United States Senate
WASHINGTON, DC 20510

June 12, 2019

The Honorable Christopher A. Wray
Director
Federal Bureau of Investigations
935 Pennsylvania Avenue, NW
Washington, D.C. 20535

Dear Director Wray:

We write to better understand the steps that the FBI has taken to investigate potential cyber-intrusions by the Russian government into election technology vendors.

In April of 2019, the Department of Justice released a redacted copy of the Report On The Investigation Into Russian Interference In The 2016 Presidential Election by Special Counsel Robert Mueller ("the Mueller Report"), which described how Russian government hackers targeted U.S. election infrastructure. The Mueller Report revealed that "[i]n August 2016, GRU officers targeted employees of [redacted], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network."

VR Systems, a Florida-based manufacturer of voter registration software and electronic pollbooks has since confirmed to the media that it was the redacted voting technology company in the Mueller Report. In a May 16, 2019, letter to Senator Wyden, VR Systems described how it participated in an August 2016 conference call with law enforcement. Participants in that call were apparently asked by the FBI to "be on the lookout for certain suspicious IP addresses." According to VR Systems, the company examined its website logs, "found that several of the IP addresses had, in fact, visited our website" and as a result, the company "notified the FBI as we had been directed to do." VR Systems indicates they did not know that these IP addresses were part of a larger pattern until 2017, which suggests that the FBI may not have followed up with VR Systems in 2016 about the nature of the threat they faced.

While the Mueller Report revealed several new details about Russia's attempts to interfere with our election in 2016, Congress and the American people still do not have a complete picture of the federal government's efforts to detect and defend against this attack against our democracy. To that end, please provide us with complete answers to the following questions by July 12, 2019:

1. What steps, if any, did the FBI take to examine VR Systems' servers for evidence of a successful cyber breach after the company alerted the FBI, in August of 2016, to the presence of suspicious IP addresses in its website logs? If the FBI did not examine VR Systems' servers or request access to those servers, please explain why.
2. Several months after VR Systems first contacted the FBI, electronic pollbooks made by the company malfunctioned during the November 8 general election in Durham County,

North Carolina. In the two and a half years since that incident in Durham County, has the FBI requested access to the pollbooks that malfunctioned, and the computers used to configure them, in order to examine them for evidence of hacking? If not, please explain why.

3. VR Systems contracted FireEye to perform a forensic examination of its systems in the summer of 2017. Has the FBI reviewed FireEye's conclusions? If so, what were its key findings?
4. Ahead of the 2020 elections, how is the FBI ensuring that local and state election officials feel comfortable reporting potential cybersecurity incidents? How will the FBI improve the speed and completeness of the information it shares with election officials, so they have the knowledge of the threats they need to do their job?

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Amy Klobuchar
United States Senator