Questions for the Record from Senator Charles E. Grassley
To Mr. Kenneth Wainstein
U.S. Senate Committee on the Judiciary
"Election Interference: Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm"
Submitted on June 18, 2018

1. You've spoken about the importance of DOJ's Civil Investigative Demand (CID) authority in Foreign Agents Registration Act (FARA) investigations. Please discuss why that authority is needed and how it can help curb improper foreign influence.

As noted in my testimony, the criminal provisions of the Foreign Agents Registration Act (FARA) have rarely been enforced, with only a handful of criminal prosecutions thereunder over the past 50 years. One reason for the lack of enforcement is that the Justice Department lacks authority to compel the production of records that would be instrumental in bringing a FARA prosecution short of empaneling a grand jury to issue a subpoena. These circumstances present an intractable dilemma for the Justice Department: it cannot obtain the subpoena authority to investigate a potentially unregistered foreign agent without establishing the factual predicate of a FARA violation necessary to convene a grand jury, yet it cannot establish that factual predicate without the authority to secure the records that would reveal such a violation in the first place.

Permitting the Justice Department to employ Civil Investigative Demands (CIDs) in FARA investigations would help resolve the existing investigative quandary by permitting limited investigation subject to a lower burden of proof. CIDs have proven effective in investigations brought under other statutes, including the False Claims Act, and this experience can serve as a model for legislating the use of CIDs in FARA investigations.

For example, the Justice Department could issue a CID where it has reason to believe that any person may be in possession, custody, or control of any documentary material, or may have any information relevant to an investigation under FARA. In turn, the Justice Department can use the information it collects to build cases and pursue violators.

More robust FARA enforcement can be expected to not only stop intentional violation of the law but also encourage self-policing and cooperation to avoid punishment. The proper operation of FARA curbs improper foreign influence by better informing the government and the public of the motives and funding of foreign agents engaged in the domestic political process on behalf of foreign principals. Armed with this information, the Justice Department, private organizations, and individuals can better monitor and interdict improper efforts to interfere with domestic elections. For these reasons, I share the view expressed by the Inspector General's Office in its September 2016 FARA report and that of a number of members of Congress, that FARA should be reformed to permit the use of CIDs subject to appropriate procedural safeguards.

2. You've also talked about the need for civil injunctive authority against botnets. Please tell us how Russia and others have used botnets and how civil injunctive authority can be used to stop them.

Russia, other foreign countries, and non-state actors have all made use of botnets in recent years to interfere with the internet operations of our government and critical private-sector industries. Threat actors use botnets for a range of purposes including: to overwhelm servers so that they cannot receive lawful traffic ("DDoS" attacks); to steal sensitive corporate information; to harvest user account information; and to sow and promote disinformation via social media.

There have been a number of noteworthy botnets in recent years. For example, the GameOver Zeus Botnet, operated by Russian Evgeniy Mikhailovich Bogachev, affected as many as a million computers between September 2011 and June 2014 and caused millions of dollars in losses for financial institutions in the form of fraudulent transfers.[1] Others, like the Kelihos botnet, operated by Russian Peter Yuryevich Levashov from 2010 to 2017, used infected computers to distribute spam e-mails, harvest user credentials, and further distribute malware.[2] We also increasingly see botnets used by state actors to advance geopolitical ambitions such as the Advanced Persistent Threat 28 botnet launched no later than 2016 by a Russia-affiliated hacking group named "Sofacy Group."[3] And these examples represent only the tip of the iceberg – only those attacks that our law enforcement identified and stopped.

Our law enforcement deserves credit for dismantling GameOver Zeus in 2014, Kelihos in April 2017, and Advanced Persistent Threat 28 in May 2018, among other successful efforts. Nevertheless, when law enforcement disrupts a botnet, the underlying malicious code often enters the public domain only to re-emerge later in a varied form. Further, as businesses and individuals continue to connect new types of devices to the internet from industrial control systems to cars and "smart speakers" the pool of vulnerable devices and avenues of attack continue to grow.

Given the growing threat posed by botnets, we should empower law enforcement with appropriate response measures. One tool in law enforcement's arsenal is the use of a civil injunction to stop the ongoing activities of a botnet while a criminal case is being built. At present, the government may only seek a civil injunction against a botnet where the government sues for specified acts of fraud or illegal wiretapping. However, as noted above, threat actors

---

[1] U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator, (June 2, 2014), https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware (last visited July 17, 2018).

[2] Justice Department Announces Actions to Dismantle Kelihos Botnet, (April 10, 2017), https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0 (last visited July 17, 2018).

[3] New VPNFilter malware targets at least 500K networking devices worldwide (May 23, 2018), https://blog.talosintelligence.com/2018/05/VPNFilter.html?utm_source=dlvr.it&utm_medium=twitter&utm_campaign=Feed%3A+feedburner%2FTalos+%28Talos%E2%84%A2+Blog%29 (last visited July 17, 2018); Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices (May 23, 2018), https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected (last visited July 17, 2018).

increasingly use botnets to engage in illegal conduct that does not fit these offenses, which leaves law enforcement under-equipped to disrupt botnet activities and provides threat actors a playbook for avoiding interference from law enforcement. Congress can strengthen law enforcement's capabilities and better adapt the law to the various tactics for which botnets are employed by expanding the list of offenses for which injunctive relief may be sought under 18 U.S.C. § 1345, including to address the use of botnets for political interference. Congress has previously considered expanding the list of offenses as recently as 2016 with the Botnet Prevention Act of 2016. I would encourage Congress to revisit these efforts.