ATTORNEY GENERAL JOSH STEIN

February 19, 2018

The Honorable Kirstjen Nielsen
Secretary of Homeland Security
Department of Homeland Security
Washington, DC 20528

RE: Protecting North Carolina's Election Systems Against Attacks by Malicious Actors

Dear Secretary Nielsen:

As the Attorney General of North Carolina, I have grown increasingly alarmed as more and more evidence has emerged publicly about malicious actors' use of digital technology to interfere with state-run elections. Based on recent public testimony from national intelligence officials, this issue relates not just to past elections, but also to future ones, including in 2018.

To recap some of the information that has come to light:

- In the fall of 2016, leading up to the general election, the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (DNI) confirmed that the Russian government had orchestrated the hacking of private computer systems of the Democratic National Committee.[1] DHS and DNI also determined that servers operated by a Russian company had scanned and probed certain state election systems.[2] In some instances, "malicious actors gained access to state voting-related systems."[3] DHS and DNI did not publicly reveal at that time which states had been targeted.

- On Election Day 2016, North Carolina experienced significant software-related problems in several of the state's largest cities. These issues resulted in hours-long delays in some polling places and may have led some voters to leave before casting their ballots. The source of these problems is still under investigation. To

[1] *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security* (Oct. 7, 2016), *available at* https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.
[2] *Id.*
[3] *Statement by Secretary Johnson About Election Systems' Cybersecurity* (Oct. 1, 2016), *available at* https://www.dhs.gov/news/2016/10/01/statement-secretary-johnson-about-election-systems-cybersecurity.

JOSH.STEIN@NCDOJ.GOV 114 W. EDENTON STREET, RALEIGH, NC 27603 P. O. BOX 629, RALEIGH, NC 27602-0629 919.716.6400

date, there is no clear evidence that they resulted from hacking. However, it is notable that in June 2017, it was publicly reported that VR Systems, a software vendor whose products were involved in some of these disruptions in North Carolina, had itself been targeted by hackers.[4]

- In June 2017, DHS official Samuel Liles testified that Russia had targeted the election-related systems in at least 21 states, but did not publicly identify which states had been targeted.[5]

- On February 13, 2018, DNI Director Daniel Coats testified in prepared remarks to the Senate Intelligence Committee that "[t]here should be no doubt that Russia perceives its past efforts as successful and views the 2018 U.S. midterm elections as a potential target for Russian influence operations."[6]

- On February 16, the U.S. government indicted more than a dozen Russian nationalists and businesses for using "fraud and deceit for the purpose of interfering with the U.S. political and electoral system, including the presidential election of 2016."[7] Some of these attempts directly targeted North Carolina, including through the use of Russian-controlled Twitter accounts in August 2016 to disseminate false allegations that voter-fraud investigations had been launched in North Carolina, and to pose as grassroots activists after the election to arrange an anti-Trump rally in Charlotte.[8]

Attempts to interfere with technological infrastructure used in state elections, or to use misinformation to intimidate or discourage voters as they exercise their right to vote, may violate not only federal law, such as the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, but also North Carolina law.[9]

---

[4] National Security Agency, *Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors <REDACTED>, Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016, available at* https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1; Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim, *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, The Intercept (June 5, 2017), *available at* https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/;

[5] *Written Testimony of I&A Cyber Division Acting Director Dr. Samuel Liles, and NPPD Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra for a Senate Select Committee on Intelligence Hearing Titled 'Russian Interference in the 2016 U.S. Elections* (June 21, 2017), *available at* https://www.dhs.gov/news/2017/06/21/written-testimony-ia-cyber-division-acting-director-dr-samuel-liles-and-nppd-acting.

[6] Matthew Rosenberg and Nicholas Fandos, *Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn*, The New York Times (Feb. 13, 2018), *available at* https://mobile.nytimes.com/2018/02/13/us/politics/russia-sees-midterm-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html?emc=edit_na_20180213&nl=breaking-news&nlid=56986533&ref=cta&referer.

[7] *United States v. Internet Research Agency LLC*, Indictment ¶ 2 (D.D.C. Feb. 16, 2018).

[8] *Id.* ¶¶ 36, 57.

[9] N.C. Gen. Stat. § 14-458 (outlawing computer trespass and providing criminal and civil remedies); N.C. Gen. Stat. § 163-275(17) (outlawing use of mass communication technology to intimidate or discourage voters).

Malicious actors' attempts to disrupt our elections systems are not merely illegal; they strike at the very heart of our democracy. To respond adequately to this grave threat, government officials at all levels—federal, state, and local—must work together in a coordinated and constructive fashion, with pertinent, actionable information flowing in all directions.

North Carolina's situation illustrates the need for information-sharing among all levels of government: federal officials need information from states and localities about the particularities of their election systems, while state officials need information from federal agencies about known vulnerabilities and risks. Election systems in North Carolina for federal, state, and local elections are jointly administered by the State and its 100 counties. Some items of election-related computers and software are owned and operated by the State, while others are owned and operated by counties. In September 2017, DHS informed North Carolina that it was not aware at that time of evidence that *state*-owned or *state*-operated elections infrastructure in North Carolina had been accessed by unauthorized individuals. However, it is my understanding that DHS did not provide information about whether it has evidence of hackers having targeted *county*-owned or *county*-operated infrastructure. DHS also did not provide information about whether it is aware of evidence of hackers having targeted third-party vendors (such as VR Systems) that contract with the State or with its counties in ways that could impact the State or counties.

Many public reports indicate that the DHS and federal intelligence agencies have collected substantial information and evidence related to actual and potential interference with state-run election processes. I am aware that some information is being shared with state election administrators around the country, including in North Carolina, as well as with some other state officials. Since September 2017, North Carolina has taken advantage of certain programs and tests offered by DHS to address election security. We appreciate these efforts by DHS. However, I am also aware of many reports and concerns that federal officials have at times been slow to share information and have not sufficiently coordinated their efforts with state officials.[9]

It is of urgent importance to the integrity of our electoral processes that DHS and other federal agencies coordinate extensively and effectively with state officials – including those responsible for law enforcement, electronic security, elections administration, and public safety. While I understand the sensitive nature of much of the information that has been collected by federal agencies, it is vital that federal officials share pertinent information with state officials. DHS should make as much information as possible available to state officials regarding past, current, and anticipated future attempts to compromise electronic elections systems in our state. Without this information, state officials may be unable to take appropriate and necessary actions to ensure that hacking and other forms of disruption by malicious actors do not occur in upcoming elections.

The right of eligible citizens to vote and to have their votes accurately counted is sacrosanct. Efforts by anyone, but particularly foreign nationals or foreign governments, to tamper with the security of our elections systems is not only criminal, but it also undermines public confidence in the highest act of democracy and is intolerable. As Attorney General of

[9] *See, e.g.*, Brian Slodysko, *State election officials worry about 2018 election security*, PBS NewsHour (Jul. 9, 2017).

North Carolina, I am committed to doing everything I can to ensure the fairness and integrity of my state's voting processes to protect our democracy and to restore people's confidence in our elections. Therefore, I ask that DHS share with us all relevant information about how we can protect our citizens and our system of elections administrations.

Specifically, I request that DHS and other federal agencies and departments expeditiously provide my office with as much detail as possible about the following issues:

1. Whether DHS or other federal agencies are aware of specific or general vulnerabilities in the digital election infrastructure currently used in North Carolina.
2. Whether DHS or other federal agencies are aware of specific or general vulnerabilities in other commonly used elections hardware and software systems and if so, what they are.
3. Whether DHS or other federal agencies have identified any countermeasures that county, state, and federal officials may use to attempt to mitigate any vulnerabilities.
4. An update to the NSA report detailing Russian hacking efforts in the 2016 election as it relates to North Carolina or any election-system vendors whose products are used in North Carolina.
5. Any other information that would be of potential value in helping the State of North Carolina or our counties take appropriate and effective proactive measures to prevent malicious interference with our elections in 2018 and beyond.

Time is of the essence. This year, North Carolina will be holding federal, state, and local elections. Our primaries will occur in fewer than three months. I would appreciate a written response by March 5, 2018 with as much supporting information as you can provide at that time. I understand that some of this information may be classified and may only be able to be shared with members of my staff with appropriate security clearances.

Thank you very much for your cooperation with this important inquiry. We look forward to your response.

Sincerely,

Josh Stein

cc: Director Daniel Coats
North Carolina Congressional Delegation
Governor Roy Cooper

Enclosures