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