LOS ANGELES COUNTY
REGISTRAR-RECORDER/COUNTY CLERK

DEAN C. LOGAN
Registrar-Recorder/County Clerk

October 9, 2026

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

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

CYBERSECURITY READINESS FOR THE 2026 GENERAL ELECTION

As the Los Angeles County Registrar-Recorder/County Clerk (RR/CC) prepares to conduct the November 3, 2026 General Election, this report provides an overview of the Department's cybersecurity readiness. The Department maintains a comprehensive Cybersecurity Program that incorporates best practices in cybersecurity and collaborates with election security partners at the local, state, and federal levels, with the California Secretary of State (SOS) serving as the Department's primary state partner.

High-Level Threat Summary

Election infrastructure continues to face a broad range of cyber and physical threats. In its 2026 Election Infrastructure Security Plan, the Cybersecurity and Infrastructure Security Agency (CISA) notes that election infrastructure is often reachable from general enterprise networks, which can allow an adversary who compromises email systems, workstations, or other IT assets to move laterally toward election systems.[1] CISA also reports that, over the last decade, hackers have attempted to breach voter registration systems in all 50 states, with confirmed success in at least 20.[2] Nation-state activity remains a concern: in April 2026, CISA, the Federal Bureau of Investigation (FBI), and partner agencies warned that Iranian-affiliated actors were exploiting internet-

[1]Cybersecurity and Infrastructure Security Agency (CISA), 2026 Election Infrastructure Security Plan: Securing the Next 250, September 2026. https://www.cisa.gov/sites/default/files/2026-09/2026-CISA-Election-Security-Plan-FINAL-508c.pdf
[2]CISA, 2026 Election Infrastructure Security Plan, supra note 1.

connected industrial control devices across multiple U.S. critical infrastructure sectors, and the agencies updated that warning in July 2026.[3]

The federal support available to election offices has also changed since prior election cycles. In February 2025, the U.S. Department of Homeland Security (DHS) ended federal funding for election-related activities, including services provided through the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).[4] At the end of September 2025, CISA's cooperative agreement supporting the Multi-State Information Sharing and Analysis Center (MS-ISAC) was not renewed,[5] and the MS-ISAC had moved to a fee-based membership model in June 2025.[6] CISA's 2026 Election Infrastructure Security Plan was published in late September 2026, approximately 40 days before Election Day.[7]

In this environment, the Department's election security coordination is anchored at the state level through the SOS Office of Elections Cybersecurity, while the Department continues to work with regional, County, and federal partners. These partnerships are described in the Election Security Coordination section of this report.

As in previous years, the threat landscape is vast and continually evolving. This report highlights specific threats to Los Angeles County election operations and the Department's efforts to mitigate them. The RR/CC's Cybersecurity Program addresses the following threats:

- **Supply Chain and Third-Party Attacks:** Election administrators rely on third-party vendors and service providers for software, hardware, and infrastructure support. A compromise of one of these providers could introduce vulnerabilities into systems outside the Department's direct control or disrupt critical election operations.

  RR/CC mitigates this risk through layered controls focused on independence, isolation, and verification. The Voting Solutions for All People (VSAP) system is

[3]CISA, FBI, and partner agencies, Joint Cybersecurity Advisory AA26-097A, "Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure," April 7, 2026, updated July 22, 2026. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a
[4]Wisconsin Elections Commission, "EI-ISAC/MS-ISAC Updates," memorandum to clerks, March 19, 2025. https://elections.wi.gov/sites/default/files/documents/Clerk%20Communication%20-%20EI-ISAC%20MS-ISAC%20Updates.pdf
[5]StateScoop, "CISA confirms it's ending MS-ISAC support," September 29, 2025. https://statescoop.com/cisa-confirms-its-ending-ms-isac-support/
[6]Center for Internet Security, "Albert: A Smart Solution for Network Monitoring." https://www.cisecurity.org/insights/blog/albert-a-smart-solution-for-network-monitoring
[7]Fast Company, "CISA issues election infrastructure security plan 40 days before midterms," September 24, 2026. https://www.fastcompany.com/91612709/elections-cybersecurity-midterms-cisa-states

publicly owned, which reduces reliance on any single vendor; the current version, VSAP 4.0, was approved by the SOS in March 2026 for use in Los Angeles County.[8,9] All core VSAP components are isolated (air-gapped) from external networks, which is designed to prevent direct external access. Systems are deployed in secured locations with 24/7 physical security, and chain-of-custody procedures, Federal Information Processing Standards (FIPS)-compliant seals, and digital signatures help ensure that devices and ballots remain protected and verifiable. The Department's tabletop exercises during this election cycle address a range of technical and operational compromise scenarios.

- **Ransomware Attacks:** Malicious actors may encrypt critical systems and demand payment for decryption keys. A successful attack could disrupt voter registration databases or communication networks, delay operations, and require recovery procedures to maintain continuity.

  RR/CC mitigates this risk through layered controls focused on resilience, detection, and recovery. Backup systems support rapid restoration of systems and data in the event of an incident. Election-related systems are monitored and protected through intrusion detection and prevention systems (IDS/IPS). The Department's network is also monitored through Albert network intrusion detection sensors, alongside other County security tools; the Albert sensors are now administered solely by the MS-ISAC.[10,11] The Department is continuing its partnership with a ransomware resilience platform to strengthen detection, containment, and recovery capabilities for the 2026 elections.

- **Phishing, Social Engineering, and Identity-Based Attacks:** Threat actors may use phishing emails, text messages, impersonation, or other social engineering techniques to steal credentials or gain unauthorized access to systems and data. Compromised accounts could allow unauthorized access to sensitive systems or data, increasing the risk of operational disruption or data exposure.

  RR/CC mitigates this risk through layered controls focused on awareness, access control, and response. Department staff complete the County's mandatory 2026 cybersecurity awareness training, and phishing simulation

[8]California Secretary of State, Office of Voting Systems Technology Assessment, "Los Angeles County VSAP" (VSAP 4.0 certification, March 11, 2026; administrative approval, March 19, 2026). https://www.sos.ca.gov/elections/ovsta/voting-technology-vendors/los-angeles-county-vsap/
[9]California Secretary of State, CC/ROV Memorandum #26058, "Voting Systems: Approval of the Los Angeles County Voting Solutions for All People (VSAP) 4.0 Voting System," March 2026. https://elections.cdn.sos.ca.gov/ccrov/2026/march/26058nr.pdf
[10]StateScoop, September 29, 2025, supra note 5.
[11]Center for Internet Security, Albert, supra note 6.

campaigns are conducted in coordination with the Internal Services Department (ISD). Email and content filtering reduce exposure to malicious messages, and an AI-driven phishing detection platform has significantly reduced the volume of malicious email reaching employee inboxes. Since March 2026, the Department has enhanced its management of privileged accounts, and the County now restricts access to County systems from locations outside the United States. Multi-factor authentication (MFA) protects important applications that host election-related data. The Department maintains an established incident response capability, and critical voting systems remain isolated from external networks.

- **Data Integrity Attacks:** Unauthorized modification of election-related data—including voter registration records, system configurations, or reporting outputs—could compromise the accuracy and reliability of election outcomes and undermine confidence in results.

  RR/CC mitigates this risk through layered controls focused on prevention, validation, and traceability. Critical election systems are isolated (air-gapped) from external networks, significantly reducing the risk of unauthorized access or modification. Strict access controls, including enhanced privileged account management, limit system interaction to authorized personnel. Chain-of-custody procedures, digital signatures, and audit logging are designed to ensure that changes to systems and data are tracked, verified, and attributable.

- **Deepfake Disinformation and Influence Campaigns:** Advances in artificial intelligence (AI) enable the creation of realistic but fabricated audio, video, and images designed to mislead voters or undermine public trust. Such campaigns could create confusion about election processes or results.

  RR/CC mitigates this risk through layered controls focused on monitoring, communication, and response. Active monitoring of social media and public information channels supports early identification of disinformation trends during the election period. The Department maintains a comprehensive voter outreach program that promotes the RR/CC as the authoritative source of election information, consistent with CISA's recommendation that election offices proactively share accurate information about election processes.[12] The Department also uses CrowdINT (Crowdsourcing Intelligence) so that members of the public can report suspicious content.

[12]CISA, 2026 Election Infrastructure Security Plan, supra note 1.

- **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks may target election-related websites or online services, potentially limiting public access to voter information, election results, or public communications, particularly during high-demand periods such as election night.

  RR/CC mitigates this risk through layered controls focused on resilience, monitoring, and availability. Network protections and continuous threat monitoring provide early detection of abnormal traffic patterns. Redundant disaster recovery capabilities and cloud-based technologies with auto-scaling are designed to keep systems available during periods of high demand or attack and to support rapid recovery from disruptions.

- **Threats to Election Facilities and Personnel:** Election offices and staff nationwide continue to receive threats. CISA reports that it tracked 107 election-related incidents through its Technical Resource for Incident Prevention (TRIPwire) system from January 2022 through September 2026, 96 of which were bomb threats, and that more than a dozen election offices received threatening letters in 2024, some containing white powder.[13] Incidents of this kind could disrupt operations, require evacuations, or endanger staff.

  RR/CC mitigates this risk through layered controls focused on screening, preparedness, and coordination. In September 2026, the Department implemented enhanced entry screening at the Ballot Processing Center (BPC), including metal detection and inspection of bags and personal belongings for all individuals entering the facility, a defined list of prohibited items, and a requirement that employees visibly display identification badges. Sheriff's Department canine units inspect all mail received at the BPC, and naloxone (NARCAN) nasal spray and related training have been provided to key staff. Election facilities are protected by 24/7 security, and the Department coordinates with the Sheriff's Department and regional partners on threat information.

- **Disruption of Critical Infrastructure and Supporting Services:** Election operations depend on power, telecommunications, and other services outside the Department's control. Federal agencies have warned that Iranian-affiliated actors disrupted industrial control devices across several U.S. critical infrastructure sectors, resulting in operational disruption and financial loss.[14] An outage affecting a key facility or network could interrupt ballot processing or vote center operations.

[13]CISA, 2026 Election Infrastructure Security Plan, supra note 1.
[14]Joint Cybersecurity Advisory AA26-097A, supra note 3.

RR/CC mitigates this risk through layered controls focused on continuity, redundancy, and rehearsal. The Department's tabletop exercises in this election cycle have included a scenario involving a power outage at the BPC, to test continuity procedures. Redundant disaster recovery systems support recovery of critical services, and the Network Operations Center (NOC) has completed readiness training that includes backup communications capabilities.

Recent Incidents

Recent incidents show that election risks extend beyond voting systems to supporting infrastructure, official communications, and public perception. The following developments from the past year are relevant to Los Angeles County.

Regional infrastructure. In March 2026, the Los Angeles County Metropolitan Transportation Authority (Metro) identified a breach that led it to shut down a portion of its network. Reuters later reported, citing Israeli security researchers, that Iran-linked hackers were responsible and that roughly 700 gigabytes of data were taken.[15] The incident shows that public agencies within the County are being targeted and that disruptions to regional services can affect the public services residents rely on.

Critical infrastructure targeting. In April 2026, and again in a July 2026 update, CISA, the FBI, and partner agencies warned that Iranian-affiliated actors were exploiting internet-connected industrial control devices in multiple U.S. critical infrastructure sectors.[16] Because election operations depend on power and communications, the Department plans for disruptions to these services regardless of their cause.

Impersonation of election offices. In July 2026, the Rhode Island Department of State warned voters of a phishing email that imitated an official election address and asked recipients to click a link to verify their voter information.[17] Messages that imitate election offices can mislead voters and erode trust in official communications, which is why the Department directs voters to its official channels for registration and voting information.

Covert recording at polling places. During a state primary election in August 2026, individuals posing as voters used concealed cameras at several polling places and later published edited videos of their interactions with poll workers.

---

[15]Reuters, as reported by FOX Television Stations, "Israeli researchers say Iran behind Los Angeles transit system attack," May 27, 2026. https://www.fox29.com/news/israeli-researchers-iran-los-angeles-transit-system-attack

[16]Joint Cybersecurity Advisory AA26-097A, supra note 3.

[17]Rhode Island Department of State, "SCAM ALERT: Rhode Island Department of State Alerts All Voters to Phishing Scam," July 24, 2026. https://www.ri.gov/press/view/51200

The state's chief election official reported that poll workers promptly reported the visits and that law enforcement was reviewing the matter.[18] The incident illustrates how recorded or edited content from election sites can be used to cast doubt on election procedures, reinforcing the importance of transparent observation and accurate public information.

AI-enabled influence operations. In September 2026, researchers attributed a campaign of AI-manipulated videos, falsely branded with a news outlet's logo and targeting specific U.S. Senate candidates, to a Russia-linked influence network.[19] Similar fabricated content could be used to spread false information about where, when, or how to vote in Los Angeles County.

CISA 2026 Election Infrastructure Security Plan

In July 2026, the Secretary of Homeland Security tasked CISA with developing the 2026 Election Infrastructure Security Plan, which CISA published in September 2026.[20] The Plan describes the components of election infrastructure, identifies cyber, insider, and physical threats, and lists the no-cost, voluntary services CISA provides to election officials on request. Its principal observations and recommendations include the following:

- **Cyber vulnerabilities.** CISA identifies limits on patching certified voting systems, inconsistent vendor transparency, and uneven cybersecurity maturity in state and local networks as factors shaping election security. It recommends paper ballots that can be easily reviewed and post-election manual audits of paper ballots before results are certified.
- **Voter registration databases.** Recommended safeguards include MFA for administrative and remote access, network monitoring and anomaly detection, least-privilege access, audit logging with critical logs retained for at least one year, and separation of public-facing services from the master database.
- **Insider threats.** CISA notes that reliance on a large temporary workforce makes insider risk a structural feature of election administration, and that longstanding practices such as chain-of-custody procedures and observation of ballot counting were designed to reduce that risk.

---

[18]Minnesota Secretary of State, "Secretary Simon Statement on Hidden Camera Videos Inside Polling Places," August 14, 2026. https://www.sos.mn.gov/about-the-office/news-room/secretary-simon-statement-on-hidden-camera-videos-inside-polling-places/

[19]AI Incident Database, entry on a Russia-linked influence operation using AI-cloned voices and fabricated news-style videos, September 2026. https://incidentdatabase.ai/cite/1715/

[20]CISA, 2026 Election Infrastructure Security Plan, supra note 1.

- **Physical security.** CISA recommends procedures for handling mail and potential hazardous materials, incident response and continuity of operations plans reviewed at least annually, and proactive public communication that establishes election offices as the authoritative source of election information.
- **Information sharing.** CISA identifies state and regional fusion centers as a key channel for sharing election threat information and states that it is supporting a no-cost information-sharing platform for election officials during the 2026 cycle.

Many of these recommendations correspond to measures described in this report, including chain-of-custody procedures, access controls and audit logging, MFA, network intrusion monitoring, mail-screening procedures, and voter outreach. The Department's regional fusion center, the Joint Regional Intelligence Center (JRIC), is among its information-sharing partners. The Department is also exploring the use of an information sharing platform that CISA successfully operationalized for the 2026 FIFA World Cup.

(Mis)(Dis)(Mal) Information

Misinformation, disinformation, and malinformation describe different types of inaccurate or misleading information. Although related, each term has a distinct meaning, and the distinctions matter during the election period for protecting election integrity and public trust.

- **Misinformation** is false or inaccurate information that is spread without necessarily an intent to deceive. It can result from mistakes, misinterpretation, or sharing information without verifying it, and it can often be corrected through fact-checking and accurate information.
- **Disinformation** is false information that is deliberately created and spread to mislead. Its goal is often to manipulate public opinion, sow confusion, or advance a specific agenda, and those behind it know the information is false.
- **Malinformation** is true information shared with the intent to cause harm to a person, organization, or entity—for example, by exposing private or sensitive information. It focuses on the malicious use of information rather than on falsehood.

The RR/CC has instituted a comprehensive program to address the spread of mis-, dis-, and malinformation. A social media monitoring system identifies trends in misleading information, and the Department passes that information to outreach staff so that inaccurate information can be addressed promptly. Proactive voter engagement through social media and other channels helps voters receive accurate information, and during every election the RR/CC informs the public where to find official, authentic election information.

The Department also maintains a dedicated telephone line for the public to report misleading information that may affect the election, and a dedicated web page for the public to report tampering with ballot drop boxes throughout the County.

Impact of Artificial Intelligence

AI is changing election security, introducing both opportunities and challenges. AI technologies can strengthen threat detection, anomaly identification, and data analysis, and they support advanced authentication and encryption techniques. While the use of AI helps defenders keep pace with sophisticated adversaries, it is equally important to address ethical considerations, ensure transparency in AI-supported decision-making, and prioritize privacy protection.

The RR/CC's Election Cybersecurity Operations Center (EC-SOC) uses AI-based systems to identify trends in the threat landscape and to filter routine activity from events that require human attention. At any given time, millions of probes and attempted attacks occur around the world; machine learning algorithms analyze these events and signatures in real time and escalate only the small number that require investigation by staff. In a typical election, the system analyzes approximately 600 million events in real time. AI, in combination with machine learning and robotic process automation, is also used for data analytics and reporting.

RR/CC Cybersecurity Program

With the rollout of VSAP in 2020, the RR/CC instituted a department-wide cybersecurity program. The program is based on cybersecurity frameworks defined by the National Institute of Standards and Technology (NIST).

Security and Integrity of Election Devices

From the manufacture and rollout of VSAP, the RR/CC has worked to ensure that election devices maintain their security and integrity. Manufacturing followed practices defined in the NIST Cybersecurity Framework, and contractors and supply chain management followed best practices defined by the Center for Internet Security (CIS) Controls.

All election devices, primarily Ballot Marking Devices (BMDs) and electronic pollbooks (ePollbooks), are stored and managed at the VSAP Operations Center (VOC), a 215,000-square-foot secure facility. Equipment at the VOC includes:

- 31,100 BMDs and 6,200 carts
- 8,647 ePollbooks
- 2,500 uninterruptible power supply (UPS) units

- 1,500 CradlePoint routers
- 480 ePollbook storage racks and 324 auxiliary storage racks

The Department uses MFA for important applications that host election-related data, such as cloud systems supporting ePollbooks. FIPS-compliant tamper-evident seals on devices help ensure that any tampering is promptly identified and addressed, and periodic chain-of-custody procedures at vote centers (VCs) help maintain device integrity throughout the voting period.

Physical Security

Physical security is a foundational element of 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 that monitors both internal and external premises. Access is authorized through a pre-approved, name-specific access list that security personnel verify against identification. The BPC and VOC are the two primary centers for election operations, systems, and equipment.

The BPC houses critical operations, including Vote by Mail (VBM) signature verification, tally, the NOC, the IT Call Center, and the Election Command Center. A fence encloses the entire property and surrounding parking lot. Vehicle gates are accessible only through the main entrance, which is monitored by armed security during operational hours, or through keycard access at alternate entrances. Beginning in September 2026, all individuals entering the BPC are subject to metal detector screening and inspection of bags, packages, and personal belongings; a defined list of prohibited items, including weapons, applies; and employees must visibly wear identification badges. Members of the public may observe ballot processing as permitted by the California Elections Code, and Department personnel are on site to provide access and escort observers.

To safeguard against mail-borne threats such as fentanyl and other substances, naloxone (NARCAN) nasal spray has been supplied to key staff along with training. The Department continues to partner with the Sheriff's Department to provide canine units that inspect all mail received at the BPC. Daily inspections are coordinated with VBM operations and will continue through certification of the election.

At the VOC, where no major physical security changes have been made for this election, a visitor tracking system at the front office and dock entrance issues one-day badges to guests who are not on the access list. The central control room is protected by biometric access so that only authorized individuals can load election data. Each device is electronically signed so that only authorized devices are stored in the facility, and staff are alerted if an unsigned device enters. BMDs are managed on an isolated (air-gapped) network with no internet connection, which is designed to keep external data out of the network and protect the integrity of device data.

A chain-of-custody system maintains an audit trail of activities on election devices, such as data loading, quality assurance, and physical transport, giving the Department visibility into the actions taken on each device. A mobile device management (MDM) solution supports control of all devices deployed in an election. Certificate-based security pairs ePollbooks with routers so that only authenticated devices can communicate with the RR/CC network from VCs, which is designed to prevent unauthorized devices from reaching the voter registration database from the field.

The RR/CC has also implemented an Enterprise Signing Authority (ESA) infrastructure that enables secure interoperability among VSAP components, so that only authorized systems can transfer data to one another. The ESA is protected by multiple security controls.

Ballot Security

VBM ballots are received in a secured location at the BPC that is protected by 24/7 multi-layered security. Building access is centrally controlled through keycard protocols and access logs, and chain-of-custody procedures account for ballots throughout processing. Ballots from VCs are transported with multiple chain-of-custody events at the VC, the check-in center, and the BPC, and are then scanned and tabulated at the BPC using the VSAP Tally system.

Dedicated Election Cybersecurity Operations Center (EC-SOC)

In addition to the County security operations center managed by ISD, the RR/CC operates a dedicated EC-SOC for elections. For this election, the EC-SOC will provide 24/7 coverage from October 24 through November 6, 2026, monitoring network traffic between the RR/CC network, vote centers, and election-related systems. Procedures are in place to address and respond to any activity that may threaten election systems, and the team monitors social media trends and collaborates with local, state, and federal agencies.

Dedicated Network Operations Center (NOC)

The RR/CC operates a dedicated NOC during major elections. The NOC is located at the BPC and staffed by approximately 35 network experts. It monitors network traffic and communications from every VC so that only authentic traffic passes through the Department's systems, and it serves as the first line of support for network and communication issues during the election.

Election Security Coordination

The Department's primary election security partner is the SOS. Under state law, the SOS Office of Elections Cybersecurity coordinates efforts between the SOS and local elections officials to reduce the likelihood and severity of cyber incidents, and

coordinates the sharing of election threat information among federal, state, and local agencies.[21] For this election, the Department regularly participates in the 2026 California Election Security Task Force meetings, has an established incident reporting path with the SOS, and participates in the SOS-sponsored Election Situation Awareness Room. The SOS Office of Voting Systems Technology Assessment conducted the review and approval of VSAP 4.0.[22]

The Department also coordinates with the California Cybersecurity Integration Center (Cal-CSIC) within the California Governor's Office of Emergency Services (Cal OES), which serves as the central organizing hub for state government cybersecurity activities and information sharing;[23] the JRIC, the regional fusion center whose area of responsibility includes Los Angeles County;[24] the FBI, including regular participation in the FBI's Cyberhood Watch, where election topics are routinely discussed; and the EI-ISAC, including participation in its election situation room. The Department maintains contact with CISA, at a reduced level of support compared with prior election cycles.

Program Updates Since the March 2026 Report

Since the Department's March 2026 report, the following updates have been made:

- **Voting system.** VSAP 4.0 was approved by the SOS in March 2026 and is in use for this election.[25,26]
- **Physical security.** Enhanced entry screening was implemented at the BPC in September 2026, as described above.
- **Access controls.** The Department enhanced its privileged account management, and the County implemented restrictions on access to County systems from outside the United States.
- **Assessments.** The Department has completed an internal risk assessment and will conduct an external penetration test in partnership with Cal OES.
- **Training and exercises.** Activities include:

[21]California Elections Code section 10.5 (Office of Elections Cybersecurity). https://codes.findlaw.com/ca/elections-code/elec-sect-10-5/
[22]California Secretary of State, Los Angeles County VSAP, supra note 8.
[23]California Governor's Office of Emergency Services, "California Cybersecurity Integration Center" (quoting Government Code section 8586.5). https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/cybersecurity-task-force/
[24]Joint Regional Intelligence Center, "Who We Are." https://www.jric.org/default.aspx?MenuItemID=265&MenuSubID=111&MenuGroup=Public+Home
[25]California Secretary of State, Los Angeles County VSAP, supra note 8.
[26]CC/ROV Memorandum #26058, supra note 9.

- September 2026: an election simulation; a live security tabletop exercise; Contact Center training and operational updates; field support technician (FST) training planning and simulation preparation; and security tooling and alert-tuning training.

October 2026: continuing election operations training; staffing partner training assignments for FSTs; Media Call Center training; NOC readiness training; surge staff security training; and a Countywide executive stakeholder tabletop exercise.

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.

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