MEMORANDUM
August 2, 2017

To: Senate Homeland Security and Governmental Affairs Committee Members

Fr: Homeland Security and Governmental Affairs Committee Democratic Staff

Re: Additional Information from DHS Concerning Election Infrastructure

---

At the direction of Ranking Member Claire McCaskill, the Democratic staff of the Senate Committee on Homeland Security and Governmental Affairs is conducting ongoing oversight over the designation of election infrastructure as a critical infrastructure subsector by the U.S. Department of Homeland Security (DHS). This memorandum provides additional information to committee members based on materials recently received from DHS on this matter.

I. BACKGROUND

On October 7, 2016, DHS and the Office of the Director of National Intelligence (ODNI) issued a joint statement explaining, "Some 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."[1] It has been publicly reported that state and local election databases were subjected to a large scale hacking attempt during the 2016 election. According to the congressional testimony of DHS officials "One comprehensive intelligence report … established that Internet connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors."[2] DHS officials also testified: "a small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states where only preparatory activity like scanning was observed."[3]

It has been reported that in one state, more than 90,000 records, more than 90 percent of which contained personal identification information such as driver's license numbers and partial

---

[1] U.S. Department of Homeland Security and the Office of the Director of National Intelligence, *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security* (Oct. 7, 2016) (https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national).

[2] Senate Select Committee on Intelligence, Joint Testimony of Jeanette Manfra, Acting Deputy Under Secretary for Cyber Security and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, and Dr. Samuel Liles, Acting Director, Cyber Division, Office of Intelligence and Analysis, U.S. Department of Homeland Security, *Hearing on Addressing Threats to Election Infrastructure*, 115th Cong. (Jun. 21, 2017).

[3] *Id.*

Social Security numbers were stolen.[4] Reports also indicate that at least one attempt to alter voter information contained in the hacked databases was successful.[5] In another state, the press has reported that hackers successfully accessed a campaign finance database, and in Illinois there is evidence that cyber intruders attempted to delete or alter voter data.[6] News outlets have reported that as early as June 2016, Illinois and Arizona both experienced successful intrusions into voter registration databases, although no information was altered at that time.[7] DHS said that none of the hacked systems were involved in vote counting; there is no evidence that votes were changed.[8]

In January 2017, ODNI released a report documenting Russian intervention in the 2016 election. The report found that Russian agents employed a multi-faceted strategy to affect 2016 state and local elections, influencing the United States' electorate through social media, television programming, and direct hacking attempts.[9] The Intelligence Community (IC) found that this effort represented the most recent of many Russian attempts to undermine the U.S.-led democratic order, and was a significant escalation in the scope of activity. [10] The report concluded that given the perceived success of the influence campaign to undermine United States democracy, Russia will use the information and tactics gained during the 2016 election effort to inform future operations in the United States and worldwide.[11] The IC found:

> We assess Moscow will apply lessons learned from its campaign aimed at the US presidential election to future influence efforts in the United States and worldwide, including against US allies and their election processes.[12]

On January 6, 2017, the Obama Administration announced that election infrastructure would be designated a critical infrastructure subsector within the Government Facilities Sector.[13]

---

[4] *Election Hackers Altered Voter Rolls, Stole Private Data, Officials say*, Time Magazine (Jun. 22, 2017) (http://time.com/4828306/russian-hacking-election-widespread-private-data/).

[5] *Id.*

[6] *Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known*, Bloomberg (Jun. 13, 2017) (https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections).

[7] *FBI director: Hackers 'poking around' voter systems*, CNN (Sept. 28, 2016) (http://www.cnn.com/2016/09/28/politics/fbi-james-comey-election-cyberattacks/).

[8] *DHS officials: 21 states potentially targeted by Russia hackers pre-election*, CNN (Jul. 18, 2017) (http://www.cnn.com/2017/06/21/politics/russia-hacking-hearing-states-targeted/index.html).

[9] Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent US Elections* (ICA 2017-01D) (Jan. 6, 2017).

[10] *Id.*

[11] *Id.*

[12] *Id.*

Former Homeland Security Secretary Jeh Johnson described "election infrastructure" as "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments."[14] The designation allows states, localities, tribal, and territorial governments to voluntarily receive prioritized cybersecurity assistance from DHS.[15]

Ranking Member McCaskill wrote to former Secretary John Kelly on March 7, 2017, seeking information about the designation and the implementation plans of the Department. This memorandum provides additional information based on the responses recently received by the Ranking Member from DHS.

II. CRITICAL INFRASTRUCTURE DESIGNATION

On January 6, 2017, the Obama Administration announced that election infrastructure would be designated a subsector of the government facilities critical infrastructure sector.[16] According to former Secretary Kelly, this designation "enables state, local, tribal, and territorial governments, and private sector owners and operators to receive prioritized assistance from the Federal Government for their efforts to mitigate risks to election infrastructure."[17] DHS emphasizes that participation with the federal government is voluntary "and does not involve federal intrusion, takeover, or regulation of any kind."[18]

DHS informed the Ranking Member:

> This designation does not allow for technical access by the Federal Government into the systems and assets of election infrastructure, without voluntary legal agreements made with the owners and operators of these systems. This dynamic is consistent with engagements between the Federal Government and other previously established critical infrastructure sectors and subsectors, including the chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities,

---

[13] U.S. Department of Homeland Security, *Fact Sheet: Designation of Election Infrastructure as Critical Infrastructure* (Jan. 6, 2017).

[14] U.S. Department of Homeland Security, *Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector* (Jan. 6, 2017).

[15] *Id.*

[16] U.S. Department of Homeland Security, *Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector* (Jan. 6, 2017).

[17] Letter from John Kelly, Secretary of the U.S. Department of Homeland Security, to Senator Claire McCaskill, Ranking Member of the U.S. Senate Committee on Homeland Security and Governmental Affairs (Jun. 13, 2017).

[18] *Id.* at answer 7.

healthcare and public health, information technology, nuclear reactors, material, waste, transportation systems, and water and wastewater systems sectors.[19]

The Department has confirmed: "There are no plans to make any changes to the designation of election infrastructure as a critical infrastructure subsector."[20]

A. Covered Assets

The Department informed the Ranking Member that in order to address risks "holistically," it defines election infrastructure as "the key parts of the assets, systems, and networks most critical to the security and resilience of the election process, both physical locations and information and communication technology."[21] DHS details that the definition covers "at least the information, capabilities, physical assets, and technologies which enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections."[22]

B. Assistance Provided

DHS informed the Ranking Member that the prioritized assistance it can provide includes "cybersecurity services," as well as "threat intelligence, risk assessments, training, and best practices related to physical threats."[23] In advance of the 2016 election, DHS offered cybersecurity services to all state and local government election officials upon request. DHS explained:

> Subject to the availability of its resources and at no cost to state and local governments, DHS can furnish voluntary assessments, services, and technical assistance to assist election officials in informing their decision making and election administration processes, if requested by those officials.[24]

One such service provided by DHS is cyber hygiene assessments. These technical assessments consist of configuration error and vulnerability scanning, which are conducted remotely on a recurring weekly basis.[25] According to DHS, these assessments can provide "an

---

[19] *Id.* at answer 7.

[20] *Id.* at answer 7.

[21] *Id.* at answer 3.

[22] *Id.* at answer 3.

[23] *Id.* at answer 4.

[24] *Id.* at answer 4.

[25] *Id.* at answer 1. *See also* U.S. Department of Homeland Security and the Office of the Director of National Intelligence, *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security* (Oct. 7, 2016) (https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national).

objective view of an agency's public security posture" and "reduced exposure to known threats."[26] Note that voting machines are excluded from cyber hygiene assessments.[27] DHS asserts voting machines and vote tallying systems "should not have active connections to the internet during the voting process, and are rarely, if ever connected to the internet at all."[28]

DHS also provides risk and vulnerability assessments (RVA), a no-cost service that includes penetration testing, social engineering, wireless discovery and identification, and scanning of databases and operating systems scanning.[29] These RVAs constitute an "[i]n-depth, onsite assessments of internal and external networks."[30] DHS offers recommendations on remediating any issues that are identified.[31]

DHS shares technical information with thousands of state and local election officials including cyber threat indicators, analytic reports, interagency guidance, and best practices on election infrastructure security.[32] DHS also works closely with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide information and technical assistance to state and local governments.[33]

DHS is not responsible, however, for risk management, procurement, and the administration of the elections process.[34] State and local governments are the owners and operators of election infrastructure and the critical infrastructure designation has no impact on state and local control over election administration.[35]

---

[26] U.S. Department of Homeland Security, *DHS Cybersecurity: Services for State and Local Officials,* at 7 (Feb. 2017).

[27] Letter from John Kelly, Secretary of the U.S. Department of Homeland Security, to Senator Claire McCaskill, Ranking Member of the U.S. Senate Committee on Homeland Security and Governmental Affairs (Jun. 13, 2017) at answer 1.

[28] *Id.* at answer 10.

[29] *Id.* at answer 1.

[30] U.S. Department of Homeland Security, *DHS Cybersecurity: Services for State and Local Officials,* at 8 (Feb. 2017).

[31] Letter from John Kelly, Secretary of the U.S. Department of Homeland Security, to Senator Claire McCaskill, Ranking Member of the U.S. Senate Committee on Homeland Security and Governmental Affairs (Jun. 13, 2017) at answer 5.

[32] *Id.* at answer 1.

[33] *Id.* at answer 1. The Department adds: "All state and local election officials are or could be receiving direct or indirect cybersecurity assistance from MS-ISAC, if requested." *Id.* at answer 1.

[34] *Id.* at answer 4.

[35] *Id.* at answer 4.

DHS asserts that the critical infrastructure designation "should allow for more tailored and useful information sharing."[36] The Department has identified that the designation will facilitate creating a sector coordinating council focused on the security and resilience of election infrastructure; convening meetings with election officials and private vendors by leveraging the Critical Infrastructure Partnership Advisory Council framework; and protecting voluntary information sharing from disclosure in response to Freedom of Information Act requests, use in civil litigation, and regulatory use.[37]

The designation also enables DHS to provide security clearances to election officials if necessary. According to DHS, "[e]lection officials could be briefed on relevant classified intelligence and leverage that to secure their systems in a manner more informed of the threats they face."[38]

C. Participation

DHS informed the Ranking Member that by the date of the 2016 election, 33 state election offices and 36 local election offices requested and received cyber hygiene assessments of their Internet-facing election infrastructure.[39] One state requested and received a "more in-depth risk and vulnerability assessment of their election infrastructure."[40] DHS further explained:

> This suite of services – also no-cost and voluntary – includes penetration testing, social engineering, wireless access discovery and identification, as well as database and operating system scanning.

DHS noted that since the 2016 election, "several" additional stakeholders have requested this in-depth suite of services.[41] DHS further reports that since the critical infrastructure designation on January 6, 2017, two states and six local governments requested to begin cyber hygiene scanning. DHS also received one request for the risk and vulnerability assessment service.[42] One state has since ended its cyber hygiene service agreement with DHS.[43]

---

[36] *Id.* at answer 8.

[37] *Id.* at answer 8.

[38] U.S. Department of Homeland Security, *DHS Cybersecurity: Services for State and Local Officials*, at 21 (Feb. 2017).

[39] *Id.* at answer 1.

[40] *Id.* at answer 1.

[41] *Id.* at answer 1.

[42] *Id.* at answer 1.

[43] *Id.* at answer 1.

D. Remediation of Vulnerabilities

As described above, the owners and operators of election infrastructure – the state, local, tribal, and territorial governments that administer the elections process – are responsible for risk management, procurement, and other decisions related to election administration.[44] If DHS identifies vulnerabilities, DHS will offer recommendations on remediating the issues.[45] The Department explained to the Ranking Member:

> [T]he decisions of what risks and vulnerabilities are deemed acceptable is entirely the responsibility of the state or local government, as are the costs to remediate the vulnerabilities and configuration errors they deem to be unacceptable.[46]

Following a request to DHS for its assistance, technical assistance services will be provided by the agency to state and local governments at no cost; however, the state or local government is responsible for paying for the cost of remediation.[47]

III. ADDITIONAL INFORMATION

A. DHS Seeks No Additional Resources

The Department acknowledges that election capabilities are "becoming increasingly dependent on information and communications technology" and that "election officials are assuming greater responsibility for the cybersecurity of these systems."[48] Despite this acknowledgement, DHS declined to request additional personnel, resources, or authorities in response to questions posed by the Ranking Member inquiring if DHS anticipates needing additional resources to fulfill its responsibilities associated with the critical infrastructure designation.[49]

DHS provides local, in-person support through a workforce consisting of eight cyber security advisors and approximately 100 protective security advisors across the country.[50] These regionally-located DHS personnel "provide immediate and sustained assistance, coordination,

---

[44] *Id.* at answer 4.

[45] *Id.* at answer 5.

[46] *Id.* at answer 5.

[47] *Id.* at answer 5.

[48] U.S. Department of Homeland Security, *DHS Cybersecurity: Services for State and Local Officials,* at p. 6 (Feb. 2017).

[49] Letter from John Kelly, U.S. Department of Homeland Security, to Senator Claire McCaskill, Ranking Member of the U.S. Senate Committee on Homeland Security and Governmental Affairs (Jun. 13, 2017) at answer 9.

[50] U.S. Department of Homeland Security, *DHS Cybersecurity: Services for State and Local Officials,* at p. 14 (Feb. 2017).

and outreach to prepare and protect from cyber and physical threats" to election infrastructure.[51] The Department informed the Ranking Member that it "has been utilizing existing personnel, resources, and authorities" and intends to "prioritize assistance using limited existing personnel, resources and authorities."[52]

B. Targeting of Voting Systems

The ODNI report released in January 2017 on Russia's activities and intentions stated: "DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying."[53] In response to questions posed by the Ranking Member, DHS responded:

> DHS, in coordination with partners from the Intelligence Community, federal law enforcement, and MS-ISAC, observed Russian cyber actors attempting to access voter registration databases prior to the 2016 elections. Voter registration databases are used by states to register new voters and maintain their voter rolls. Voter registration databases – distinct from voting systems – are not involved in vote tallying.
>
> There are no indications nor observed evidence of Russian actors using cyber or physical means to target voting systems, which include voting machines (the electronic machines used by voters to cast ballots) and vote tallying systems (the electronic machines used by election officials to count and tally marked ballots). These voting systems should not have active connections to the internet during the voting process, and are rarely, if ever connected to the internet at all. Thus, they are more difficult for an adversary to access and affect remotely; however, the possibility exists that an adversary could target voting systems through close-access operations or a compromise of the supply chain.
>
> Based on the observed threat, DHS focused its efforts on providing election officials with information to protect their internet-connected election infrastructure, such as voter registration databases, election websites that provided information for voters on where to find their polling places, and election night reporting systems.[54]

###

[51] *Id.* at pp. 14, 15.

[52] Letter from John Kelly, U.S. Department of Homeland Security, to Senator Claire McCaskill, Ranking Member of the U.S. Senate Committee on Homeland Security and Governmental Affairs (Jun. 13, 2017) at answer 9.

[53] Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent US Elections* (ICA 2017-01D) (Jan. 6, 2017).

[54] Letter from John Kelly, U.S. Department of Homeland Security, to Senator Claire McCaskill, Ranking Member of the U.S. Senate Committee on Homeland Security and Governmental Affairs (Jun. 13, 2017) at answer 10.