Written Testimony of
Andrew J. Grotto
Stanford University

Before a Joint Informational Hearing of the California Legislature on
"Cybersecurity and California Elections"
Assembly Committee on Elections & Redistricting and
Senate Committee on Elections & Constitutional Amendments

March 7, 2018

Thank you for that introduction, Chairman Stern, and thank you Chairman Berman for asking me to join you this morning. Thank you distinguished legislators for your time and attention. Preserving the integrity of our electoral infrastructure is vital to our democracy, and I am grateful as an American, and as a newly re-registered California voter, for your focus on this topic.

Normally, interest in our electoral infrastructure peaks in even numbered years, only to fade in odd numbered years as our attention as a nation is drawn to other priorities. This wasn't the case in 2017, however. As a result of important work done by election professionals, civil society, and other stakeholders throughout 2017 on cybersecurity challenges facing our electoral infrastructure, I think the contours of what constitutes cybersecurity best practices for electoral infrastructure are beginning to come into focus. That wasn't the case in 2016.

In light of this positive development, I believe the key cybersecurity questions for the 2018 election cycle revolve primarily around implementation and incident response, including public communications: Do state and local election officials have sufficient management, staffing, and budget resources to implement best practices? And, since incidents can still occur even when best practices are implemented, are contingency plans calibrated for the challenges ahead?

You received a considerable amount of information this morning from our state's election professionals about their cognizance of cybersecurity best practices and their readiness to conduct a cybersecure election this fall. The focus was understandably on what these election professionals are doing to ensure that election outcomes in November reflect the will of the people of California. What I want to primarily emphasize in my prepared remarks is the equally vital role that candidates for public office must play in upholding the public's confidence in our electoral infrastructure. You too are at the front lines of combating cyber risks to our electoral infrastructure. I will provide some perspective and some recommendations on how candidates for office can contribute to the fight.

For context, I'll begin with a brief reminder of the threat we are facing as a nation. In January 2017, the U.S. intelligence community issued an unclassified report on Russia's interference in our election process. I'll quote:

"We assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election, the consistent goals of which were to undermine public faith in the U.S. democratic process..."

And in January of 2017, CIA Director Mike Pompeo said that he expected Russia to interfere in the 2018 election as part of the Kremlin's strategy to "undermine Western democracy."

How will the Kremlin attempt to do this? Through so-called "active measures." That's the English term for Russia's doctrine of information warfare that combines hacking with information operations and other malicious covert and overt actions. I think we need to be prepared for the Kremlin to intensify its use of active measures in 2018 to hack our election infrastructure and feed corrosive narratives about election fraud, about violence at polling places, about long lines and other irregularities before, during and even after election day.

Notice how the success of the Kremlin's strategy doesn't necessarily depend on any actual hacks or irregularities. The Kremlin wins by sowing doubt, which it can accomplish by making it hard for us to discern ground truth, to separate fact from disinformation. Doubt is corrosive to faith in the U.S. democratic process.

And that observation takes me to the first of the three recommendations that I want to leave you with today.

Given this threat, it is vital that our election professionals practice their cybersecurity incident response plans before November, through scenario planning exercises. Contingency planning is already part of the DNA of our election professionals, but it is important that their incident response planning be conducted with two goals in mind: first, and obviously, to enable the Secretary of State to certify that election results reflect the will of the people of California; second, and less obviously but no less important, that the conduct of the response supports public confidence in our electoral institutions. A Secretary of State could certify an election, but that does not necessarily guarantee the public's overall confidence in our institutions.

These exercises don't need to be elaborate affairs, but they do need to be robust enough to help our election professionals test both their technical response plans and their public affairs strategy. The exercises will help them identify and resolve problems, and in general, enable them to build some muscle memory around how to respond to cybersecurity incidents, regardless of perpetrator, including active measures from Moscow.

That's my first recommendation.

My second recommendation is that those of you running for reelection develop your own response plans to purported cybersecurity incidents. If a Twitter meme about hacked E-Pollbooks in your district starts to develop on election day, or stories about violent protests at a polling place show up in Facebook news feeds, how will you and your team respond? Who should your team call in the first instance for ground truth? What due diligence is appropriate before making a statement? I've spent most of my career at the intersection of policy and politics, so I fully appreciate the merciless news cycle and how intense campaigns can be. That said, don't allow you or your campaign to be coopted by the Kremlin as part of an active measures campaign. Develop incident response plans in advance, ideally with appropriate coordination and consultation with election officials and other stakeholders, and then practice them. And by the way, demand that your opponents do the same.

But don't stop there. Political campaigns are vital electoral infrastructure as well. Different, of course, than the infrastructure administered by state and local governments. But important nonetheless. Campaigns must also implement cybersecurity best practices to protect their systems and data from compromise. And it starts with leadership establishing a culture of security, and building from there.

I want to close with a third recommendation on a topic that's a bit more future oriented, but I think action must start now.

We have already seen the toxic impact that fake news, in the form of doctored photos and made-up text, can have on our civic discourse. As my Stanford colleague Dan Boneh and I document in a forthcoming paper, what's coming next is fake video—so-called "deep fakes" that use machine learning technologies to generate spoofed videos. These videos can depict a person saying and doing whatever the author of the video desires, with potentially breathtaking realism. You may have seen some examples of deep fakes already—they are already impressively persuasive, and soon it will be virtually impossible to distinguish a fake video from a real one.

There are many malicious applications of this technology, but we are especially concerned about its misuse in election campaigns to make it even harder for people to separate fact from fabrication and learn truths about candidates and issues.

Companies such as Facebook and Twitter have a social responsibility to prevent their platforms from being abused to spread malicious deep fakes. We should hold them to a high standard.

But the reality is that there is no technological or regulatory silver bullet to this problem. We must also demand leadership from the men and women who run for office and hold leadership positions in our political institutions. The risk of misuse of this technology in an electoral context is as much a function of what our political leaders consider to be appropriate norms of behavior as it is a function of what the technology can do. Put differently, an exclusive focus on technological tools ignores the key role that candidates and their supporters and allies play in setting, enforcing, and breaking norms of conduct in our political discourse.

Candidates must join in this fight.

For that reason, I believe an essential part of managing the risk that this technology poses to our democracy is for our leaders to establish a clear norm of restraint around this technology, which leads to my third and final recommendation for today: candidates and their formal campaign infrastructure, including the national political parties, should mutually agree to not produce, promote, or otherwise distribute a fake video depicting a person without that person's consent. They should also send a clear message to their allies and proxies that they should not abuse this technology either, and energetically call out groups that defy this norm.

That concludes my prepared remarks. I look forward to your questions.