THE MCMILLAN LAW FIRM

A PROFESSIONAL CORPORATION
4670 Nebo Drive, Suite 200
La Mesa, CA 91941-5230

Scott A. McMillan
Bryan C. Rho

All lawyers licensed to practice in California.

Tel: (619) 464-1500
Fax: (619) 828-7399

Attorney's Direct Contact Information:

Scott A. McMillan, Lawyer
Office: (619) 464-1500 ext 14
Direct Telephone: (619) 393-1751
Cellular Telephone: (619) 274-0884
Email: scott@mcmillanlaw.us

May 21, 2021

Via Email Delivery [rov-info@sonoma-county.org], First Class, and Certified Mail [7021 0350 0001 8153 9829] Return receipt requested

Deva Marie Proto
County Clerk-Recorder for Sonoma County
PO Box 11485
Santa Rosa, CA 95406
Phone: 707-565-6800

Re: General Election, November 3, 2020
Subject: **Demand for Inspection or Production of Public Records Numbers 1-69.**

Dear Ms. Proto:

On behalf of my client, who presently wishes to remain anonymous, I request inspection, copying and/or production of the documents set forth in the following requests in electronic format.

I demand inspection of these documents according to Article 1, Section 3 of the California Constitution and/or the California Public Records Act (Gov't. Code § 6250 et seq.)

I will execute the statement required according to Elections Code section 2194. Please immediately, upon your receipt of this letter, forward that statement and it will promptly be returned to you. The below requests are made for a journalistic, scholarly, political or governmental purpose, and such the information will not be used to sell a product or service. (Gov't Code § 6254(f)(3).)

We intend to publish some of the documents which are sought below to the public, or otherwise disclose those publicly. Thus, as to any documents that are produced that should not be published to the public, either based upon Elections Code section 2194, or some other section, we request that such documents be marked as "non-public", "restricted" along with the legal basis for the restriction, on the document. We also request that the documents produced be identified, page by page, with a Bates number so that we can track the documents, and that the "non-public" documents be produced in a separate packet from such document that lacks any restriction from public disclosure.

The Registrar's responses to these requests for inspection may result in litigation to the extent that we do not believe that the Registrar has made a good faith effort to locate responsive documents. Thus, we request that you keep a record of the efforts to search for the documents, and be prepared to tender a knowledgeable witness that will be able to testify at deposition, or at court hearing, regarding the search for responsive documents, and to provide documents substantiating such a search.

We intentionally refrained from requesting to inspect any particular ballot, or the contents of ballots as we are aware of the privacy of the ballots. Please do not construe the requests herein as such an effort and interpose a refusal to produce requested documents. Such a misconstruction of the request will result in my immediately filing legal action.

We are entitled to inspection of the documents, subject to appropriate redactions, according to Article 1, Section 3 of the California Constitution and/or the California Public Records Act (Gov't. Code § 6250 et seq. "CPRA".)

The California Supreme Court described the background of the CPRA:

> The Legislature enacted the CPRA in 1968. (Stats. 1968, ch. 1473, § 39, p. 2945.) It was modeled after the 1967 federal Freedom of Information Act (5 U.S.C. § 552). (*Los Angeles County Bd. of Supervisors v. Superior Court* (2016) 2 Cal.5th 282, 290 [212 Cal. Rptr. 3d 107, 386 P.3d 773].) HN1 The CPRA explains that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state." (§ 6250.) To promote this fundamental right, the CPRA provides that "every person has a right to inspect any public record, except as hereafter provided." (§ 6253, subd. (a).) "In other words, all public records are subject to disclosure unless the Legislature has expressly provided to the contrary." (*Williams v. Superior Court* (1993) 5 Cal.4th 337, 346 [19 Cal. Rptr. 2d 882, 852 P.2d 377] (Williams).)

> Proposition 59, a measure submitted to the voters in 2004, enshrined the CPRA's right of access in the state Constitution: "The people have the right of access to information concerning the conduct of the people's business, and, therefore, the meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny." (Cal. Const., art. I, § 3, subd. (b)(1), added by Prop. 59, as approved by voters, Gen. Elec. (Nov. 2, 2004).) The state Constitution implemented this right of access with the general directive that a "statute, court rule, or other authority … shall be broadly construed if it furthers the people's right of access, and narrowly construed if it limits the right of access." (Cal. Const., art. I, § 3, subd. (b)(2).)

(*Am. Civil Liberties Union Found. v. Superior Court* (2017) 3 Cal. 5th 1032, 1038-39, 221 Cal. Rptr. 3d 832, 837, 400 P.3d 432, 436.)

Where we were able to do so, We have set forth the provisions of the specific provision of Title 2, California Code of Regulations. Thus, to the extent that there is any ambiguity in the request, your office will be guided by the preceding reference to the applicable regulation. If no such documents exist that were created in compliance with the regulation, please advise, individually to each request.

The California Supreme Court holds that:

> In considering claims for exemption, we are guided by the general principle that "exemptions are construed narrowly, and the burden is on the public agency to show that the records should not be disclosed."

(*Cal. First Amendment Coal. v. Superior Court* (1998) 67 Cal. App. 4th 159, 167, 78 Cal. Rptr. 2d 847, 850.)

Accordingly, we demand that the County provide an exemption log reflecting the documents withheld, the exemption claimed, and that such log describes the documents with sufficient particularity that litigation regarding the production of such documents can be meaningfully addressed in the Superior Court. The specific documents should be uniquely numbered so as to facilitate an in camera review. None of the documents sought are the subject of an evidentiary privilege. Thus, an in camera review must be ordered. (Gov. Code § 6259.)

We are aware of the provisions of two relevant statutes implicated by some of the requests.

Government Code section 6254, subd. (aa) states:

> "(aa) A document prepared by or for a state or local agency that assesses its vulnerability to terrorist attack or other criminal acts intended to disrupt the public agency's operations and that is for distribution or consideration in a closed session."

We anticipate that you will be able to accommodate the requests by appropriate redactions. We are not interested in the assessment of the vulnerability. Rather, it is the process that any vulnerabilities are assessed that was undertaken prior to the

None of the documents sought by the requests below should fall expressly within that category. To the extent such documents do fall within that category, redactions can be made removing the details. The Registrar was required to assess vulnerability. We doubt that such assessment took place. We don't believe that the Registrar followed the protocols.

Government Code section 6254.19, provides:

> Nothing in this chapter shall be construed to require the disclosure of an information security record of a public agency, if, on the facts of the particular case, disclosure of that record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency. Nothing in this section shall be construed to limit public disclosure of records stored within an information technology system of a public agency that are not otherwise exempt from disclosure pursuant to this chapter or any other provision of law.

Once again, to the extent that the disclosure would reveal **existing** vulnerabilities, or otherwise increase the potential for an attack on the system, make a redaction. However, given the controversy regarding the November 3, 2020 election, we would hope that previously existing vulnerabilities have been addressed and corrected.

If such vulnerabilities have not been corrected, thereby entitling the county to claim exemption from production according to section 6254.19 we will expect that you will explicitly so state.

Outbound, public facing addresses are but one example of information that is not private. External router traffic, and connection requests and logs, are by definition public. Wifi networks which are detectable from the exterior of a building, or within the public areas of a building are not private information.

We request an estimate of the cost of the production, by specific request, to the extent that the total cost of production of the matters requested herein exceeds $125.00.

If any portions of the records are exempted from disclosure, the non-exempt portions of relevant records are demanded. To the extent that an administrative appeal is available for refusal to provide these documents to me, please provide details for the means of such administrative appeal.

2 CCR § 19060(c)

> *(c) The Secretary of State shall maintain the official statewide voter registration system. County elections officials shall synchronize voter registration records in the county election management system with the statewide voter registration system and use the official statewide voter registration system to determine eligibility to vote*

1. Provide those documents identifying, by date, time and means, all synchronization transmissions between the California Secretary of State and the county Registar of Voters.

2. Provide those documents with the results of each synchronization transmission between the California Secretary of State and the county Registar of Voters, by number of registrants confirmed as valid, and those that are identified as invalid.

2 CCR § 19061. Immediate Action Required.

> *Unless otherwise provided in state or federal statute, state or federal regulation, or a binding court decision, if a county elections official receives notification from a voter, the Secretary of State, another county, or a court requesting or directing a modification to a voter's registration record, the county elections official shall immediately take all reasonable actions to apply the modification or research and resolve the notification, including but not limited to, reviewing registration and voting history, reviewing source documents, matching signatures, or contacting the voter directly. The notification shall be resolved no later than five (5) business days from receipt by the county elections official. The modification shall not be effective until the county elections official has submitted the update to the statewide voter registration system.*

3. Provide those documents which reflect notifications from the Secretary of State requesting or directing modifications to a voter's registration record between September 1, 2020 and November 15, 2020.

4. Provide those documents that reflect, in summary form, the modifications to the voter registration record, by date, time, and by any unique voter registration number or name of voter, for those records modified between September 1, 2020 and November 15, 2020.

2 CCR § 19064. County Security.

> *(c) Each county shall complete a security assessment of its election information system prior to a statewide primary election. The security assessment shall evaluate the:*
>
> * * *
>
> *(2) Active management (inventory, tracking, and correction) of all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is found and prevented from installation or execution.*

5. Provide those documents identifying where, by geographic location, ballots were counted in the County between October 15, 2020, through November 30, 2020.

6. Provide those documents, i.e., logs, narratives of inspection, created between September 1, 2020 and November 15, 2020 reflecting "Active management (inventory, tracking, and correction) of all software on the network so that only authorized software is installed and can execute" took place in compliance with 2 CCR § 19064(c)(2).

> *(3) Establishment, implementation, and active management (tracking, reporting, and correction) of the security configuration of laptops, servers, and workstations in order to prevent attackers from exploiting vulnerable services and settings.*

7. Provide those documents, i.e., logs, narratives of inspection, created between September 1, 2020 and November 15, 2020 reflecting "active management (tracking, reporting, and correction) of the security configuration of laptops, servers, and workstations in order to prevent attackers from exploiting vulnerable services and settings" took place in compliance with 2 CCR § 19064(c)(3).

2 CCR § 19064(c)(9) *Active management (tracking, control, and correction) of the ongoing operational use of ports, protocols, and services on networked devices in order to minimize vulnerabilities available for attack.*

8. Provide those documents, i.e., logs, narratives of inspection, created between September 1, 2020 and November 15, 2020 reflecting "Active management (tracking, control, and correction) of the ongoing operational use of ports, protocols, and services on networked devices in order to minimize vulnerabilities available for attack" took place in compliance with 2 CCR § 19064(c)(9).

9. Provide the log files for all data traffic, including connection requests accepted and refused, between the county's election information file and any other location between September 1, 2020 and November 15, 2020.

2 CCR § 19064(c)(15) *Tracking, controlling, preventing, and correcting the security use of wireless local area networks, access points, and wireless client systems.*

10. Provide those documents, i.e., logs, narratives of inspection, created between September 1, 2020 and November 15, 2020 reflecting " Tracking, controlling, preventing, and correcting the security use of wireless local area networks, access points, and wireless client systems" which took place in compliance with 2 CCR § 19064(c)(15).

11. Provide those documents, i.e., logs, narratives of inspection, created between September 1, 2020 and November 15, 2020 reflecting the inventory and identification of all wireless connections in the County's ballot processing location.

12. Provide those documents, i.e., logs, narratives of inspection, created between September 1, 2020 and November 15, 2020 reflecting the inventory and identification of all wireless-capable devices in the County's ballot processing location.

13. Provide those documents, identifying by serial number, MAC address, device, and location, and the custodian of, all wireless-capable devices in the County's ballot processing location between November 2, 2020 and November 13, 2020.

2 CCR § 19064(c)(19) *Protection of the organization's information, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight).*

14. Provide those documents, reflecting any incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight) operational prior to October 15, 2020, which took place in compliance with 2 CCR § 19064(c)(19).

15. Provide those documents, reflecting training on any incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight) prior to October 15, 2020.

16. Provide those documents, reflecting roles on any incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight) prior to October 15, 2020.

17. Provide those documents, reflecting communications on any incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight) prior to October 15, 2020.

18. Provide those documents, reflecting management oversight on any incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight) prior to October 15, 2020.

2 CCR § 19064

> *(d) Each county and its EMS vendor shall take the following security measures to provide security for the county's EMS and election information system, as well as for environments that interface with the statewide voter registration system and/or contain statewide voter registration system data:*
>
> > *(1) At all times servers hosting county voter registration and election information systems including the county's EMS as well as any Secretary of State property, such as routers, shall be secured in a designated area away from public access. The designated area shall be secured with a method to determine the identity of each person that has accessed the designated area and unauthorized access to this designated area must be detectable*

19. Provide those documents reflecting the hardware and software system configurations of the Election Management System ("EMS").

20. Provide those documents reflecting the memory sticks and similar technology that contain software and/or data used in the November 2020 election.

21. Provide those documents reflecting the EMS operating system, adjudication, ranked choice voting, and election event designer logs.

22. Provide those documents reflecting the identity of each person that has accessed the routers for the county's EMS and election information systems between October 15, 2020 and November 13, 2020.

2 CCR § 19064(d)

> *(2) Only staff authorized by the county shall have physical access to servers hosting the county's EMS and election information system, including servers containing the county's EMS as well as any Secretary of State property, such as routers.*

23. Provide those documents which identify all persons, not permanently employed by the County, who accessed servers or routers of the EMS and election information system between October 15, 2020 and November 14, 2020.

2 CCR § 19064(d)

> *(3) The county's EMS and election information system shall only be accessible by persons authorized by the county.*

24. Provide documents which identify all persons authorized by the county who accessed servers or routers of the EMS and election information system between October 15, 2020 and November 14, 2020.

2 CCR § 19064(d)

> *(4) No peripheral devices (e.g., disks, flash drives, smartphones, etc.) shall be attached to Secretary of State property, such as routers, installed at the county.*

25. Provide those documents which identify all persons with USB or "flash drives" that were allowed access to any location where votes were tallied or processed in the County.

2 CCR § 19064(d)

(12) Direct user access to the county's EMS and election information system shall require, at a minimum, single sign-on authentication. However, effective July 1, 2021, direct user access to the county's EMS and election information system shall require, at a minimum, two (2) sign-on authentications.

26. Provide those documents which identify all persons with sign-on authentication authorization as a direct user to the county's EMS and election information system between September 15, 2020 and December 1, 2020.

2 CCR § 19064(e)

(e) The county's EMS and election information system shall implement security log management, which includes the following:
(1) Log all systems and network devices with sufficient information collection.
(2) Securely store log files separately from the systems monitored, keep these files archived, and protect these files from unauthorized modification, access, or destruction.
(3) Use log monitoring tools to send real-time alerts and notifications.
(4) Utilize multiple synchronized United States-based time sources.

27. Provide the log files for the county's EMS and election information system with entries between September 15, 2020 and December 1, 2020.

28. Provide those documents or records reflecting a network topology plan or map referencing the devices attached each other device within the county's EMS and election information system.

29. Provide those documents or records reflecting memory sticks and similar technology that contain software and/or data used in the November 2020 election.

30. Provide those documents or records reflecting the log monitoring tools used to send real-time alerts and notifications.

31. Provide the "real-time alerts and notifications", as referenced in 2 CCR 19064(e)(3) sent between September 1, 2020 through December 10, 2020.

2 CCR 19064(f) Counties shall regularly review log(s) for any errors, abnormal activities, and any system configuration changes.

32. Provide those documents or records reflecting review, at any time, of "any errors, abnormal activities, and any system configuration changes", identified between September 1, 2020 through December 10, 2020.

33. Provide those documents or records reflecting Tabulator machine reports and error rate histories/logs.

34. Provide those documents which reflect "any errors" in the county's EMS and election information system identified between September 1, 2020 through December 10, 2020.

35. Provide those documents which reflect "abnormal activities" in the county's EMS and election information system identified between September 1, 2020 through December 10, 2020.

36. Provide those documents which reflect "system configuration changes" in the county's EMS and election information system identified between September 1, 2020 through December 10, 2020.

> *2 CCR 19064. (g) Counties shall report detected unauthorized use, suspected breach, or denial of service attack on the county's EMS and election information system to the Secretary of State Elections Division Help Desk within 24 hours of discovery.*

37. Provide those documents which reflect "unauthorized use" in the county's EMS and election information system identified between September 1, 2020 through December 10, 2020.

38. Provide those documents which reflect "suspected breach" in the county's EMS and election information system identified between September 1, 2020 through December 10, 2020.

39. Provide those documents which reflect "denial of service attack " in the county's EMS and election information system identified between September 1, 2020 through December 10, 2020.

40. Provide those documents which reflect Native ballot scanned images.

41. Provide those documents reflecting a report to the Secretary of State Elections Division Help Desk of a "detected unauthorized use, suspected breach, or denial of service attack" between September 1, 2020 through December 10, 2020, as required under 2 CCR 19064 (g).

2 CCR § 19079. State Death and Felony Status Records.

> *(d) Upon receipt of a notice of potential match, the county elections official shall determine whether the registration record matches a record of a deceased person or person who is currently in state or federal prison or on parole for the conviction of a felony which renders that person ineligible to vote in accordance with Section 19061. If a match is confirmed by the county elections official, the county elections official shall accept the potential match and that voter's record shall be cancelled.*
>
> *(e) When the Secretary of State receives a record of a voter with a federal felony conviction which renders them ineligible to vote, the record shall be forwarded to the county elections official of the voter's county of residence. The county elections official shall process the record in accordance with Section 19061.*
>
> *(f) County elections officials shall process county death records in accordance with Elections Code section 2205, and upon identifying a match with a voter's record shall submit any change in the registration record to the statewide voter registration system in accordance with Section 19061.*
>
> *(g) County elections officials shall process county felony records in accordance with Elections Code section 2212, and upon identifying a match with a voter's record shall submit any change in the registration record to the statewide voter registration system in accordance with Section 19061.*

42. All records reflecting change in registration status submitted to the statewide voter system by the county due to felony status processed between September 1, 2020, and November 10, 2020.

43. All records reflecting change in registration status submitted to the statewide voter system by the county due to federal felony status processed between September 1, 2020, and November 10, 2020.

44. All records reflecting change in registration status submitted to the statewide voter system by the county due to county death records reflecting voter to be deceased processed between September 1, 2020, and November 10, 2020.

45. All records reflecting the total cancellations directed by the Secretary of State processed by the county between September 1, 2020, and November 10, 2020.

46. All records reflecting searches of county felony records between September 1, 2020, and November 10, 2020.

47. All records reflecting searches of county death records between September 1, 2020, and November 10, 2020.

2 CCR § 19080. *DMV Change of Address Notification.*

* * *

48. All records reflecting county searches of DMV Change of Address (DMV COA) between September 1, 2020, and November 10, 2020.

49. All records reflecting total submissions by changes in the registration record to the statewide voter registration system in accordance with Section 19061, between September 1, 2020, and November 10, 2020.

2 CCR § 19086. *Report of Registration.*

* * *

50. Those documents reflecting the dates of certifications of information provided to the Secretary of State according to 2 CCR § 19086(b).

2 CCR § 19087. *Official List Extract.*

* * *

51. Those documents reflecting the date of generation of the official list extract from the statewide voter registration system for the purpose of conducting the 2020 General Election.

52. Those documents reflecting the date of each subsequent or supplemental rosters, after the initial roster for the purpose of conducting the 2020 General Election.

2 CCR § 19098. *Certification of County Elections Official.*

* * *

53. All certifications executed by any county election official for the November 3, 2020 General Election.

General Requests

54. The number of ballots determined by the county through adjudication for the November 3, 2020 election.

55. All ballots duplicated by the county through adjudication for the November 3, 2020 election.

56. Those documents that identify the records of ballots duplicated for the November 3, 2020 election.

57. Those documents that identify the records of ballots adjudicated for the November 3, 2020 election..

58. Those documents that identify the records of changes to ballots made for the November 3, 2020 election.

59. All correspondence, whether such correspondence occurred by physical letter, email, text message, with any person employed by or affiliated with Dominion Voting Systems, Inc. between April 1, 2019 through December 10, 2020.

60. All correspondence, whether such correspondence occurred by physical letter, email, text message, with any person employed by or affiliated with the California Secretary of State's Office of Voting Systems Technology Assessment between April 1, 2019 through December 10, 2020.

61. All electronic documents containing the phrase "Image Cast Remote 5.10".

62. All electronic documents containing the phrase "Image Cast Remote 5.10A".

63. All electronic documents containing the phrase "Image Cast Remote 5.2".

64. All electronic documents containing the phrase "Suite 5.10A".

65. All electronic documents containing the phrase "Suite 5.10".

66. All electronic documents containing the phrase "Suite 5.2".

67. All electronic documents containing the phrase " ImageCast Evolution 5.10.9.3".

68. All electronic documents containing the phrase " ImageCast ICX 5.10.11.11.".

69. All electronic documents containing the phrase "Eric Coomer"

We request that records be produced, unaltered, except where a statutory privilege applies and in that event that the basis for the privilege be stated with sufficient information to address that in court.

Further,

1. That emails be provided in native format, i.e., an Outlook export file, with all header information intact.
2. That documents be provided in pdf format.
3. That data files be provided in Excel format, or comma-delimited format.

Respectfully yours,

/s/ Scott A. McMillan

Scott A. McMillan