Statement of Jeh Charles Johnson
Before the House Permanent Select Committee on Intelligence
June 21, 2017

Representative Conaway, Representative Schiff and other Members of this Committee:

In 2016 the Russian government, at the direction of Vladimir Putin himself, orchestrated cyberattacks on our Nation for the purpose of influencing our election – plain and simple. Now, the key question for the President and Congress is: what are we going to do to protect the American people and their democracy from this kind of thing in the future?

I am pleased this Committee has undertaken this investigation, and I hope you find answers.

From December 23, 2013 to January 20, 2017 I served as Secretary of Homeland Security. During that time, I had the privilege of working with Congress to provide additional authorities to the Department of Homeland Security ("DHS") to defend the Nation's and the federal government's cybersecurity, through the Cybersecurity Act of 2015,[1] the National Cybersecurity Protection Advancement Act,[2] the Federal Information Security Modernization Act of 2014,[3] and other new laws.[4]

But, there is more to do.

Cyberattacks of all manner and from multiple sources are going to get worse before they get better. In this realm and at this moment, those on offense have the upper hand. Whether it's cyber-criminals, hacktivists, or nation-state actors, those on offense are ingenious, tenacious, agile, and getting better all the time. Those on defense struggle to keep up. As in other matters of homeland security, we must mobilize our Nation in support of stronger cyber defenses.

The views I express here are my own, based upon my personal experiences in national security and, now, as a concerned private citizen. The factual testimony I offer here is based on my best recollection of events months past, without the opportunity to review internal government documents or classified material.

[1] Pub. L. No. 114-113, 129 Stat. 2935 (2015).
[2] Pub. L. No. 113-282, 128 Stat. 3066 (2014).
[3] Pub. L. No. 113-283, 128 Stat. 3073 (2014).
[4] *See also* the Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277, 128 Stat. 2995 (which includes additional authorities for cybersecurity recruitment and retention).

Sometime in 2016 I became aware of a hack into systems of the Democratic National Committee. Fresh from the experience with the Office of Personnel Management, I pressed my staff to know whether DHS was sufficiently proactive, and on the scene helping the DNC identify the intruders and patch vulnerabilities. The answer, to the best of my recollection, was not reassuring: the FBI and the DNC had been in contact with each other months before about the intrusion, and the DNC did not feel it needed DHS's assistance at that time.

As summer 2016 progressed, my concerns about the possibility of a cyberattack around our national election grew. I probed with the cybersecurity experts at DHS what more we could and should be doing. We developed a plan to engage state election officials to offer our cybersecurity assistance to them. My staff also suggested to me that I could, under my existing authorities, declare election infrastructure to be "critical infrastructure" in this country. There are 16 infrastructure sectors – *e.g.*, financial services, dams, transportation, government facilities, the defense industrial base – that are already considered critical infrastructure. By adding election infrastructure to that list, for cybersecurity purposes it would principally mean two things: (1) that election officials, upon request, would be a top priority for the receipt of DHS's services, and (2) that, as part of critical infrastructure, election infrastructure would receive the benefit of various domestic and international cybersecurity protections.

On August 3, 2016, in an on-the-record session with reporters, I publicly floated the idea of designating election infrastructure in this country as critical infrastructure.

Twelve days later, on August 15, I convened a conference call with secretaries of state and other chief election officials of every state in the country. I told state officials that we must ensure the security and resilience of election infrastructure, and offered DHS's assistance to the states in doing that. I also reiterated the idea of designating election infrastructure as critical infrastructure.

To my disappointment, the reaction to a critical infrastructure designation, at least from those who spoke up, ranged from neutral to negative. Those who expressed negative views stated that running elections in this country was the sovereign and exclusive responsibility of the states, and they did not want federal intrusion, a federal takeover, or federal regulation of that process. This was a profound misunderstanding of what a critical infrastructure designation would mean, which I tried to clarify for them.

But, based on what I heard on the call, my team and I decided that a critical infrastructure designation at that time, during the election season, would be

counterproductive. I remained convinced it was a good idea, but we put the idea on the back burner. Instead, and more importantly in the time left before the election, we encouraged the states to seek our cybersecurity help. Prior to the election, encouraging the horses to come to the water had to be the primary objective.

At around the same time we were engaging state election officials, my staff and I began to see and hear very troubling reports of scanning and probing activities around various state voter registration databases. This was obviously a matter of great concern. In the latter half of August, the FBI issued an alert to the states about these activities, which included the IP addresses of those associated with the attempted hacks.

Both publicly and privately, my staff and I repeatedly encouraged state and local election officials to seek our cybersecurity assistance.

On September 16, I issued one of a number of public statements encouraging the state election officials to strengthen their cybersecurity, and describing the range of services DHS could provide. In that statement I also said the following:

> *"In recent months we have seen suspicious cyber intrusions involving political institutions and personal communications. We have also seen some efforts at cyber intrusion of voter registration data maintained in state election systems. We have confidence in the overall integrity of our electoral systems. It is diverse, subject to local control, and has many checks and balance[s] built in. Nevertheless, we must face the reality that cyber intrusions and attacks in this country are increasingly sophisticated, from a range of increasingly capable actors that include nation-states, cyber hacktivists, and criminals. In this environment, we must be vigilant."*

In September, President Obama personally asked congressional leaders to issue a bipartisan call to state election officials to seek DHS's cybersecurity assistance. Speaker Ryan, Leader Pelosi, and Senators McConnell and Reid did so, in a joint letter dated September 28.

On October 1, I issued a public statement thanking the congressional leaders for their letter, and once again encouraged the states to seek our assistance. Here again I warned of the threat we were seeing to state voter election data:

> *"In recent months, malicious cyber actors have been scanning a large number of state systems, which could be a preamble to attempted intrusions. In a few cases, we have determined that malicious actors gained access to state voting-related systems. However, we are not aware at this time of any manipulation of data. We must remain vigilant and continue to address these challenges head on."*

Meanwhile, in the August-September timeframe, our intelligence community became increasingly convinced that the Russian government was behind the hacks of the DNC and other political institutions and figures.

I and others also became personally convinced that we needed to inform the American public, prior to the election, of what we knew the Russian government was doing. In the midst of the politically-charged election season, with accusations by one of the candidates that the election was going to be "rigged," attribution was going to be a big and unprecedented step, and required careful consideration. However, we recognized we had an overriding responsibility to inform the public that a powerful foreign state actor had covertly intervened in our democracy.

Therefore, on October 7, Director Clapper and I issued the statement formally and publicly accusing the Russian government of directing cyber "thefts and disclosures [that] are intended to interfere with the US election process." In this statement, we also warned again that "[s]ome states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company" (we were not then in a position to attribute this activity to the Russian government) and once again encouraged state election officials to seek DHS's assistance.

Three days later, on October 10, I issued another public statement encouraging states and other jurisdictions to seek our assistance in the 29 days before the election.

Prior to election day, I also personally reviewed with the CEO of the Associated Press its long-standing election-day reporting process, including the redundancies and safeguards in its systems.

By election day on November 8, a large number of state and local election officials did in fact respond to our offers of cybersecurity assistance. More specifically, almost every state contacted DHS about its services, and 33 states and 36 cities and counties used DHS tools to scan for potential vulnerabilities and/or sought mitigation advice from us. Overall, DHS proactively provided election-related mitigation advice and cyber threat indicators/information for network defense to likely hundreds, if not thousands, of state and local officials.

On election day, DHS assembled a crisis-response team to rapidly address any reported cyber intrusions into the election process.

To my current knowledge, the Russian government did not through any cyber intrusion alter ballots, ballot counts or reporting of election results. I am not in a position to know whether the successful Russian government-directed hacks of the DNC and elsewhere did in fact alter public opinion and thereby alter the outcome of the presidential election.

Following the election, and at the direction of President Obama, on December 29 the U.S. government took a number of steps in response to the Russian government's efforts to interfere with our election. These included a joint report by DHS and the FBI providing details about the tools and infrastructure used by the Russian government to compromise networks associated with the election.

On January 6, 2017, and also at the direction of President Obama, the intelligence community released an unclassified public report, "Assessing Russian Activities and Intentions in Recent US Elections," to better educate the public about what had happened.

Following the election, I also returned to the issue of the designation of election infrastructure as critical infrastructure. Throughout the fall, my staff had continued the dialogue with state election officials about the designation. Following the election, my staff reported to me that state officials' stated views of the designation had not changed, and continued to be neutral to negative.

On January 5, I had one more conference call with state election officials to be sure I understood their reservations. Notwithstanding what I heard, I had become convinced that designating election infrastructure as critical infrastructure was something we needed to do.

The next day, January 6, I issued a public statement announcing my determination that election infrastructure in this country should be designated as a

subsector of the existing "Government Facilities" critical infrastructure sector. I am pleased that Secretary Kelly has reaffirmed that designation.

This very troubling experience highlights cyber vulnerabilities in our political process, and in our election infrastructure itself. With the experience fresh in our minds and clear in our rear-view mirror, we must resolve to further strengthen our cybersecurity generally, and the cybersecurity around our political/election process specifically. As I said at the outset, the key question for the President and Congress is: what are we going to do to protect the American people and their democracy from future cyberattacks?

I am prepared to discuss my own views on this topic, and look forward to your questions.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu