November 29, 2017

Susan Hennessey,
Written Statement for the House Committee on Oversight and Government Reform:
Subcommittees on Information Technology and Intergovernmental Affairs

Cybersecurity of Voting Machines

Thank you to Chairman Hurd and Ranking Member Kelly, to Chairman Palmer and Ranking Member Butler Demings, and to the distinguished members for the opportunity to speak to you today.

My name is Susan Hennessey and I am Fellow of National Security Law in Governance Studies at the Brookings Institution and the Executive Editor of Lawfare. My research at Brookings focuses in particular on the law and policy governing cybersecurity and surveillance. Prior to joining Brookings, I served as an attorney in the Office of General Counsel for the National Security Agency from 2013 to 2015. My comments here today reflect only my personal views and not those of my current or prior employer.

I want to begin by noting the extraordinary fact that a full year after the last presidential election, there is still enduring attention—among the public, in academia, in the executive branch, and on Capitol Hill—to the issue of election security. This moment presents a remarkable opportunity to take long-overdue steps toward securing federal and state elections.

Today, I hope to map some of the current landscape, both with respect to the nature of the foreign threat, domestic considerations, and possible solutions. Broadly, I want to suggest that Congress work in concert with the executive branch to:

- *Develop a national strategy for securing elections.*
- *Provide federal resources in the form of funding, support, and best practices.*
- *Regulate election-technology vendors.*
- *Lead the development of international norms against election interference.*
- *Renew and sustain political commitment to the issue of election security.*

Before turning to those recommendations, however, it may be useful to review some necessary background.

Defining the “Election Security” Threat

First, how should we understand the election-security threat? As demonstrated by the 2016 U.S. presidential election, the pertinent security issues are immensely complex and wide-ranging. In order to develop a sensible framework, we must disentangle pure election-security issues from broader information operations or covert influence campaigns.

Information operations certainly impact the broader context in which elections occur—including the process of public debate and decision-making as we exercise the fundamental democratic choice. The threat of disinformation campaigns in elections is extremely high, it has materialized in the past, and it will persist in the future. However, for this committee's purposes, that issue should be viewed as a distinct challenge with its own set of available solutions, some of which may come into tension with core American values such as freedom of speech.

The matter currently before this body is more easily defined, though no less difficult and pernicious: the threat to election infrastructure and "voting systems" related to the management and administration of elections. Election infrastructure should be understood to include voter-registration systems, voter check-in systems (also known as poll books), voting terminals, central tabulation and election-night reporting systems, as well as post-election auditing systems. A more difficult question is which, if any, systems used by campaigns, parties, and candidates should also be considered part of election infrastructure.

Understanding the Nature of the Threat

Other experts before the committee today will discuss the technical threats to voting machines and systems. I believe, in context, a fair layperson characterization of that threat is to say that actually changing vote tallies is not a technical impossibility, but it is extremely difficult to do so on the scale necessary to predictably change the outcome of a statewide or national election. The most probable actors with both the incentives and technical capacity to carry out sophisticated attacks are foreign governments, which would need to evade not only forensic detection, but also detection by the United States and allied intelligence communities in order to be successful. As we've seen following the 2016 election, that is an exceptionally difficult task.

Unfortunately, U.S. foreign adversaries' intentions are not merely to change outcomes, but rather a more achievable aim: to undermine confidence. If our adversaries can successfully shake the confidence of the American people in their government, in their processes and institutions, and in the selection of their leaders, then that is a successful assault on liberal democracy. That is far easier to achieve than predictably changing election outcomes. To do so, a malicious actor needs only to penetrate systems such that experts and election officials can no longer express sufficient certainty in the integrity of a system or result.

The timeline of the 2016 U.S. election interference and response demonstrates the importance of public confidence in voting systems. The prior administration did not publicly comment on or confirm early reports of Russian attempts to influence the U.S. election. Despite detailed public accounts as early as June 2016, the administration waited until October 2016 to issue its first formal attribution. The administration released its statement only after media reports that election systems in up to twenty-one states had been targeted and the statement had the clear purpose of reassuring the American public that voting systems remained secure.[1] This is a good illustration of how such activity—in this case described as the "scanning and probing of [state] election-related systems" but not successful penetrations—can force the government to respond publicly, even where it does not suspect impactful interference has occurred.

Other methods to undermine confidence might include disrupting the election process through denial-of-service attacks, interfering with voter registration, manipulating voting interfaces to generate bias, or compromising audit trails.

Information operations may similarly target public confidence in elections. Indeed, many of the information operations that occurred in 2015 and 2016 were aimed at creating the social conditions in which delegitimizing U.S. election results might be most fruitful. The Intelligence Community Assessment of Russian Activities and Intentions in Recent U.S. Elections notes that Russian social media bots had prepared a #DemocracyRIP hashtag campaign to call into question the legitimacy of the election had it been decided for Secretary Clinton instead of President Trump.[2] While it is important to acknowledge the interactions between the two, it remains useful to distinguish to the extent possible information operations like these from election-security issues.

If the goal of threats to election infrastructure is to undermine confidence, rather than to change outcomes, the importance of careful messaging becomes clear. The manner in which we discuss vulnerabilities to election systems could inadvertently achieve our adversaries' goals. If the American people receive the message that voting systems are not secure and cannot be secured, or that there is reason to question the reliability of

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

[2] "Assessing Russian Activities and Intentions in Recent US Elections." *Office of the Director of National Intelligence* at 12, Jan. 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf

election results, that risks undermining confidence in the electoral system. The appropriate response is not to ignore the existence of genuine problems, but instead to exercise caution in public messaging.

Surveying Recent Threats

It is important to note the range of objectives and actors in the space. The lion's share of attention over the past year has been on Russia, but any number of U.S. adversaries, including China, North Korea, and Iran possess the capabilities and interests to be of genuine concern. This means that enduring solutions cannot be Russia-specific.

Below are examples of specifically Russian-backed election interference, not offered to minimize other threats, but in order to illustrate the range of a single actor on a global scale and to situate the 2016 U.S. election interference in a broader context.

Ukraine 2014

In May 2014, four days before the scheduled national election, hackers associated with the Ukrainian-based Cyber Berkut group infiltrated computers at Ukraine's Central Election Commission and destroyed files essential to vote-counting.[3] Two days after the breach, the Ukrainian government said the system was repaired. On the morning of the poll, however, websites sending vote counts to the commission were hit with a denial-of-service attack later attributed to Cyber Berkut, delaying the vote count by several hours.[4] Following the election, government officials revealed that on the night the vote tally was announced, experts discovered malware in the commission's computers that would have incorrectly called the election for far-right leader Dmytro Yarosh with 37 percent of the vote and Petro Poroshenko with 29 percent. The government removed the malware before the commission released the official projections, which accurately showed Poroshenko to win with a majority of the vote, and Yarosh to win just one percent.[5] Notably, a Russian news outlet reported the results that the malware would have projected.[6]

Germany 2015

[3] "Authorities: Hackers foiled in bid to rig Ukraine presidential election results." *Kyiv Post*, May 25, 2014. https://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html

[4] "Ukraine election narrowly avoided 'wanton destruction' from hackers." *Christian Science Monitor*, June 17, 2014. https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

[5] *Id.*

[6] *Id.*

In 2015, the German parliament was hacked by the group known as APT28 or Sofacy[7]—the same Kremlin-linked group what would later target the U.S. Democratic National Committee and other groups during the 2016 U.S. election. The attack was designed to install malware to give intruders permanent access to the computers of members and staff and involved the theft of unknown amounts of data. The attack persisted for three weeks and included monitoring member and staff communications before it was detected. Because precisely what was stolen remains unclear, fears surfaced prior to the 2017 German elections that damaging information might be released in order to compromise or influence that process.[8]

Montenegro 2016

During the October 16, 2016, Montenegrin parliamentary elections, multiple media and government websites—including the website of Montenegro's top nongovernmental election observer[9] and sites affiliated with the governing Democratic Party of Socialists, which campaigned on further alignment with NATO—were targets of denial-of-service attacks. Despite allegations of Russian involvement, the Kremlin denied any connection.[10] In April 2017, the week that President Trump signed ratification papers officiating Montenegro's entrance into NATO, the U.S. government said there were "credible reports" that Russia tried to interfere with Montenegro's elections.[11]

France 2017

Two days before the second round of voting in France's 2017 presidential election, then-candidate Emmanuel Macron's *En Marche* party released a statement saying it was "the victim of a massive, coordinated act of hacking" as hackers released nine gigabytes of stolen emails from the left-leaning candidate's campaign.[12] Trend Micro, a

[7] "Russia 'was behind German parliament hack.'" *BBC News*, May 13, 2016. http://www.bbc.com/news/technology-36284447

[8] "Germany fears Russia stole information to disrupt election." *Politico*, May 6, 2017. https://www.politico.eu/article/hacked-information-bomb-under-germanys-election/

[9] "White House Readies to Fight Election Day Cyber Mayhem." *NBC News*, Nov. 3, 2016 https://www.nbcnews.com/news/us-news/white-house-readies-fight-election-day-cyber-mayhem-n677636

[10] *Id.*

[11] "U.S. says 'credible reports' Russia tried to interfere with Montenegro elections." *Reuters*, April 12, 2017. http://www.reuters.com/article/us-usa-trump-montenegro/u-s-says-credible-reports-russia-tried-to-interfere-with-montenegro-elections-idUSKBN17E22F

[12] "Macron Campaign Says It Was Target of 'Massive' Hacking Attack." *The New York Times,* May 5, 2017. https://www.nytimes.com/2017/05/05/world/europe/france-macron-hacking.html?_r=0

security firm, had said in April that a known group of hackers, which it called Pawn Storm, had targeted Macron's campaign in a phishing attack.[13] U.S. intelligence agencies and cybersecurity firms said that Pawn Storm was the group also known as Fancy Bear and APT 28,[14] an arm of Russian intelligence and one of two Russian government–linked entities that targeted the Democratic National Committee during the 2016 U.S. election.

These examples are non-exhaustive of the suspected Russian activity related to foreign elections over the past three years. They are intended to illustrate the breadth of activity of a single, committed nation state. They demonstrate that the election-security challenge is vast and that an effective policy response will require a range of technical, as well as domestic and international policy solutions.

Domestic Policy Considerations

To develop solutions, Congress must account for the domestic constitutional and political landscape. In the United States, state and local governments, rather than the federal government, primarily administer elections. The Elections Clause of the Constitution vests the states with regulatory power over elections, but allows Congress to "at any time by Law make or alter such Regulations…."[15]

Notwithstanding the explicit override authority of Congress, perceived federal overreach is likely to meet strong resistance from states on political and policy grounds, if not necessarily constitutional objections. In 2016, at least one state declined even voluntary assistance from the Department of Homeland Security and went on to erroneously accuse DHS of improperly breaching state election systems.[16] In recognition of privacy sensitivities, another state's Secretary of State responded to requests from the Presidential Advisory Commission on Election Integrity for voter records by telling the commission to "go jump in the Gulf of Mexico."[17] Thus, voluntary efforts—those designed to be more carrot than stick—are more likely to be successful in the short-term.

[13] "Russia-linked hackers targeting French election, security firm says." *CBS News*, April 25, 2017. https://www.cbsnews.com/news/russia-hacked-french-election-trend-micro-report-fancy-bear-pawn-storm/

[14] *Id.*

[15] US Constitution, Art. I, Sect. 4, Clause I.

[16] "Correspondence Between DHS and U.S. Representative Jason Chaffetz." *Department of Homeland Security.* Dec. 8 2016-Feb. 28, 2017. https://www.dhs.gov/sites/default/files/publications/Correspondence%20between%20DHS%20and%20U.S.%20Representative%20Jason%20Chaffetz%20%28R-UT%29.pdf

[17] "Secretary Hosemann's Statement on Request for Voter Roll Information." *Secretary of State of Mississippi.* June 30, 2017. http://www.sos.ms.gov/About/Pages/Press-Release.aspx?pr=800

States are under-resourced in funding, training, expertise, equipment, and auditing capabilities. For example, according to the Brennan Center for Justice, forty-one states have voting machines that are more than ten years old. And while election officials in twenty-nine states express a desire to replace voting machines, 80 percent report a lack of secure funding.[18] There are also substantial variations not only between states, but also in some instances from county to county. Under these conditions, states cannot reasonably be expected to withstand sophisticated nation-state attacks—to not only counter known threats, but also to anticipate unknown threats. While respecting states' rights, the federal government must assume responsibility for providing necessary support.

The federal designation of election systems as critical infrastructure is a necessary but insufficient step. Former DHS Secretary Jeh Johnson designated election infrastructure as a critical infrastructure sub-sector of the existing government facilities sector on January 6, 2017.[19] This designation allows DHS to better prioritize services and support and to share intelligence information, but it does not supplement any regulatory authority.

Moving Toward Solutions

There are no obvious or easy solutions here. However, there are clearly areas where congressional action could lead to demonstrable gains. Below are recommended areas for congressional attention.

- *Develop a national strategy for securing elections.*

The United States should develop a national strategy to secure elections aimed at protecting systems, deterring bad actors, and bolstering public confidence.[20] This approach should empower state and local authorities and focus on defense-in-depth and resiliency by design. A successful strategy must not only work to prevent attacks, but also to implement systems to rapidly restore confidence in the event of an attack.

[18] "American Voting Machines at Risk." *The Brennan Center for Justice.* June 12, 2017. http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_180930.pdf

[19] Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, Jan. 6, 2017. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[20] For additional analysis, see David P. Fidler, Presentation for the National Academy of Sciences Committee on the Future of Voting, available at https://livestream.com/accounts/7036396/events/7752647.

This strategy must balance security with other important objectives, such as preserving and promoting voter access.

A strategy that sets neutral standards and thresholds well in advance of the next national election can help avoid politicization. The 2016 election demonstrated how the fear of even a perception of political motivation can inhibit the executive branch from responding to known threats. Setting standards for baseline security, recount and auditing thresholds, and deterrent response options will strengthen public confidence and avoid excessive inhibition where nation-state attribution or response is necessary.

- *Provide federal resources in the form of funding, support, and best practices.*

Additional federal resources designed to improve election security should be made available to states on a voluntary basis. Currently, the Senate has offered amendments to the National Defense Authorization Act that would take this approach.[21] These resources should be contingent on implementing security measures aimed at long-term sustainability. Additional federal support should be conditioned on meeting federally developed best practices for election administration and security. Best practices would include the use of paper ballots, routine audits, training, and penetration testing.

- *Regulate election-technology vendors.*

Both federal and state governments must better regulate the commercial industry surrounding elections. Currently, this is a limited and proprietary market that too often leaves states with insufficient power to dictate security standards. In addition to setting standards for secure design, manufacturing, and storage of voting systems, the government must mandate ongoing processes such as routine penetration testing. Election technology vendors should also be required to promptly report any discovered vulnerabilities to state election officials and the Department of Homeland Security. At the same time, Congress must eliminate the legal barriers to independent vulnerability research contained in the 1998 Digital Millennium Copyright Act and the Computer Fraud and Abuse Act.

- *Lead the development of international norms against election interference.*

The United States should lead to establish international norms against election interference. Such norms can differentiate between espionage—which is an accepted

[21] Protecting Electoral Infrastructure–Klobuchar/Graham and the NDAA, *Lawfare*, Sept. 5, 2017. https://www.lawfareblog.com/protecting-electoral-infrastructure%E2%80%93klobuchargraham-and-ndaa

international practice—and active measures or covert influence operations. There are instructive prior examples, such as agreements on norms against commercial espionage. But heeding this suggestion means that the United States must embrace a policy of self-restraint in order to develop the necessary international consensus. Some have pointed to past allegations of U.S. activity in foreign elections. Rather than focus on the distinct factual situations in which such activity might have occurred, effective policy should clearly articulate which activities the United States and international community deem unacceptable and include assurances that the U.S. will not itself engage in such behavior.

- *Renew and sustain political commitment to the issue of election security.*

Finally, Congress, as our primary elective body, must recalibrate the political climate surrounding election security if progress is to be made. It must reestablish norms that have been broken, and demand that candidates behave more responsibly in discussing elections moving forward. If we persist in describing elections as “rigged,” in tolerating the suggestion that a candidate is not bound to accept an election outcome if he or she does not win, and in demeaning the conclusions of the U.S. and allied intelligence communities, then we ourselves will create the conditions for a crisis of public confidence. Opponents of liberal democracies will not hesitate to exploit that opportunity.

Thank you again for the opportunity to address these subcommittees. I look forward to taking members’ questions on this important national security issue.