ELECTION SECURITY: VOTING TECHNOLOGY VULNERABILITIES

Statement of

Neal Kelley

Registrar of Voters, Orange County, California

and

Past President, California Association of Clerks and Election Officials (CACEO);
Past President, National Association of Election Officials;
Past Chair, United States Election Assistance Commission (EAC) Board of Advisors;
Member, EAC Voting Systems Standards Board;
Member, Department of Homeland Security (DHS) Election Security Task Force (Government Coordinating Council);
Member, 2018 National Academy of Sciences, Engineering and Medicine's Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology Committee

before the

The Subcommittee on Investigations & Oversight; and
The Subcommittee on Research & Technology

House Committee on Science, Space, and Technology

U.S. House of Representatives

June 25, 2019

Good afternoon, Chairwoman Sherrill, Chairwoman Stevens, Ranking Member Baird, Ranking Member Norman, and members of the Subcommittee on Investigations & Oversight and the Subcommittee on Research & Technology. My name is Neal Kelley and I am the Chief Election Official, Registrar of Voters for Orange County, California. Thank you for the invitation to speak at this joint hearing to address:

- The key findings of the National Academies of Sciences, Engineering, and Medicine Consensus Study Report, "*Securing the Vote*, *Protecting American Democracy*",[1] specifically as they pertain to the National Institute Standards of Technology (NIST).;
- The best practices used in Orange County, including the use of paper trails with voting machines, electronic pollbooks and risk-limiting audits;
- Barriers states and counties encounter in the pursuit of enhancing election security; and
- How Congress can further assist states and counties with securing election system technologies.

As a member of the National Academies of Sciences, Engineering, and Medicine's Committee on the Future of Voting, I would like to share the key findings of the committee's report, "*Securing the Vote*, *Protecting American Democracy*", as they relate to NIST. I have submitted the Report Highlights for Federal Policy Makers along with my testimony today. I would also like to share the insights I have gained as an election administrator.

[1] For the full report, please see https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy. This report was undertaken with grants to the National Academy of Sciences from the Carnegie Corporation of New York (#G-16-53637) and the William and Flora Hewlett Foundation (#G-2016-5031) and with funds from National Academy of Sciences' W. K. Kellogg Foundation Fund and the National Academies of Sciences, Engineering, and Medicine's Presidents' Circle Fund.

In the two decades following the 2000 Presidential Election, numerous initiatives have been undertaken to improve our election systems. Although progress has been made, old and complex problems persist, and new problems emerge. Aging equipment, the targeting of our election infrastructure by foreign actors, a lack of sustained funding dedicated to election security, inconsistency in the skills and capabilities of elections personnel, and growing expectations that voting should be more accessible and convenient as well as secure complicate the administration of elections in the United States.

Working together, NIST and the Election Assistance Commission (EAC) have made numerous contributions to the improvement of electronic voting systems by providing critical technical expertise. The voluntary voting systems guidelines (VVSG), developed by the EAC in collaboration with NIST, are particularly important. Nevertheless, despite the critical roles that these agencies play in strengthening election infrastructure, the federal government currently provides limited ongoing financial support. While one-time funding has been historically allocated, election cybersecurity is known to be an ongoing challenge that will require ongoing efforts to better understand threats and vulnerabilities and develop strategies and solutions to defend and protect America's election systems.

Our report recommends that the EAC and NIST — the architects, developers, and shepherds of the VVSG — continue the process of refining and improving the VVSG to reflect changes in how elections are administered, to respond to new challenges to

election systems as they occur (i.e., cyberattacks), and to research how new digital technologies can be used by federal, state, and local governments to secure elections. Our report further recommends that a detailed set of cybersecurity best practices for state and local election officials be developed, maintained, and incorporated into election operations and that the VVSG be periodically updated in response to new threats and challenges.

The draft guidelines also require software independence for all voting systems so as to allow for the determination of the correct outcome even if the software does not perform as intended. Our report echoed this principle, recommending that the computers and software used to prepare ballots should be separate from the computers and software used to count and tabulate ballots.

Electronic voting systems that do not produce a human-readable paper ballot of record are of particular concern as the absence of a paper record raises security and verifiability issues. Because of this, our report recommended that all elections should be conducted with human-readable paper ballots. We further recommended that states mandate risk-limiting audits (RLA) prior to the certification of election results.

An RLA is not considered to be a performance audit as it seeks to ensure accuracy that the reported outcome would be the same if all ballots were examined manually and that any different outcome has a high likelihood of being detected and corrected.

In 2018 I chose to implement two RLA pilot programs in both the 2018 Primary and

General Elections in Orange County. These audits identified best practices and allowed us to share lessons learned with other county election officials and policymakers for consideration when developing post-election audit procedures and policies.

The report recommends that use of the Internet, or any network connected to the Internet, for a voter cast a ballot or the return or market ballots should not be permitted. There is no known technology that guarantees the secrecy, verifiability, and security of a marked ballot transmitted over the Internet. No matter how well constructed or prepared, it is impossible to anticipate and prevent all possible attacks through the Internet and we know that there are actors who look for vulnerabilities with the deliberate intention to compromise America's elections.

Voter registration databases are also vulnerable to cyberattacks, whether it is standalone or it is connected to other applications. Presently, election administrators are not required to report any detected compromises or vulnerabilities in voter registration systems. The report recommends that states make it mandatory for election administrators to report these instances when it occurs to the DHS, the EAC, and state officials. In Georgia, more than 6.5 million voter records and other privileged information were exposed due to a server error. The security vulnerability had not been addressed 6 months after it was first reported to authorities, even though it could have been used to manipulate the state's election system. This is exactly the kind of scenario that can be avoided if the proper agencies were notified and had an opportunity to act.

Since voter registration databases are increasingly being integrated with other databases, the report recommends that election administrators routinely evaluate the integrity of voter registration databases and the other databases they are connected to. In Illinois, Russian actors targeted and breached an online voter database in 2016 by exploiting a coding error. For three weeks, they maintained undetected access to the system. Ultimately, personal information was obtained on more than 90,000 voters. Strict standards and funding can be established to prevent the likelihood of similar instances in the future.

As the fifth largest voting jurisdiction of the nearly 9,000 voting jurisdictions in the United States, Orange County is in the fortunate position of being able to allocate resources and staff to support pilot programs and determine best practices for the use of paper audit trails (with voting machines and electronic pollbooks). I am pleased to share what my team and I have practiced and learned over the past 15 years as one of the leading election administration agencies in the country.

On the matter of election security, we remain closely connected to our local fusion center and to Information Sharing and Analysis. In addition, we invite security experts to conduct audits and testing on our systems to identify vulnerabilities and to propose solutions as necessary. When considering potential vendors for professional services, we maintain strict security requirements to ensure vendor integrity.

Starting in 2006, California Elections Code section 19250 required the use of a Voter Verifiable Paper Audit Trail (VVPAT) for any electronic voting machine in California. Although Orange County is in the process of obtaining new voting equipment, we currently use a voting system (Hart InterCivic HVS 6.1) which contains a VVPAT printer, installed by my office, that has been certified for use in California. A VVPAT allows a voter to manually verify that the selections on the ballot reflect their intentions, regardless of whether the ballot is paper or electronic ballot. This is particularly helpful in a recount because the original paper record can be used to verify that the final tally is correct.

Electronic pollbooks must meet high level security requirements to be used in California, and Orange County has placed additional requirements on potential electronic pollbook solutions. Data must be encrypted while in transmission and while at rest. Mobile device management allows advanced remote management of pollbooks and includes the ability to remotely wipe all data from a pollbook if it were to be misplaced or stolen. Additionally, electronic pollbooks are never connected to voting systems. This “air gap” eliminates the capability of affecting voting machines via pollbooks.

As you know, states and counties differ not only in geographic area and population size but also in terms of their access to resources, funding, and information. Yet, the election security challenges that local election officials face have no bearing on the size of their jurisdiction, access to funding and resources, and ability to mitigate or respond to such threats. My office is considered by many to be at the forefront of

election innovation by virtue of its participation in working groups that communicate election security information, its participation in trainings, and its prioritization reviews of all processes and procedures so as to identify and resolve vulnerabilities and be resilient against on-going and expanding threats.

Nevertheless, not every election office has the resources that we have in Orange County. There are hundreds, if not thousands, of election offices where only a handful of dedicated staff are on hand to run their jurisdiction's elections fairly and securely. The lack of personnel in many of these small jurisdictions make it difficult to add additional responsibilities. The magnitude of what is involved in maintaining election security can be overwhelming to any individual seeking to expand their knowledge and remain abreast of the ever-changing field of election security. We must not lose sight of smaller jurisdictions that could benefit greatly from shared resources.

To share the knowledge and experience gained by being at the forefront of election cybersecurity, I released the *2018 Election Security Playbook: Orange County, CA Elections* to provide other local elections officials and the public with an opportunity to understand the role of election systems as critical infrastructure, to share core information security principles, and to identify critical threats and vulnerabilities.

The *Playbook* was reviewed by the Department of Homeland Security, the Election Assistance Commission, and the Federal Bureau of Investigation and it is available to the public in the Orange County Registrar of Voters' website in our Election Library. I have included the Playbook as an appendix to my testimony.

Congress has a unique ability to address issues affecting multiple states. It is incredibly challenging to coordinate resource and knowledge sharing amongst states and local jurisdictions. Congress can greatly assist states and counties with securing election system technologies by assisting in the standardization of information sharing and by providing funding for the digital tools, training, and staff resources necessary to secure our elections. States and local governments are ready to work with Congress to secure our elections, and agencies such as EAC and NIST, if given the opportunity, could build upon their research and standards to support the development of the digital tools necessary to provide election security.

Thank you and I look forward to your questions.