT: This likely indicates that the spear-phishing campaign occurred either on 31 October or 1 November , although th e exact date of the spear-phishing campaign was not confirmed.)

That latest date (on a report published six months later) is interesting because we know President Obama used the cyber "red phone" to contact Vladimir Putin on October 31, for the first time in his presidency, to complain about election-related hacking. The dates here at least suggest that there were no more phishing attempts initiated after that call.

Of course, now Russia knows more details about how granularly, and on what schedule, NSA might learn such details.

The other big part of this incident, however, is the revelation that contractors well outside the known entities (like Booz Allen Hamilton) have access to FISA information — as indicated by the classification stamp — and that even people without a need to know that information can access it.

18. At all times relevant to this affidavit. WINNER has maintained an active Top Secret clearance. The U.S. Government Agency confirmed that although WINNER had the required access to search for and view the intelligence reporting, the information contained in the intelligence reporting is unrelated to her job duties, and WINNER therefore does not possess a "need to know."

This leak was discovered because another of Intercept's sources alerted the NSA. But had that not happened (or had the Intercept not showed the NSA a folded document), then it's not clear this would have been discovered.

I get why we need to disseminate such information widely. But even if this information merely reports on stuff that had already been reported (to the WaPo, long ago), it nevertheless is testament to the degree to which adding contractors adds the likelihood of leaks.

Or let's put it this way: we're sharing FISA information with contractors who don't have a need to know. But we're not sharing it with defendants whose freedom depends on contesting it. Maybe those priorities are screwy?