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.

The National Academies' report begins with a discussion of the 2016 Presidential Election, which exposed new technical and operational challenges faced by state and local governments, the federal government, researchers, and the American public. Specifically, the 2016 elections showed that we must become more discerning consumers of information and become more proactive in our efforts to defend our election systems against bad actors who seek out opportunities to infiltrate and undermine the credibility of our election infrastructure. The 2016 Presidential Election made it clear that the federal, state, and local governments must work collaboratively to secure our election infrastructure and that we must discuss the threats to our elections candidly and apolitically.

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.

We must prevent efforts to corrupt our electoral process while continuing to administer elections for an electorate that is increasing in size and complexity. The threats and challenges will continue to grow, and the security of the American elections process will only be achieved through collaboration, cooperation, and the allocation of sufficient resources.

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.

As elections will likely involve the use of even more technology in the future, the committee's report called upon NIST to develop security standards and validation protocols for electronic pollbooks in addition to the standards and verification and validation protocols that the agency has developed for voting systems. The development of such standards is crucial, but limited funds and staff resources make it difficult for NIST to address these and other challenges involved in protecting our election infrastructure. If the challenges currently facing our election systems are ignored, we risk an erosion of confidence in our elections system and in the integrity of our election processes.

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.

VVSG was first adopted in 2005 to increase security requirements for voting systems and it augmented the 2002 Voting System Standards to address advancements in election practices and computer technologies. The next iteration occurred 10 years later in 2015 with the approval of VVSG 1.1, which enabled NIST to create test environments for the proposed changes. Almost immediately following the adoption of VVSG, it was clear that we cannot wait another 10 years for updated voting system guidelines and principles and the EAC and NIST began working on the next iteration, entitled VVSG 2.0. Rather than provide device-specific guidance as previous VVSG versions did, VVSG 2.0 has a new structure to provide high-level principles and guidelines on all functions that are incorporated into a device or devices that make up a voting system. In addition, VVSG 2.0 will include requirements to provide technical details necessary for manufacturers to design devices that meeting the established principles and guidelines and test assertions that allow laboratories to test a voting system against the prescribed requirements.

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.

While many of the discussions related to elections revolve around cybersecurity, continued attention must be paid to modernizing our election systems. Our report recommends that NIST should establish Common Data Formats for auditing, voter registration, and other election systems. Through conformance with such standards, new election systems would be better protected against infiltration attempts.

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 prior to the certification of election results. With current technology, this requires the use of paper ballots. Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible.

Whether required by law or because local officials have independently adopted an audit requirement, most jurisdictions conduct audits after an election. Some audits focus on the processes followed by election officials, which are performance audits, but those do not check for the accuracy of election results. The report specifically recommends states mandate risk-limiting audits (RLA) prior to the certification of election results and all federal and state contests, and for local contests where feasible for that reason. 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. Colorado was the first state in 2018 to conduct RLAs in a statewide election.

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. Although cybersecurity is a never-ending challenge, best practices such as adopting state-of-the-art technologies and best practices more widely and developing new knowledge about cybersecurity will achieve stronger defenses against cyberattacks.

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, it is recommended 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. In California, hackers penetrated state registration databases and gained access to the personal information of a large number of voters and demanded ransom. Election infrastructure should not be at the mercy of hackers motivated by money or a desire to inflict chaos upon the American people. Strict standards and funding can be established to prevent the likelihood of similar instances in the future.

In addition to recommendations directed to the EAC and NIST, our report offers recommendations for the federal government, state governments, and election administrators and calls for research on voting that supports basic, applied, and translational research relevant to the administration, conduct, and performance of elections.

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 Centers such as Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). Information sharing in both directions is tremendously helpful for maintaining awareness of innovative digital tools and security threats or challenges. In addition, we invite security experts to conduct audits and testing on our systems to identify vulnerabilities and to propose solutions as necessary. To increase staff awareness of election security, staff participate in regular table top exercises with government and private partners. Staff are also required to take and pass an annual countywide cybersecurity training. When considering potential vendors for professional services, we maintain strict security requirements to ensure vendor integrity.

In addition, Orange County partnered with DHS on its “See Something, Say Something” campaign to encourage staff, volunteers, and voters to speak up when there is something suspicious. The DHS “See Something, Say Something” campaign logo was prominently displayed in poll worker training manuals, polling place set-up guides, and office materials and the campaign was discussed in in-person trainings that thousands of poll workers participated in.

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.

In 2018 I chose to implement two risk-limiting audit (RLA) pilot programs in both the 2018 Primary and General Elections. 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. While having a legacy voting system does not prohibit an elections agency from conducting a risk-limiting audit, I recommend that voting systems be updated in order to better support risk-limiting audits at a ballot comparison level. This added ability, included only in modern voting systems, allows jurisdictions to provide voters with increased confidence in election outcomes.

Orange County has a long history of supporting the movement toward risk-limiting audits:

- In 2007, Orange County participated in the California Secretary of State's Post-Election Audit Standards Working Group to evaluate the 1% manual tally and other post-election audit models.
- In 2010, Orange County conducted an RLA audit pilot and submitted findings to the EAC.

Orange County specifically conducted RLA pilots in 2018 in advance of being allowed to conduct RLAs in lieu of the currently mandated 1% manual tally starting with the March 2020 Primary Election. Additionally, we partner with academic institutions to review our methodology. We solicit feedback from institutions such as MIT, UC Berkeley, Princeton, and Caltech.

To share our experiences and best practices, I released the *2018 Risk-Limiting Audit Pilot Project Report* in April 2019. This report is available on our website. It includes a glossary of terms and basic outline of RLA procedures to help those new to the concept of an RLA to become familiar with it.

Having served as the Chief Elections Official in Orange County, California for the past 15 years, I have seen the election security landscape change dramatically. In the current landscape, the focus is on developing digital defense strategies against ongoing foreign state sponsored attacks that seek to undermine confidence in our democratic institutions. State and local election officials need broad support to protect America's election infrastructure. As the Academies' report states, "To fully address the challenges inherent in electronic election systems and to prevent foreign interference, federal, state, and local officials must adopt innovative measures to ensure that the results of elections reflect the will of the electorate." The failure to do so will result in unforeseeable and lasting damage to the American public's confidence in elections, which is the underpinning of the democracy we live in and pride ourselves in.

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. Sending staff to trainings or bringing trainings to small or rural voting jurisdictions can be particularly challenging because it reduces the number of staff on hand at the elections office. 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* is the only guide to be published from the perspective of a local election official. It provides scenarios and tips that are relatable to other local election officials seeking to build their election security knowledge and implement basic safeguards to protect election systems.

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. The *Playbook* has been downloaded thousands of times and has been publicly shared by the Department of Homeland Security, the National Association of State Election Directors, and the Cybersecurity and Infrastructure Security Agency as a resource for election offices to use as a starting point in building their foundation in election security. I have included the *Playbook* as an appendix to my testimony.

Additionally, I am the Co-Chair of the Department of Homeland Security's Digital Networking Development Working Group. A newly formed working group, the Department of Homeland Security Digital Networking Development (DND) Working Group is a partnership between representatives from the government and private sectors tasked with reviewing and providing recommendations on the development and utilization of digital tools to both private and public members of the election infrastructure community. This working group seeks to evaluate digital tools intended to communicate critical information to help secure election infrastructure, share digital tools to partners in government and private sectors, and research innovative digital tools that support cybersecurity and protect election infrastructure.

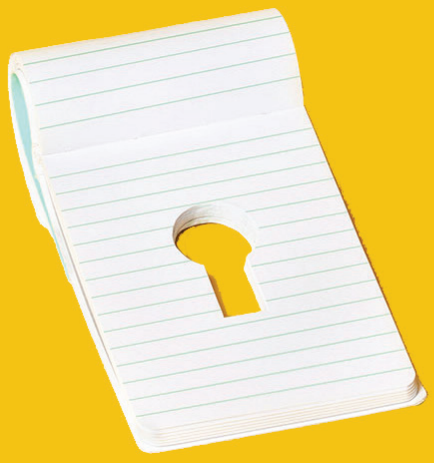
The first of its kind, the working group seeks to serve as a clearinghouse for information on digital tools that support election security. Local election officials have found the numerous sources of election security information to be overwhelming. This makes it difficult to identify the most up-to-date and relevant information. This contributes to the challenge local election officials face in remaining current on the latest digital tools, threats, and challenges. I am grateful for our partnership with DHS in making this information available in a constructive way.

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.

2018 ELECTION SECURITY PLAYBOOK

ORANGE COUNTY, CA ELECTIONS



Your vote. Our responsibility.
ocvote.com

ORANGE COUNTY REGISTRAR OF VOTERS

Table of Contents

Executive Summary

A paradigm shift occurred in election security in 2016 when widely reported attempts were made to disrupt elections in the United States. In addition, there has been a great deal of attention on issues related to ballot integrity, voter registration systems, and ensuring the eligibility of voters.

As a result, Orange County has been aggressively pursuing security measures to protect the integrity of our elections. We believe a proactive “ring of security” is critical to safeguard the millions of ballots that are cast in Orange County during each election cycle.

The purpose of this physical and cybersecurity election playbook is to provide a guide to anticipate, mitigate and respond to physical and cybersecurity threats. As threats continue to increase and evolve, having a playbook is one of many pieces that will help to improve our security profile. Although threats are constantly changing, and incidents are unique, this playbook provides a guide and a set of best practices to be better prepared for threats and incidents. This playbook also provides a set of standards to reference as we continue to improve our current systems and implement new ones.

We have implemented physical and cybersecurity controls as outlined throughout this playbook, while incorporating extensive physical and cybersecurity training for our employees. There are also classified security measures in place to ensure that these mitigation efforts are not compromised.

Our office has already implemented many of the items addressed in this playbook, including the following:

- Physical security surveys were executed.
- Physical security improvements were put into action.
- Partnerships were established with federal agencies, local agencies, and information sharing centers.
- Administrative, technical and physical controls have been enhanced.
- An internal playbook and Incident Response Plan has been developed.

- Plans are in place to conduct risk limiting ballot-polling audits based on a random sample of ballots.
- Proactive list maintenance above and beyond statutory requirements continues.

Orange County will continue to focus our resources on the protection of our election systems, ballot integrity and overall election security. We remain diligent and proud of our involvement at the forefront of election security planning.

Neal Kelley
Registrar of Voters
Orange County, CA

Neal Kelley is an appointee of the U.S. Department of Homeland Security, Election Infrastructure, Government Coordinating Council (GCC) and serves as a member of the U.S. Election Assistance Commission (EAC) Board of Advisors and Voting Systems Standards Board and is a member of the National Academies of Sciences, Engineering, and Medicine's Committee on the Future of Voting.

Introduction

The Orange County Registrar of Voters (OCROV) is responsible for the management of elections for its over 1.5 million registered voters; in fact, there are more registered voters in Orange County than in 21 individual states. The OCROV security systems and controls are in place to enable secure, yet efficient execution of this mission. This public physical and cybersecurity plan was developed to ensure that the information provided by our systems and information remains confidential, available, and accurate. The OCROV is dedicated to protecting the integrity and authenticity of our data as well as the integrity of all votes cast.

The cybersecurity playbook provides clear, actionable tasks using tactical approaches to counter the growing number of cyber as well as physical threats. It is important that we take a strong, proactive approach to our security campaign efforts. This approach is a combination of strategies, best practices, along with cybersecurity policies and procedures to reduce our risks and to minimize and prevent threats.

The importance of a cybersecurity playbook is illustrated by the following quote from the Harvard Kennedy School:

> "The consequences of a cyber breach can be substantial and devastating. For the foreseeable future, cyber threats will remain a real part of our Election process. As democracy's front line, we must recognize the risk of an attack, develop a strategy to reduce that risk as much as possible, and implement response strategies for that moment when the worst happens. While no campaign can achieve perfect security, taking a few simple steps can make it much harder for malicious actors to do harm. Ironically, the most sophisticated state actors often choose the least sophisticated methods of attack, preying on people and organizations who neglect basic security protocols. That is our primary reason for creating this Cybersecurity Campaign Playbook.[1]"

1 Harvard Kennedy School (2017) Defending Digital Democracy / Version 1.3: Retrieved from https://www.belfercenter.org/sites/default/files/files/publication/Playbook%201.3.pdf

Elections as Critical Infrastructure

On January 6, 2017, the Secretary of the Department of Homeland Security (DHS), Jeh Johnson, designated the Election Infrastructure in the United States as a subsector of the existing Government Facilities Critical Infrastructure sector. This designation by DHS means that the Election Infrastructure has become a priority for cybersecurity assistance and protections that DHS provides to a range of private and public-sector entities. Election Infrastructure has been defined as storage facilities, polling places and centralized vote tabulation locations used to support the election process. It is also defined as information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and to report and display results on behalf of state and local governments. Critical Infrastructure is a major concern for cybersecurity threats and vulnerabilities.

Core Information Security Principles

The OCROV has adopted guiding principles that describe our security objectives, which we refer to as our core information security principles. The core information security principles are an integral part of our information security architecture. The principles are the basis for many of our efforts outlined throughout this document. Our office uses a principle referred to as CIA, which is defined as[2]:

> Confidentiality – Confidentiality refers to protecting sensitive information, such as Personally Identifiable Information (PII). Any two of the following data points together – a name with address, Social Security number, driver's license, etc. – are considered PII and must be protected as data assets. The principle of "least privilege" is the idea that only authorized individuals or systems should have access to information on a need-to-know basis. This principle is intended to prevent unauthorized disclosure of voter information, PII or other sensitive voter data.
>
> Integrity – Integrity refers to the prevention of unauthorized or improper modification of systems and information. Integrity includes the principle that information should be protected from intentional, unauthorized, or accidental changes. Controls are put in place to ensure that information is only modified

2 Tipton, Harold F. Official (ISC)2 guide to the CISSP CBK. Boca Raton, FL: CRC Press, 2010. Print.

through accepted practices. This is to ensure that data has not been altered.

Availability – Availability refers to the idea of minimizing downtime. We have controls in place to ensure that our data is highly available, redundant and replicated securely offsite. In case of a disaster, it is important to have plans in place to ensure business continuity while minimizing downtime and impact to voters, which is critical. Future planning will continue to include designing and building everything with redundancy in mind. In addition, disaster recovery policies are in place to overcome disasters such as power failures, fires, and other unplanned disasters. Secure back up of data is also important to make sure access to our data is not disrupted in the event of a disaster.

Top Threats and Vulnerabilities

In order to properly develop a security plan, the potential threats and exploits must first be identified. In the following section, we give examples of potentials and threats that we have identified.

The National Institute of Standards and Technology (NIST), in Special Publication SP 800-30 defines[3] threats as "the potential for a particular threat-source to successfully exercise a particular vulnerability."

NIST Special Publication 800-30 Rev. A defines vulnerability as "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised accidentally, triggered or intentionally exploited and result in a security breach."

Threat of Foreign States

Foreign States are a significant threat because they have access to resources and technologies that make their cyberweapons more dangerous and difficult to defend against. A large amount of cyber threat intelligence data focuses on preventing a breach or a leak from happening; however, even with companies and governments spending more on network defense, breaches from Foreign States are still occurring. A proper defense strategy must be proactive and engaged. We need to combine technology and techniques to combat Foreign States that try to intervene in our elections and

3 NIST Special Publication 800-30 Revision 1 Retrieved from nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

disrupt our democracy. We must take strong actions to prevent interference including misinformation, phishing expeditions, and any other forms of meddling, mischief, and disruptions from Foreign States. Throughout this cybersecurity playbook, the threat from Foreign States is incorporated into the planning process.

Examples of Threats

We have identified examples of potential threats and exploits specific to elections, and later in this report, we will describe some mitigation strategies. Listed below are examples of identified threats:

- Computer virus
- Malware
- Breach of confidential information
- Denial of access
- Bomb threats and physical threats
- Phishing attack
- Hacking
- Social engineering
- Tampering of voting equipment
- Power outage
- Disgruntled poll worker or employee
- Fake information, including from social media
- Physical access to voting machines
- Lost access to voter database
- Voter registration tampering
- Vendor related threats

- Supply chain threats

Potential Impacts to an Election

The above threats must be addressed, because they can potentially impact an election by causing failures to meet election deadlines, causing failures to process results on-time, and causing overall failures of the voting system.

Preventative Measures and Mitigations

In order to address the threats and vulnerabilities listed above, our office implements preventative measures through security mitigations and controls.

Security Mitigations and Controls

Categorizations of Security Controls

Security requires a comprehensive strategy, consisting of multiple facets. Security mitigations can be classified by the types of controls necessary for a secure organization. The types of controls are[4]:

Administrative controls - Administrative controls are procedures implemented to define the roles, responsibilities, policies, and administrative functions needed to manage the environment. The employee hiring and separation procedures listed below are examples of the administrative controls we have in place.

Technical controls – Technical controls are electronic hardware and software solutions implemented to control access to information and information networks. The intrusion detection systems listed below are examples of the technical controls we have in place.

Physical controls - Physical controls protect the organization's people and physical environment, such as locks, fire management, gates and guards. The security cameras and badge access controls listed below are examples of the physical controls we have in place.

In our process of identifying preventative measures and mitigations for our systems, we

4 Tipton, Harold F. Official (ISC)2 guide to the CISSP CBK. Boca Raton, FL: CRC Press, 2010. Print.

attempt to address each of these categories of controls. This helps to ensure we are approaching physical and cybersecurity from a comprehensive perspective.

Examples of Specific Security Controls

Listed below are examples of specific security controls in place, which include examples of administrative, technical and physical controls.

Voting System

- "Air gap" mitigation – An "air gap" refers to the idea that the voting system is not connected to any other network at any other time, including local networks and the internet. Our office uses an "air gap" with our voting system, which is one of the most effective ways of mitigating security risks.

- Ballot creation security – The ballot creation team is located in a room with limited security access, multi-factor badge access, surveillance systems, and no network connections. The printed ballot contains a tint and watermark.

- Chain of custody – Strict chain of custody controls are in place for ballots and voting components.

- Ballot printing - Ballot printing is conducted in-house, mitigating the risk of relying on a vendor for ballot production.

Network Security

- Security Information and Event Management (SIEM) system – SIEM includes intrusion detection, vulnerability assessment, asset discovery and inventory, behavioral monitoring, and log management.

- Physical Security – Strict badge access control and alarm monitoring are important components of our physical security.

- Firewalls – Firewalls are used to protect our networks.

- Intrusion Detection/Prevention Systems – Intrusion detection and prevention systems help to detect attempts of unauthorized access.

- User login security controls – Requiring password complexity, and using least privileged access are important user security controls.

- Critical and security updates, and patch management – Applying security patches is a basic security measure.
- Legacy workstations – Minimizing the use of outdated Operating Systems and software, as well as replacing legacy systems.
- User account management – Immediately disabling unused accounts is a standard security practice.
- Center for Internet Security (CIS) benchmarks – We review their recommendations and utilize them when possible to harden our systems.
- Enforce strong passphrase policy – We enforce password complexity for user accounts.

Website Security

- Encrypted web communication – The website is viewed over a secure connection. Forms submitted by users are encrypted using SHA-xxx Cryptographic Hash Algorithm and utilizes SSL Web Security Certificates (Cryptographic Hash Management Latest Security Certificates).
- SQL injection – Web applications are periodically checked for SQL injection vulnerabilities.

Training and Personnel

- Employee hiring and separation procedures – Background checks are performed on new employees, and all are required to receive security training. Separated employees' accounts are promptly disabled, and badges are deactivated.
- Phishing campaign simulation – Phishing campaign with OCROV staff are periodically simulated in order to test the efficacy of our training.
- Cybersecurity training program – All employees must complete a professionally created cybersecurity training program. Supplemental training is also provided, and security updates are routinely given in staff meetings.
- Physical security accountability – Personnel are held accountable for enforcing physical security practices.

Administrative

- Business continuity plan – A business continuity plan is updated periodically.
- Policies and procedures – Policies and procedures are developed with cybersecurity in mind.
- Incident response plan – An incident response plan is developed in the event of a cybersecurity incident.
- RFP security review – When requesting bids or proposals from vendors, we are including strict security requirements from the vendors.

Physical

- Physical security improvements – Since 2016 (and through 2018) we have made numerous improvements as a result of recommendations from independent assessments.
- Enhanced physical security around election cycles – Security is provided by the Orange County Sheriff's Department on and around the election.
- Surveillance systems – Physical security is enforced with security cameras and other monitoring devices throughout our facilities.

Collaboration

- Collaboration at the federal level – We have developed a direct relationship with DHS, FBI, and the Election Assistance Commission (EAC).
- Collaboration at the local level – We have developed a relationship with our Orange County's Chief Information Security office, and the Orange County Intelligence Assessment Center (OCIAC).
- Increased collaboration around election cycles – Before and after the election, we enhance our security awareness and communication, including regular meetings with the County's security office, DHS, and the FBI.
- Cyber resilience self-assessment criteria report – We will be performing the cyber resilience self-assessment as provided by DHS.

User Level Security

- Improved malware detection - We are currently using endpoint protection that is pattern and behavior based.
- Email encryption - We currently have the ability to send encrypted emails when necessary.
- Email spam\virus filter - Systems are in place that prevent potentially malicious emails from being sent to the users.
- Email links - All links received by users in emails are checked for safety before a user can open the link.
- Data loss prevention - The County is in the process of enabling data loss prevention, which helps to prevent users from sending sensitive information that should not be sent.

Mobile

- Mobile encryption – Any mobile devices and laptops that contain sensitive data will be encrypted before deploying them outside the office.
- Mobile Device Management (MDM) – Mobile devices used, including electronic poll books, will have the ability to be managed remotely, including the ability to remotely wipe the data.

Public Information

- Comprehensive election information – We will continue to provide accurate information to voters through multiple channels, which can be used to counteract false information.

Overall Security

- Third party security audit – We are using a third party to conduct a cybersecurity audit, which can help to discover additional vulnerabilities.

Voting System Security Controls

The voting system currently used in Orange County is a Direct Record Electronic (DRE) voting system, with a Voter Verifiable Paper Audit Trail (VVPAT). In order for a voter to access a ballot at a polling place, a four-digit random access code is used for activation. The electronic voting booth and poll worker control system possess

only minimal functionality as compared to a fully operational personal computer, thus minimizing the risk of unauthorized system access and code modification. Furthermore, the voting system is a standalone system without connectivity to any external network or the internet, which makes unauthorized access from a network virtually impossible. Additional technical controls are in place and required in order for the voting system to be certified for use in the State of California.

Information Integrity and Accuracy

Important administrative controls are the extensive logic and accuracy audits that are conducted before the election to make sure the voting system is properly recording the cast vote records. After the election, random audits are performed manually to ensure the paper record matches the final tally. Paper audit trails allow us to compare totals and check the results against the votes verified by the voters.

Risk Limiting Audits

California does not currently require Risk Limiting Audits (RLA). However, as a component of our security plan for 2018, we will be conducting pilot RLAs to ensure that the integrity of the votes cast are true and correct. Computerized systems may produce incorrect results due to programming errors or deliberate subversion. Even hand counts may be erroneous. RLA audits systematically check the election outcomes reported by vote-counting systems.

Specifically, a risk limiting audit checks some voted ballots or voter-verifiable records in search of strong evidence that the reported election outcome was correct – if it was. Specifically, if the reported outcome (usually the set of winner(s)) is incorrect, then a risk-limiting audit has a large, pre-specified minimum chance of leading to a full hand count that reveals the correct outcome. A risk-limiting audit can stop as soon as it finds strong evidence that the reported outcome was correct. (Closer elections generally entail checking more ballots.)[5]

In addition to the required 1% manual tally (which is a hand-count of 1% of all ballots cast), in 2018 our office will be conducting RLAs in the form of ballot-polling audits based on a random sample of ballots. This will be reviewed by academics from Princeton University, Tufts University and the Massachusetts Institute of Technology (MIT).

5 California Risk Limiting Audits Working Group, Version 1.1, October 2012

Voter List Maintenance

Maintaining an accurate voter list is an important part of the cybersecurity playbook because it prevents widespread voter fraud, and ensures access for eligible Orange County voters. Our office has made a concerted effort in previous years to improve the accuracy of the voter database, but we also our continually looking for additional methods to improve our process of maintaining the voter list.

In 2018, we will be conducting the following list maintenance activities:

- Alternate Residency Confirmation – We send a postcard to all voters who have had no voting or registration activity for four years. If these voters do not respond, they remain in an inactive status, which means they do not receive any election materials in the mail.

- National Change of Address – We use change of address data provided by the Post Office (USPS) to update addresses of registered voters. This also helps us to identify and contact voters who may have moved out of Orange County, or the State.

- Third Party Data Provider – This is an activity that is not required by law, but we will conduct as an additional process to update our voter registration list. We utilize a credit reporting agency to find updated address information for voters who have not provided updated information through all other methods.

- DMV Address Change – We continually process change of address data provided by the Department of Motor Vehicles (DMV).

- National Deceased Voter Data – This is another activity that is not required by law, but we will conduct as an additional process to determine deceased voters. In addition to the deceased voter data provided by the State and the County, we use a service which matches voter information to national deceased records. This provides an additional step to locate voters who have deceased records throughout the entire country.

- First Time Federal Voters – Our office is updating its process to validate first time federal voters. This will improve efforts to ensure voters have provided proof of residence in Orange County.

- Statewide Voter Database – The Statewide Voter Database became the official

system of record for voter registrations in California in 2016. Orange County has taken a proactive role in utilizing this new system to improve the identification of voters that move within the State. As an example, we helped to implement a statewide policy that makes registration dates consistent, in an effort to better determine the most current registrations of the voters.

Early Voting Center Security

Securing access at remote early voting centers is critical. We ensure that Request for Proposals (RFPs) include stringent security requirements of the proposed system, as well as the vendor themselves. From a technical perspective, we include a multi-layered approach to ensure the data remains encrypted and secured at all times. We will be utilizing devices that have Federal Information Processing Standard (FIPS) certified components and data will remain encrypted from point-to-point at all times.

Physical security is also consideration when choosing a location to host early voting. Only facilities that provide adequate physical security are chosen to be early voting sites.

Electronic Poll Book Security

Electronic poll books used in early voting centers must have a high level of security applied. Listed below are examples of our security requirements for electronic poll books:

- Must be certified by the Secretary of State's office.
- Must have encrypted communication between all devices.
- Must use SSL encryption when appropriate.
- The database and other data must be encrypted at all times.
- Must be able to continue to operate in the event of loss of a connection.
- All devices must be shut down and physically secured when not in use.
- Devices will not store personal identifiable information.

Mobile Device Management

Mobile device management allows total control of securing and enforcing policies to tablets, smartphones, and other devices. Mobile device management allows us to

remotely wipe a device, use password enforcement, enable application whitelisting or blacklisting, use data encryption enforcement, control application distribution and software updates, and more.

Chain of Custody Procedure

Chain of custody procedures are used by the OCROV as an administrative control as part of its overall strategy to secure our voting system. The chain of custody procedures include the following:

- Voting booth controllers are secured within a locked caged area, under video surveillance until they are deployed for the election.
- A minimum of two people are present when the voting booth controllers are returned on Election Night.
- Chain of custody documents are used for an additional layer of auditing.
- Voting booth controllers are placed in a numerically sealed transportation box.
- Memory cards are numerically sealed in the voting booth controller.
- All voting equipment is tracked when deployed and returned to the OCROV.
- Election personnel sign chain of custody documents for voting equipment at distribution locations.
- Election personnel and polling place workers are required to check the security seals periodically and report any broken seals or suspicious activity to the OCROV.
- An OCROV driver is accompanied by a Deputy with the Orange County Sheriff's Department that returns voting booth controllers to the OCROV.
- An OCROV representative signs for equipment upon its return.
- Voting equipment is inventoried and placed in a secured, video monitored location.
- Voted memory cards are tallied in a room that allows for open observation.

Partnerships and Information Intelligence Sharing

Information sharing is critical in taking a proactive security approach and is an important part of our preventative measures and mitigations. Tactics, Techniques and Procedures (TTP) is an approach that is used within a cyber threat intelligence solution. TTPs can help with predictive or emergent risk, such as sharing of a zero-day exploit on the Dark Web. A zero-day attack is an attack vector that takes advantage of a security weakness before the vulnerability becomes generally known. There is no time or opportunity for detection because the attacker exploits the vulnerability before the threat is known. TTP is an effective method in helping to prevent zero-day attacks. The TTP method can help identify possible targets, provide threat analysis data, and help with mitigation process. This data or research is provided to us by multi-state sharing cybersecurity threat analysis partners. This section focuses on some of the ways our office employs the approach of intelligence sharing as one of the mitigation strategies of our security plan.

Partnership With Orange County Agencies

The OCROV has been proactive in communicating with the County security team, and they have expressed a commitment to assist the OCROV when needed.

Orange County's Chief Information Security Officer (CISO) and a cybersecurity joint task force meet monthly to review and discuss security topics that focus on information security countywide. We are working to update and refresh policies, standards, and guidelines, which are key components of an effective information security plan. To address the CIA principles of the technology, the County security team routinely conducts a series of assessments and penetration tests on County network infrastructure, systems, and data. The County security team has also expressed a commitment to establishing an in-depth defense methodology for its infrastructure, systems, and data.

Partner with Regional and Local Law Enforcement

We interface on a regular basis with regional (California Secretary of State, Criminal Investigations) and local (Orange County District Attorney's Office) law enforcement. We routinely, when appropriate, continue to refer cases to these agencies for investigations.

In addition to these resources, our office interfaces directly with OCIAC to obtain additional threat information, and to have OCIAC help recover from an incident, if necessary.

Partnership With Federal Agencies

At the Federal level, election systems are designated as critical infrastructure by the Department of Homeland Security (DHS). This designation ensures election systems receive top priority cybersecurity assistance from DHS. Additionally, our office is in direct communication with the FBI, DHS, and EAC. As an example, the Department of Homeland Security National Cybersecurity and Communications Integration Center provides OCROV weekly cyber hygiene assessment reports. This report is intended to provide our office information regarding our office's internet accessible networks and hosts. This report includes vulnerability scan results, new vulnerabilities detected and mitigated vulnerabilities on internet facing hosts. These federal partnerships also help with the defense of risks presented by Foreign States.

Collaborative Intrusion Detection and Prevention System

The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides a security network monitoring service, which includes a near real-time automated system that identifies and alerts on traditional and advanced threats on a network, facilitating the rapid identification of threats and attacks.

Partners of the OCROV Ring of Election Security

Cybersecurity Training & Awareness Program

The OCROV has adopted the County policy of a mandated IT security and awareness training program, which is required to be completed by all employees on an annual basis. This provides employees with basic knowledge and tools that are instrumental in helping the County as a whole to combat cyber threats, including threats that have a social engineering component. The topics covered under the training program include:

- Ransomware
- Password Guidelines
- Safe Election Security and Protection Against Nation State Intrusions
- Social Engineering
- Phishing
- Physical Security
- Privacy
- Mobile Device Usage
- Malware
- Social media

Human Firewall

In any organization, cybersecurity is everyone's responsibility. Human error or targeted spear phishing has consistently been the root cause of publicized cyber attacks, and it is up to the OCROV leadership teams to weave security awareness into the culture of the organization. The term "Human Firewall" means employees, through education and cybersecurity training, are trained to detect, recognize, and report threats. The "Human Firewall" is the human shield of defense against possible social engineering attacks. Our approach is structured to change human behavior by thoroughly training our employees, including volunteer poll workers, to be cautious, and to be trained to recognize and report cybersecurity incidents. The decisions humans make are just as important as the software they use; therefore, the best approach consists of a clear employee cybersecurity program that includes awareness and focuses on continuous

training and education. Additionally, this cybersecurity training and awareness program needs to be more than just a routine requirement; instead, the concepts should be reinforced in order to change employee behavior. For example, email continues to be a significant vector of choice for malware; therefore, it is important that our employees are trained annually, in addition to being reminded in monthly meetings, to be mindful of the many forms of phishing attacks that come through professional and personal emails. Other aspects of the "Human Firewall" include background checks and setting standards for following good security protocols.

Security isn't just a technology issue; it's a personnel issue. Errant clicks, user error, and social engineering attacks such as phishing are some of the biggest threats. Educating and empowering our users to make safer choices is vital to creating a more sustainable and successful long-term defense.

Application of the NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a widely adopted framework that provides an additional perspective to our approach to cybersecurity and was created by the public and private sectors working collaboratively. This framework is composed of the following five major functions:

1. IDENTIFY assets you need to protect.
2. PROTECT assets and limit the impact.
3. DETECT security problems.
4. RESPOND to an incident or be ready to respond with a plan.
5. RECOVER from an incident.

Identify

Our agency, with guidance from Orange County Information Technology (OCIT) enterprise security, has developed the skills to manage the cybersecurity risk to systems, assets, data, and capabilities. This covers areas such as risk assessment, asset management, and governance.

Protect

We have developed and implemented the appropriate safeguards to ensure delivery of services. These security mitigations and controls are outlined throughout this document.

Detect

We have implemented the appropriate systems to identify the occurrence of a cybersecurity event as soon as possible. The security mitigations and controls include items outlined in this document such as intrusion detection systems, and collaboration with other agencies are a part of this strategy.

Respond

OCROV, along with a cybersecurity joint task force, has developed a cybersecurity incident response plan. The plan addresses the appropriate actions in the event of a cybersecurity event. These actions include response planning, communications, analysis, mitigation, and future improvements learned from the incident. This plan is an internal secure document not designed for public distribution.

Recover

We have developed appropriate activities to restore any capabilities or services that are impaired due to a cybersecurity event or physical intrusion. A business continuity plan is also a component of this aspect of the framework. The focus is also to maintain resilience for the network and protect it from further attacks.

Defense in Depth

Defense in depth is an information assurance concept in which multiple layers of security controls or defenses are placed throughout network infrastructure to detect anomalies and unusual network traffic. Preparing for a breach is very important. Multiple layers of network security minimize gaps in protection. Examples of currently used protections at the OCROV are a robust firewall, intrusion prevention, and antivirus protection.

Countermeasures that are used to help defend the network are:

- Identify, minimize and secure all network connections.
- Harden systems by disabling unnecessary services, ports, and protocols.
- Enable available security features of systems used.
- Implement robust configuration management practices.
- Continually monitor and assess the security of the systems, networks, and interconnections.

- Building a “Human Firewall” by providing cybersecurity training, providing awareness and holding individuals accountable.
- Configure our firewall and other security settings to be more restrictive.

These countermeasures are items we will be continually reviewed in order to effectively protect systems and networks from cyber-based attacks. Although defense in depth measures do not (and cannot) protect all vulnerabilities and weaknesses in an environment, they are part of the larger, overall strategy.

Incident Response Plan

Cyber Incident Management in Orange County utilizes a lifecycle approach. The Cyber Incident Management Lifecycle is composed of serial phases: preparation, identification, containment, eradication, recovery, and follow-up. It is also composed of ongoing parallel activities: analysis, communication, and documentation. This lifecycle is derived from many standardized cyber incident response processes such as those published by NIST, as well as other authorities.

The following are descriptions of those actions that comprise OCROV’s Cyber Incident Management Lifecycle:

- Preparation - Maintaining and improving cyber incident response capabilities.
- Identification - Confirming, categorizing, scoping, and prioritizing suspected cyber incidents.
- Containment - Minimizing loss, theft of information, or service disruption.
- Eradication - Eliminating the threat.
- Recovery - Restoring computing services quickly and securely.
- Follow-Up - Assessing response to better handle future incidents through utilization of reports, “lessons learned” and after-action activities, in addition to mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

The following are elements present throughout the Cyber Incident Management Lifecycle:

- Communication - Notifying appropriate internal and external parties and maintaining situational awareness.
- Analysis - Examining available data to support decision-making throughout the Cyber Incident Management Lifecycle.
- Documentation - Recording and time-stamping all evidence discovered, information, and actions taken from Identification through follow-up.

Direct contacts and methods of escalation are imperative to be defined as we prepare for any given election. In the event of an actual attack or incident, we ensure this information and the cybersecurity incident response plan are accessible. It is critical as we prepare and increase our cybersecurity presence, that all involved parties remain in frequent communication, coordination, and are well acquainted with our cybersecurity playbook plans.

Threat Intelligence Services

Threat Intelligence helps organizations understand the risks of the most common and severe external threats. Earlier in this report, we have described how we use partnerships and collaboration to help prevent and mitigate cybersecurity threats. We also utilize those partnerships to respond to incidents.

As an example, we have established a partnership with OCIAC. Not only do they help to identify threats before they occur, they also provide support to respond to an incident, and share the intelligence with other potentially affected entities.

Data Backup and Recovery

An important component of an incident response plan is to have a robust recovery plan, including the ability to restore and recover data after a major disaster. We monitor our backups closely, and we follow best practices in backing up and performing test restores of data. By simply following best practices, our backup and recovery strategy can be an effective defense against encryption and extortion attacks such as ransomware or other data loss.

Rehearsing Responses to Incidents

We will be periodically rehearing our responses to physical and cybersecurity incidents. This will help employees understand their responsibilities, as well as to refine the response plan based on findings from the rehearsals.

Crew Resource Management

Crew Resource Management (CRM) is a training program which encompasses a wide range of knowledge, skills, and attitudes including communications, situational awareness, problem-solving, decision making, and teamwork; together with each of the sub-disciplines that each of these areas entail. CRM training is conducted at the OCROV, and its concepts are reinforced by the Registrar of Voters. CRM empowers employees to respond, make decisions, and communicate effectively during an incident.

Current and Future State

Controls in Place

Our office has implemented physical and cybersecurity controls as outlined throughout this playbook. We have also established partnerships with federal and local agencies to assist with our efforts and to share information. We have incorporated extensive physical and cybersecurity training for our employees. We have also developed an incident response plan in order to be prepared to respond to an incident. There are additional security measures in place that are not shared with the public to ensure that these additional mitigation efforts are not compromised.

Plans for 2018

2018 is an election year, which means we will be required to execute on many of the planning efforts described in this playbook. Many of the controls that have been put in place will be acted upon as we approach the election. Additionally, we will utilize the partnerships we have established by increasing our frequency of communication and establishing checkpoints to evaluate our readiness before the elections.

Future Plans

Threats are constantly evolving, vulnerabilities are continually being discovered, and new systems are periodically implemented; therefore, the playbook must be used as a foundation and guide for the future. As we implement new systems and processes,

we must review this guide to ensure that we are continuing to adhere to our core information security principles, and applying security controls from all facets including technical, administrative and physical perspectives. As we will be updating our voting system in the near future, we will apply this playbook through the entire process beginning with procurement, continuing through implementation, and applying through future elections.

REGISTRAR OF VOTERS
1300 South Grand Avenure, Bldg. C
Santa Ana, CA 92705
714-567-7600
ocvote.com