LOS ANGELES COUNTY
REGISTRAR-RECORDER/COUNTY CLERK

DEAN C. LOGAN
Registrar-Recorder/County Clerk

November 4, 2024

TO: Supervisor Lindsey P. Horvath, Chair
Supervisor Hilda L. Solis
Supervisor Holly J. Mitchell
Supervisor Janice Hahn
Supervisor Kathryn Barger

FROM: Dean C. Logan
Registrar-Recorder/County Clerk

CYBERSECURITY READINESS FOR THE 2024 GENERAL ELECTION

As the Los Angeles County Registrar-Recorder/County Clerk (RR/CC) prepares for the November 5, 2024 General Election, cyber security remains one of the most complex aspects of our readiness activities. The Department has established a comprehensive cybersecurity program, incorporating best practices in cybersecurity and collaborating with other security agencies involved in election security at the local, state, and federal levels.

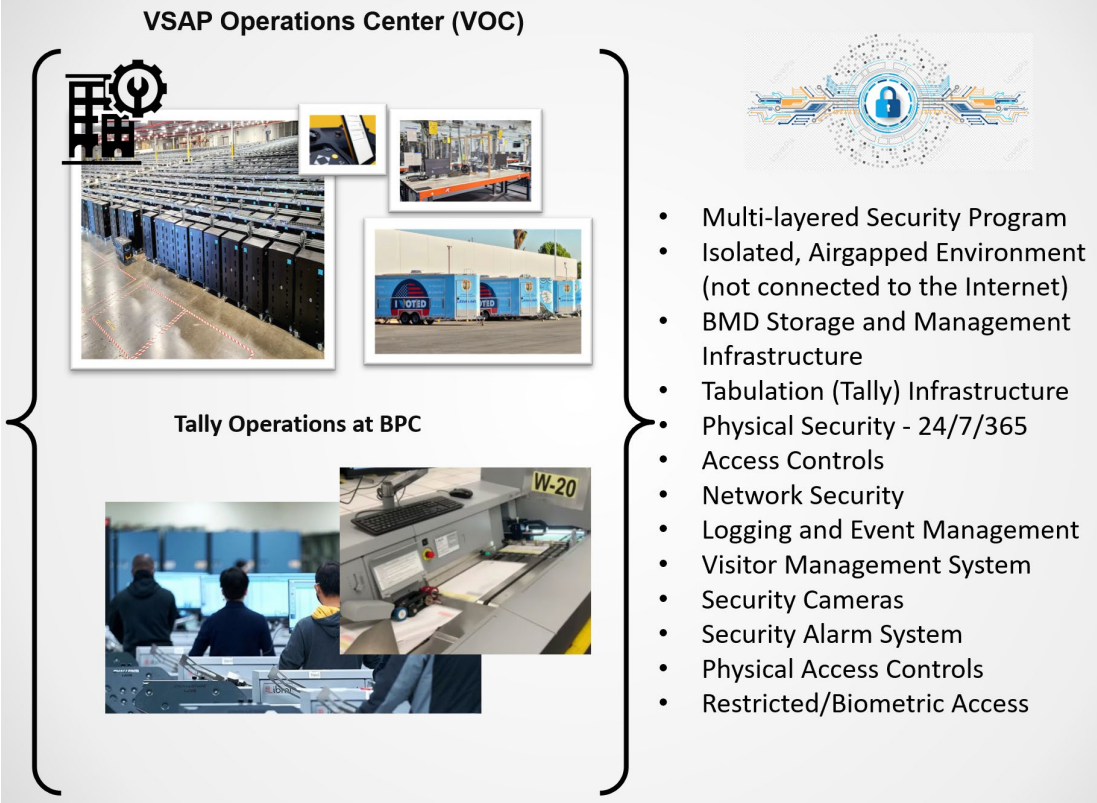
High-Level Threat Summary

The emerging cybersecurity threat landscape presents a complex and multifaceted challenge to the administration of the 2024 Presidential Election cycle. With advancements in technology, threat actors are leveraging sophisticated tactics such as deepfake manipulation, artificial intelligence (AI)-driven mis/dis/mal information campaigns, and ransomware attacks targeting critical infrastructure. The interconnected nature of digital platforms and the proliferation of social media amplify the spread of misinformation, potentially undermining the integrity of the electoral process. Nation-state actors, cybercriminal organizations, and even lone individuals pose threats to electoral systems, voter databases, and political organizations; highlighting the urgent need for robust cybersecurity measures and increased collaboration between all levels of government, technology companies, election-related business partners, and security experts to safeguard democracy against evolving cyber threats.

The threat landscape is vast and ever evolving; this report highlights specific threats posed to LA County and our efforts to proactively mitigate these risks. The RR/CC's comprehensive Cybersecurity Program covers emerging and existing threats:

- **Supply Chain Attacks**: Election administrators rely on various third-party vendors and service providers for software, hardware, and infrastructure support. Supply chain attacks targeting these vendor services could introduce malware or vulnerabilities into election systems, compromising their security and integrity.

  RR/CC's Voting Solutions for All People (VSAP) programs mitigate this risk by reducing our singular dependency on specific election vendors. This publicly owned system was rolled out in 2020, and RR/CC has enhanced it over time. The system consists of Ballot Marking Devices (BMDs), BMD-Manager (BMG), VSAP Tabulation/Tally system (Tally), VSAP Ballot Layout System (VBL) and Enterprise Signing Authority infrastructure (ESA). ***All the core components of VSAP are isolated/air-gapped with no outside network or internet connection.*** The system is deployed in secured locations with 24/7 security. Chain-of-custody procedures enable a full audit trail of devices as well as ballots. The vendors used during an election do not have any control over the devices and the data within those devices. The use of Federal Information Processing Standards (FIPS) compliant seals and digital signatures of devices ensure no tampering of devices while deployed.



- **Ransomware Attacks**: Election administrators may face ransomware attacks where malicious actors encrypt critical systems and demand payment for decryption keys. This could disrupt voter registration databases or communication networks, causing chaos and potentially compromising the

integrity of the election.

The RR/CC has implemented various controls to counter any such attack. The robust backup systems ensure that even in the case of such an attack, RR/CC has the ability to recover swiftly to ensure business continuity. All election related systems are also protected via intrusion detection and prevention systems (IDS/IPS), as well as backup systems to restore any computer system should there be any such incident. The entire network is protected via Network Access Controls and is monitored by the United States Cybersecurity and Infrastructure Security Agency (CISA). Further details of the RR/CC Cybersecurity Program are described in the proceeding sections.

- **Phishing and Spear Phishing**: Cybercriminals may employ phishing emails or targeted spear phishing campaigns to steal login credentials or spread malware within election-related applications and communications platforms. These attacks could lead to unauthorized access to sensitive voter information or the manipulation of election-related data.

  As part of the Department's Cybersecurity Program, there is mandatory cybersecurity training for all staff, which includes phishing simulation campaigns conducted by both RR/CC as well as the Internal Services Department (ISD). In addition to email and content filtering, firewalls provide protection against such threats. Additionally, RR/CC, in collaboration with ISD, has recently implemented a new AI-driven phishing detection platform, which has greatly reduced the amount of phishing email in employees' inboxes. In a situation in which such a threat penetrated the County's network, the strong collaboration and response process is well tested and may be employed to recover from such an attack. Again, the Department's critical voting systems and infrastructure are not connected to the internet and are isolated, further protecting the election processes and systems.

- **Deepfake Disinformation**: The proliferation of deepfake technology enables the creation of realistic yet entirely fabricated audio or video content. Election administrators may encounter deepfake disinformation campaigns aimed at undermining trust in the electoral process or spreading false information about candidates, potentially influencing voter perceptions and decisions.

  Robust social media monitoring systems are in place, monitoring trends during the election timeframe. As recommended by national security experts, election administrators must educate voters about the source and authenticity of election related information. The Department has instituted a comprehensive program for voter outreach (including social media). This proactive voter outreach and election observation program has created a trusted resource and boosted voter confidence in election processes. The Department also utilizes a concept, known as CrowdINT (Crowdsourcing Intelligence) so that voters and the public can also contribute to intelligence gathering by means of reporting. The Department

utilizes community-based organizations and members of the public to obtain this intelligence, via dedicated communication and social media handles. Expanded training for the 2024 General Election saw members of RR/CC's upper management and many of their direct reports participate in a tabletop exercise led by the Election Cybersecurity Operations Center (EC-SOC) that included a deepfake scenario. This simulation featured deepfake audio generated by the E-CSOC for the exercise, giving participants insight into the ease of generating such audio and its use in disinformation campaigns.

- **Social Engineering Attacks**: Sophisticated social engineering tactics may be used to manipulate election staff or volunteers into divulging sensitive information or executing unauthorized actions. For example, attackers could impersonate trusted individuals to gain access to restricted systems or manipulate election procedures.

  As part of RR/CC's Cybersecurity Program, comprehensive education is provided to help desk staff to mitigate social engineering efforts. During the election timeframe, most activities happen in-person at centralized facilities. Vote by Mail processing, signature verification, tally, and support operations occur at the newly established Ballot Processing Center (BPC).

- **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks could disrupt the availability of election-related websites or online services (i.e. election results reporting, ballot processing, online streaming services, etc.), preventing voters from accessing crucial information or participating in the electoral process. These attacks could also serve as a distraction while other malicious activities take place unnoticed.

  The RR/CC website and telephone systems are secured by means of firewalls and threat monitoring. There are various systems in place that monitor, detect, and prevent such attacks. The use of redundant disaster recovery systems allows the RR/CC to recover in case of such an incident. The use of cloud technologies with auto-scaling capabilities has enabled RR/CC to balance website loads (fluctuating and high-volume web traffic) during peak hours.

Recent Incidents

The most notable recent cyber incident related to the elections was the use of spear phishing by a nation-state actor to successfully compromise the personal email account of a senior member of one of the two main presidential campaigns. The nation-state threat actors then stole and leaked campaign materials to the media and members of the opposing campaign in an effort to undermine the electoral process.

> *"The activity was part of Iran's continuing efforts to stoke discord, erode confidence in the U.S. electoral process, and unlawfully acquire information relating to current and former U.S. officials that could be used to advance the malign activities of the IRGC, including ongoing efforts to avenge the death of*

> *Qasem Soleimani, the former commander of the IRGC – Qods Force (IRGC-QF).”*[1]

On the heels of this release comes a Cybersecurity Advisory co-authored by various agencies in the US, Canadian, and Australian governments. These advisory highlights the techniques used by Iran to compromise critical infrastructure across a variety of sectors. As elections are designated critical infrastructure, this advisory could not be more relevant.

> *“Since October 2023, Iranian actors have used brute force, such as password spraying, and multifactor authentication (MFA) ‘push bombing’ to compromise user accounts and obtain access to organizations. The actors frequently modified MFA registrations, enabling persistent access. The actors performed discovery on the compromised networks to obtain additional credentials and identify other information that could be used to gain additional points of access. The authoring agencies assess the Iranian actors sell this information on cybercriminal forums to actors who may use the information to conduct additional malicious activity.”*[2]

The use of AI to create misleading media portraying presidential candidates continues. In a recent story, the creator of a video that used AI to depict one of the presidential candidates sued the State of California over recently enacted laws restricting the use of deepfakes. Although the case has yet to be settled, it highlights issues surrounding AI and information integrity.

> *“The creator of a video that used artificial intelligence to imitate Kamala Harris is suing the state of California after Gov. Gavin Newsom signed laws restricting the use of digitally altered political “deepfakes,” alleging First and 14th Amendment violations.”*[3]

Department of Homeland Security

Various news articles have cited the threat assessment bulletin published by the Department of Homeland Security (DHS). The bulletin mentions threat actors’ intent on harming Americans through the use of violence may become more aggressive as Election Day approaches and may seek to engage in or provoke violence at voting locations, government facilities, public meetings, ballot drop box locations, or private-sector vendor locations that support elections.

> *“The complex interplay of state and local election systems also means "different potential threat vectors and areas for protection.” Would-be hackers' incursion into election infrastructure is not the only threat lurking online: the mushrooming influence of false and misleading information on the internet could sway voters' minds even before they reach the ballot box, the document warns. Foreign*

[1] https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us

[2] https://www.cisa.gov/sites/default/files/2024-10/aa24-290a-iranian-cyber-actors-conduct-brute-force-and-credential-access-activity.pdf

[3] https://www.politico.com/news/2024/09/18/california-deepfake-ban-lawsuit-harris-00179975

> *governments could attempt "to influence US policy, distort political sentiment and public discourse, sow division, or undermine confidence in democratic processes and values to achieve strategic objectives," the bulletin said – advising to look out for "indications that entities are producing or amplifying misleading information about the time, manner, or place of voting, including providing inaccurate election dates or false claims about voting qualifications or methods."*[4]

The article goes on to state that foreign actors could try to "influence US voters through psychological operations, the infiltration of political parties, or the covert dissemination of false or misleading information through social media or other means..."

RR/CC's social media monitoring toolset measures trends and passes on the intelligence to outreach staff so that any impact of misinformation can be countered. Recently, the Department successfully shut down a social media account, as a result of impersonation detection.

(Mis)(Dis)(Mal) Information

Misinformation, disinformation, and mal information are terms used to describe different types of inaccurate or misleading information. While they are related, each term has a distinct meaning. This is especially pronounced during the election timeframe to protect election integrity and public trust.

- **Misinformation** refers to false or inaccurate information that is spread, but there may not be an intent to deceive. It can occur due to mistakes, misinterpretations, or the dissemination of information without verifying its accuracy. Misinformation is often spread unintentionally and can be corrected through fact-checking and providing accurate information.

- **Disinformation** involves the intentional creation and dissemination of false information with the purpose of misleading others. The goal of disinformation is often to manipulate public opinion, sow confusion, or achieve a specific agenda. Disinformation is a deliberate act, and those behind it know that the information they are spreading is false.

- **Mal Information** refers to the intentional dissemination of true information but with the aim of causing harm to a person, organization, or entity. This could involve sharing private or sensitive information to damage someone's reputation, invade privacy, or create negative consequences. Mal information doesn't necessarily involve false information; rather, it focuses on the malicious use of information.

The RR/CC has instituted a comprehensive program to address the spread of mis/dis/mal information. There is a social media monitoring system in place to find any trends of such misleading information. Proactive voter engagement, providing correct

[4] https://www.nwnewsradio.com/2024/02/02/the-top-threats-facing-the-2024-election/

information via social media and other channels also ensures that voters are getting the correct information. During any election, the RR/CC takes steps to inform the general public about where they can find official and authentic information (which is the RR/CC).

The RR/CC has also implemented a dedicated telephone line for the public to report any case of misleading information that may affect the election in any way. Additionally, the RR/CC is piloting an insider threat form with a select group of vote center technicians. A link to the form has been deployed to the home screen of the technicians' work phones, enabling an individual to report suspicious activity with just a tap and answers to a few questions. There is also a dedicated website page for the public to report any case of tampering with Ballot Drop Boxes throughout the County.

Impact of Artificial Intelligence

The impact of artificial intelligence (AI) on election security is transformative, introducing both opportunities and challenges in the evolving landscape of democratic processes. ***Best practice shows that the most effective way to combat malicious AI is by augmenting existing cyber security tools with other AI technologies.*** AI technologies play a crucial role in enhancing election security by bolstering efforts in threat detection, anomaly identification, and data analysis.

Additionally, AI contributes to the development of advanced authentication methods and encryption techniques, fortifying the resilience of election systems against evolving cyber threats. While the use of AI in election security is imperative for staying ahead of sophisticated adversaries, it is equally important to address ethical considerations, ensure transparency in AI decision-making processes, and prioritizing privacy protection. As elections increasingly rely on digital technologies, the incorporation of AI not only fortifies the integrity of democratic processes but also underscores the ongoing need for adaptive, comprehensive cybersecurity measures to safeguard the election process.

The RR/CC's EC-SOC uses systems that rely on AI to identify trends in the threat landscape. These systems speed up the process of filtering any events that require human intervention, quickly sifting through "data noise." At any given time, there are millions of threats or probes happening from around the world. This system utilizes machine learning algorithms that analyze these events and signatures in real-time and escalate only a handful of events that require human intervention to investigate. ***In a typical election, the AI system analyzes approximately 600 million events in real-time.*** AI, in combination with machine learning and Robotic Process Automation, is being used for data analytics/reporting and ballot data. During this election, the Department will continue to use AI call sentiment analysis and data analytics. With the help of industry partners, the Department will continue to fine tune the accuracy of AI tools and functionality to ensure that those biases identified in early-generation designs related to race and gender have been remediated.

RR/CC Cybersecurity Program

With the rollout of Voting Solutions for All People (VSAP), the RR/CC instituted a department-wide cybersecurity program called Iron Cloud. The programmatic approach is based on cybersecurity frameworks defined by the National Institute of Standards and Technology (NIST).

Security and Integrity of Election Devices

From the manufacturing and rollout of VSAP, the RR/CC has been very diligent in ensuring that the election devices maintain security and integrity. During the manufacturing phase, the process adhered to practices defined in the NIST Cybersecurity framework. The contractors and supply chain management also followed best practices as defined by the Center for Internet Security (CIS) controls.

All election devices, primarily Ballot Marking Devices (BMDs) and Electronic Pollbooks (EPBs), are stored and managed in a central location called VSAP Operations Center (VOC). The VOC is a 215,000 square feet secure facility that stores and manages VSAP election equipment, such as:

- 31,100 Ballot Marking Devices and 6,200 carts.
- 8,647 ePollbooks
- 2,500 Uninterrupted Power Supply
- 1,500 CradlePoint Routers
- 480 ePollbook and 324 auxiliary storage racks

The Department has implemented multi-factor authentication (MFA) for important applications that host election-related data, such as cloud systems for EPBs. The use of Federal Information Processing Standards (FIPS) compliant tamper-evident seals on the devices ensures that any tampering is immediately identified and addressed. The periodic chain-of-custody procedures at the VCs ensure that device integrity is maintained throughout the voting period.

Physical Security

Physical security is a key element in any cyber security program infrastructure should be the first step in any cybersecurity program. All facilities responsible for preparing and processing the election are secured with 24/7 security, a full-scale intrusion alarm, and a camera system with DVR that provides full monitoring of both the internal and external premises. Access is authorized by a pre-approved, name-specific access list referenced by security personnel and validated against their ID. The two primary operation centers that house multiple election processes, systems, and equipment are the Ballot Processing Center (BPC) and the VSAP Operations Center (VOC).

The BPC houses critical operations such as Vote by Mail Signature Verification, Tally, Network Operations Center, IT Call Center, and Election Command Center. To enhance physical security, a fence that encloses the entire property and the surrounding parking

lot has been installed at the BPC. Vehicular gates are accessible only through the main entrance, which is monitored by armed security during operational hours or by use of keycard via the access control system added to the alternate entrances. Members of the public may visit to view ballot processing, as permitted by the California Election Code. During this period, department personnel will be on-site to provide public access and escort public observers throughout the facility.

To safeguard against mail-originated threats, such as fentanyl and other substances, NARCAN Nasal Spray has been supplied, along with training for key staff. Additionally, the Department continues to partner with the Sheriff's Department to provide canine units that will inspect all mail received at the BPC. Daily inspections are conducted in coordination with VBM operations and will continue through certification of the election.

At the VOC, a Visitor Tracking system is available at the front office and dock entrance for non-listed guests to check in and receive a one-day badge. The central control room of the facility is protected via biometric security so that only authorized individuals have the authority to load the election data. Each device is electronically signed so that only authorized devices can be stored within the facility. Anytime a non-signed device gets into the facility, the appropriate staff is alerted to immediately address it. The network infrastructure at VOC manages the BMDs on an isolated network (air-gapped environment) with no connection to the internet. This ensures that no external data gets into the network that can jeopardize the data integrity of the devices.

There is a Chain-of-Custody system in place that allows the Department to maintain a full audit trail of activities on election devices, such as data-loading, QA, and physical transport. This ensures that RR/CC has full visibility into all the actions taken on election devices. In addition, RR/CC utilizes a state-of-the-art Mobile Device Management (MDM) solution to ensure full control of all the devices being deployed in an election. The certificate-based security in EPBs pairs those devices with the routers to ensure that only authenticated devices can communicate with RR/CC's network from the Vote Centers (VCs). This ensures that no foreign device can communicate with the voter registration database from the field.

The RR/CC has also implemented an Enterprise Signing Authority Infrastructure to enable a digital interoperability between various VSAP components. This ensures that only the authorized systems can transfer data to one another. This state-of-the-art system is one of its kind in the election industry and is protected via various security controls and measures.

Ballot Security

The Vote-by-Mail (VBM) ballots are received in a secured location at the Ballot Processing Center (BPC). The location is protected with 24/7 multi-layered security. The access to the building is centrally controlled using keycard protocols and access logs. The chain-of-custody procedures ensure that ballots are fully accounted for while they are being processed at BPC.

The ballots from the VCs are transported with multiple Chain-of-Custody events at the VC, check-in center, and at the BPC while receiving the ballots. The ballots are then scanned and tabulated at the BPC via the VSAP Tally system.

Dedicated Election Cybersecurity Operations Center (EC-SOC)

In addition to the dedicated SOC being managed by ISD, the RR/CC also institutes a dedicated SOC specifically for elections. This center is staffed with cybersecurity experts for 30 days, immediately before and after any major election. The EC-SOC monitors all network traffic from the RR/CC network to the vote centers and all its election-related systems 24/7. There are procedures in place to address and respond to any activity that may pose any threat to election systems. The team also monitors social media trends and collaborates with other agencies (local, federal, and state).

Dedicated Network Operations Center (NOC)

There is a dedicated Network Operation Center that the RR/CC operates during any major election. This operation is located at the BPC and is staffed by approximately 35 network experts. The entire network traffic and communication from every VC is monitored to ensure that only authentic network traffic is passed through the systems. This team also acts as the first line of support in case of a network/communication-related issue during an election.

If you have any questions or need additional information, please contact me at (562) 462-2716 or dlogan@rrcc.lacounty.gov. Your staff may also contact Aman Bhullar, Assistant Registrar-Recorder/County Clerk/Chief Information Officer, at abhullar@rrcc.lacounty.gov.

DCL:JG:AB
JK:cc

c: Chief Executive Office
Executive Office of the Board
County Counsel