Statement of Jake Braun
Executive Director, University of Chicago Harris Cyber Policy Initiative

Committee on Homeland Security
"Defending Our Democracy: Building Partnerships to Protect America's Elections"
February 12, 2019

Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee, thank you for the opportunity to speak to you today on this important issue.

I would also like to thank my co-panelists, Secretary Padilla and Noah Praetz. They have led the nation in securing their elections and have become a model for other election officials around the country to follow.

My name is Jake Braun and I am Executive Director for the Cyber Policy Initiative at the University of Chicago Harris School of Public Policy.

I am also co-founder of the DEF CON Voting Machine Hacking Village. DEF CON is the largest hacker conference in the world and the Voting Village is the only public, third-party inspection of voting equipment in the world, that we are aware of.

Moreover, for the last two years, I have worked with leaders in the national security establishment to release an annual report on the national security implications of our findings at DEF CON. The reports have won multiple awards and our efforts have been hailed by people as diverse as President Trump's former White House Cyber Czar, Rob Joyce; then-Chairman of the Cyber Caucus, Congressman Will Hurd; and Congresswoman Jackie Speier; as well as a bipartisan group of senators from the Senate Select Committee on Intelligence, led by Senators Harris and Lankford.

The main question relevant for this committee is whether any of our findings are useful to the legislation you are now considering. The answer, in my estimation, is emphatically yes.

To that end, I have one overarching finding I want to highlight as well as a few key vulnerabilities which clarify the importance of the finding. Finally, I would humbly like to make a couple recommendations as to how these problems can be addressed.

The overarching finding is that attacks on our election infrastructure are NOT solely an election administration nuisance but rather a national security threat. Time and again this conclusion manifests itself in our research. This threat is not about how to eradicate hanging chads. This is about our national security apparatus marshalling its resources to do what our nation expects it to do, which is protect our country from existential threats to the United States. A county clerk or secretary of state is not equipped to defend our democracy from nation state hackers. These nation state adversaries may attempt to change vote totals or they may simply try and erode our confidence in the integrity of American elections. Either way, this is a national security threat and thus Congress must act.

Let me give you a few examples of specific key findings that draw us to the conclusion that this is a national security threat:

1. The voting machine supply chain is global and parts are made in nations unfriendly to the United States, like China. If an adversary were to infect the firmware made at a plant in China or elsewhere, which we know has happened with other products, whole classes of voting machines could be hacked all at once on Election Day from the Kremlin. No election clerk or secretary of state alone can defend against these global supply chain issues. This is a national security threat and thus Congress must act.

2. Second, we have highlighted well-known vulnerabilities in websites. The global leader on website security, The Open Web Application Security Project (OWASP), and the 2018 report by the Senate Select Committee on Intelligence have highlighted similar threats to election websites. The bottom line is no one can defend a website from a determined nation-state actor. Just ask the top 25 banks in the country who collectively spend billions on security but failed to stop members of the Iranian Revolutionary Guard from attacking their websites consistently over the course of two years. Further, since 2016, the media has reported successful attacks on election websites in the U.S by Russia. Russia also executed an attack against Ukraine's Central Election Commission website in 2014, rigging the website to announce the Russian-supported candidate won. Ukrainian officials detected the breach before the election results went live, but Russian media still erroneously named their candidate the winner. In U.S. states where there are no paper audits possible, hacking a website may be all that's necessary to cast doubt on an election's integrity. Moreover, no clerk or secretary of state alone can defend themselves against a multi-layered cyber and media campaign to cast doubt on the integrity of a national election. Rather, this is a national security threat and thus Congress must act.

3. Finally, perhaps the most disconcerting "flaw" we found is that vendors don't fix vulnerabilities when they are disclosed to them. A significant flaw with the M650 machine, which was used in 23 states as of 2018, was disclosed to the vendor in 2007. However, to our knowledge the vendor neither told its customers about the flaw nor did they fix the flaw at the time it was disclosed. Nor did they fix it after the 2016 elections when they supposedly started taking security much more seriously. Nor did they fix it, to our knowledge, after we pointed it out again at DEF CON in 2018. To be clear, this attack would allow an attacker, through a remote hack that could be carried out from abroad, to jump the so-called "air gap" and hack into a voting tabulator processing ballots for key counties in battleground states. This attack could flip the Electoral College and determine the outcome of a presidential election. Obviously no clerk or secretary of state alone can defend against adversaries who can change large number of votes without needing physical or network access to the machines." Clearly, this is a national security threat and thus Congress must act.

One might think these attacks sound pretty hard to carry out. However, most of these attacks and dozens of others we found were carried out by generalists with no specialized training on election equipment or previous knowledge of the machines or networks.

Some have claimed that the setting at DEF CON does not represent a real election environment, thus diminishing the utility of our findings. However, as said at the outset, DEF CON is the only

public, 3rd party inspection of election equipment, so it's the best we have for now. Further, as former White House Cyber Czar Rob Joyce, said, "We know our adversaries have a room just like the one at DEF CON." By which he meant that our adversaries are researching all the voting equipment we have and more because they don't have to get the machines legally, like we do at DEF CON. However, they aren't doing the research three days a year, they are doing it 365 days a year. They also don't disclose the vulnerabilities they find, like we do. Yet they are looking for the same flaws we are: Hacks that are quick, remote, and scalable.

So what can be done about these problems?

First, I would encourage you all to study the recommendations of a new report on election security from the National Academies of Sciences, Engineering, and Medicine. Their recommendations are comprehensive and sound.

Second, pass this bill. The measures in the H.R. 1 proposed legislation provide for auditable paper trails and local implementation of at least the top five of the 20 Critical Security Controls, as well as funding for cyber assessments and remediation. Congress must support state and local administrators' efforts by providing funding and assistance to implement cyber best practices that reduce America's vulnerability to these clear threats to our election infrastructure.

Finally, the election industry desperately needs funding for R&D to build voting equipment that can stand up to these modern threats. The current equipment is essentially unsecurable. The vendors will never have the enough money to fund the R&D necessary to develop equipment that can defend against nation-state attackers. H.R. 1 provides R&D funding for voting technology of the future, and I would strongly encourage the committee to keep that funding in whatever version hopefully passes.

Again, not solely an election administration nuisance but rather a national security threat. Thus Congress needs to act and fund a solution. I thank you for your efforts to pass this critically important legislation.