U.S. Department of Justice[1]
Office of Legislative Affairs

Office of the Assistant Attorney General Washington, D. C 20530

FEB 1 2 2018

The Honorable Richard M. Burr
Chairman
The Honorable Mark Warner
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance before the Committee of FBI Deputy Director Andrew McCabe on May 22, 2017, at a hearing concerning worldwide threats.

Thank you for the opportunity to present our views. Please do not hesitate to contact this office if we may be of additional assistance to you. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Stephen E. Bephen E. Boyd
Assistant Attorney General

Enclosure

RESPONSES OF ANDREW MCCABE DEPUTY DIRECTOR FEDERAL BUREAU OF INVESTIGATION

[1] **OCRed and uploaded by SHF**i, June 18, 2019. The original is https://www.intelligence.senate.gov/sites/default/files/documents/FBI%20Response%20to%20Committee%20Questions%20for%20the%20Record.pdf

To QUESTIONS FOR THE RECORD
ARISING FROM A HEARING BEFORE
THE
SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE

CONCERNING . WORLDWIDE THREATS

MAY 22, 2017

Questions from Senator Harris:

(U) As you may be aware, it has been reported that when the FBI learned that the Democratic National Committee (DNC) was hacked, it failed to reach out to DNC leadership directly, and instead called the Committee's IT "help desk." (See, e.g. The New York Times, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," Dec. 13, 2016).

1. Is the press characterization accurate? If not, please characterize FBI's notification efforts and timeline accurately.

Response:

(U//FOUO) The timeline and characterization of the FBI's notification efforts to the Democratic National Committee ("DNC") in the referenced New York Times article is incomplete. FBI began its notification efforts to the DNC on 06 August 2015 after FBI received reporting that the DNC was compromised by the advanced persistent threat actor referred to as CozyBear. After FBI requested to speak with the individual responsible for maintaining the IT systems, DNC referred the FBI to its Director of IT Yared Tamene. He was quickly identified to be the appropriate person to receive victim notifications on behalf of the DNC. The FBI was not initially aware that Tamene was a contract employee. His status as a contractor was not an issue because the DNC Chief Operating Officer Lindsey Reynolds, Technology Director Andrew Brown, DNC counsel Graham M. Wilson and DNC counsel Michael Sussmann were fully aware of the details of the compromise, and the fact that Tamene was the FBI's primary point of contact throughout the investigation. DNC executive management endorsed the FBI communicating technical details of the compromise with Tamene.

(U//FOUO) FBI provided DNC with two compromised IP addresses during this initial notification, indicated the DNC could potentially be a victim or a future victim of an ongoing e-mail spear-phishing campaign, and advised the activity may be related to open source threat reporting under the names Miniduke and Minidionis. FBI had no reason to believe the information was not being handled appropriately, or that an in-person notification was warranted.

(U//FOUO) FBI's initial notification to DNC followed FBI's well-defined procedures for conducting expeditious notification to victims via the most reliable method available. FBI typically notifies the "individual, organization, or corporation that is the owner or operator of the computer at the point of compromise or intrusion" as they are in the best position to

take immediate action on the information provided. On multiple occasions thereafter, FBI requested to be connected with the individual in charge of the IT systems at DNC, and was always directed to the same individual, Yared Tamene. Furthermore, once senior level DNC members became involved in the matter, DNC counsel confirmed that the FBI should continue to work through this individual.

(U//FOUO) FBI re-contacted DNC in December 2015 to advise that DNC systems were likely still compromised and to provide additional threat information. In January 2016, the FBI provided the DNC with an open source report titled *The Dukes: 7 Years of Russian cyberespionage*, which contained additional background on the threat actors. The FBI continued to notify the DNC when information was received that led FBI to believe that the DNC was still compromised. In February 2016, the FBI offered the use of a cyber response team to help identify the malicious traffic on DNC's network and offered to deploy a sensor on the network to help identify the malicious traffic; however, both offers were declined by the DNC.

(U//FOUO) In March 2016 FBI notified DNC about a spear-phishing campaign by a second adversary, referred to as FancyBear, against the DNC. FBI notified DNC again in April 2016 about a second set of FancyBear spear-phishing targets and identified users who clicked malicious links. FBI requested and received log files from DNC in April 2016. FBI continued to follow-up with DNC through June 2016, at which point a private security firm began providing mitigation services to the DNC, and the FBI began working directly with that firm.

2. Given the FBI's long-standing knowledge of Russia's influence efforts- including its use of cyberattacks to disrupt other countries' political processes- why wasn't the FBI's response more aggressive?

Response:

(U//FOUO) The cyber campaign in question targeted over 130 US victim companies and corporations, just one of which was the DNC. FBI exceeded standard procedures in its victim engagement with the DNC and believed the matter was being handled appropriately, so there was no reason to further elevate the notification. Due to the size and scope of the malicious campaign in the summer of 2015, the most rapid and reliable method available for notification was direct telephonic notification. The FBI did recognize the high-profile nature of this victim, and acted accordingly.. The FBI had over 30 separate interactions with DNC IT and executive management. The FBI offered the use of a cyber response team to help identify the malicious traffic on their network and the FBI offered to deploy a sensor on the network to help identify the malicious traffic; however, both were declined. Instead, the DNC retained a private security firm to manage detection and remediation.

3. Why did the FBI wait until July 2016 to open an investigation into Russian interference in the 2016 U.S. election?

Response:

As described in part above, the FBI investigated malicious activity by Russian actors (both the theft and dissemination of information) as it learned of it, well-before the election (in 2015 and earlier) and continuing until after the election, in collaboration with various components of the Justice Department, including, after his appointment, the Special Counsel.

4. What has the FBI done to better assess and respond to these types of cyber intrusions?

Response:

(U//FOUO) The Department of Justice is currently conducting a review of the FBI's victim notification procedures. Although the review is still ongoing, the FBI believes the DNC notification was compliant with both 0395PG (internal notification policy) and PPD-41 (even though not in effect at the time of initial notification(s)). [Administrative note: PPD-41 was signed July 26, 2016, or approximately 45 days after the DNC data had been posted by online persona Guccifer2.0.] PPD-41 advises the private sector and Government agencies have a shared vital interest and complementary roles and responsibilities.

(U//FOUO) FBI has taken steps to increase its outreach efforts with sectors affected by the 2015/2016 election-related intrusions and intrusion attempts, and FBI continues to use unclassified bulletins to inform private sector entities about continuing advanced persistent threat activity and mitigation strategies.

(U//FOUO) In April 2016, FBI hosted a tabletop training exercise modeled on the actual CozyBear campaign from July 2015, which DNC attended. The purpose of the exercise was to familiarize participating organizations with spear-phishing campaigns, indicators of compromise, and to provide suggestions to improve information sharing between other government agencies, the private sector, and FBI. The Republican National Committee (RNC) was also provided information from the exercise.

(U//FOUO) Between October 2016 and July 2017, FBI and/or Department of Homeland Security released five reports to the private sector regarding advanced persistent threat tactics, indicators, and recommended actions.

(U//FOUO) In April and May 2017, FBI Cyber Division re-engaged with voting systems companies and asked FBI field offices to have conversations with companies about the threat landscape and what, if any, threats they have seen since the 2016 election cycle. As of June, voting systems companies have not observed any targeting activity but communication lines remain open for information sharing and engagement. Additionally, FBI Cyber Division and related field offices are planning multiple tabletop training exercises for the 2018 election cycle.

(U//FOUO) On a larger scale, as far back as 2013, the FBI Cyber Division reorganized the manner in which it investigates state-sponsored computer intrusion activity. The Cyber Threat Team ("CTT") model established a standard to narrowly define, scope, and prioritize over 70 nation-state sponsored cyber threats. The traditional FBI investigative model focuses on the victim. If a crime occurs in a field office's geographic area of responsibility ("AOR"), then that field office opens an investigation. Due to the distributed nature of a cyber actor's victims, this

created a situation where each field office was investigating dozens of computer intrusions, Numerous field offices would be investigating the same actor's criminal activity.

(U//FOUO) The CTT model shifted the focus to the nation-state actors, with a select group of field offices responsible for each cyber threat. Each threat is investigated by a team consisting of 2-6 field offices and a FBI Headquarters support team. This team is often times assisted by resources from other USIC agencies and allied foreign partners. This proved to be a far more efficient and effective use of the FBI's cyber resources. Approximately 80% of all field offices are assigned less than 3 threats, better distributing the workload and technical expertise of the FBI. A comprehensive threat picture is developed and owned by the designated CTT, thus enabling those assigned field offices to become the subject matter experts on the threat. The 70+ global nation-state cyber threats are banded for prioritization purposes. The top priorities are categorized as National Threat Priorities ("NTP"). Additional bands are groups 2-6. The actual categorization of various threats are classified and are not appropriate for this document.

(U//FOUO) In addition, also since approximately 2012, the FBI Cyber Division has worked closely with the Department of Justice's National Security Division and U.S. Attorney's Offices around the country to bring all legal tools (including but not limited to prosecution) to bear on the threats posed by state-sponsored hacking and other malicious activities (like influence operations) that might exploit it). Through these efforts, we have charged, arrested, and successfully prosecuted individuals working for (or for the benefit of) foreign states.

In doing so, DOJ and FBI seek to raise the costs of the activity, including by supporting the efforts of other departments and agencies, and to educate the American people about the threats we face (so they can better protect themselves and their networks).

5. Are we better positioned today to prevent, detect, and respond to comparable cyber intrusions? If not, what should we be doing differently?

Response:

(U//FOUO) The FBI can only respond to reports of computer intrusions and attacks that it learns of, and many victims prefer, for a variety of reasons, to remediate intrusions in-house or with the assistance of private security firms, rather than report the intrusion to the government and avail themselves of our assistance. Encouraging reporting by victims is one of the Department of Justice's priorities in its frequent outreach events to the private sector, and we would welcome reinforcement of that encouragement.

6. From September 2015 to July 5, 2016, how was the assessment or preliminary investigation into hacking of computer systems belonging to the Democratic National Committee and the Republican National Committee (or state or local electoral boards) staffed? Please include an explanation of the number of agents assigned full-time to the investigation and the overall staffing plan.

Response:

(U//FOUO) The FBI staffs all investigations with a combination of agent and analytical support. The exact number of personnel involved varies depending on the complexity and stage of the investigation.

7. From July 6, 2016 to November 8, 2016, how was the investigation into Russian interference in the 2016 election staffed? Please include an explanation of the number of agents assigned full-time to the investigation and the overall staffing plan,

Response:

(U//FOUO) See the response to the preceding question.

8. How is the investigation into Russian interference into the 2016 election currently staffed? Please include an explanation of the number of agents assigned full-time to the investigation and the overall staffing plan.

Response:

(U//FOUO) This question should be referred to the Special Counsel.