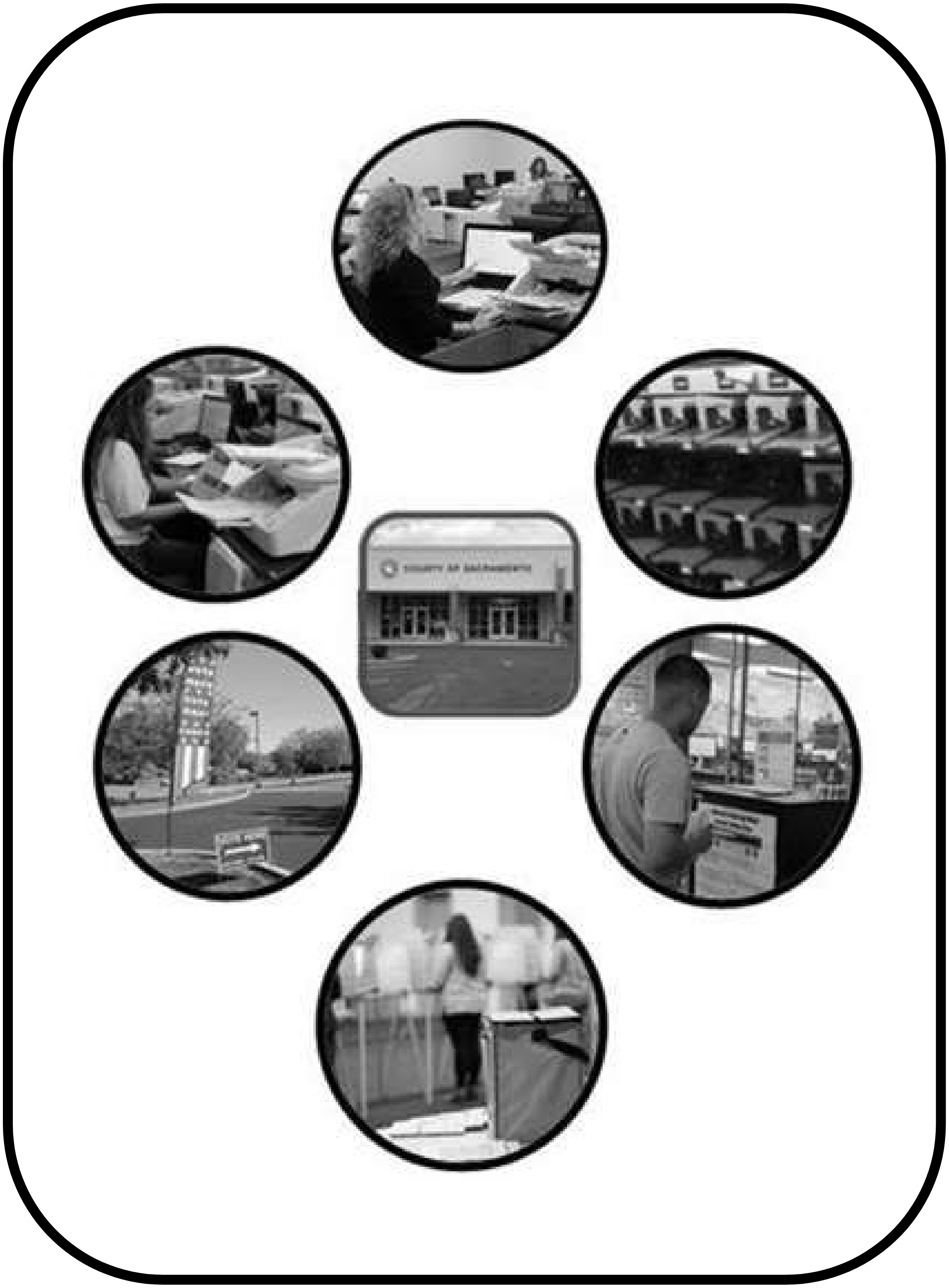
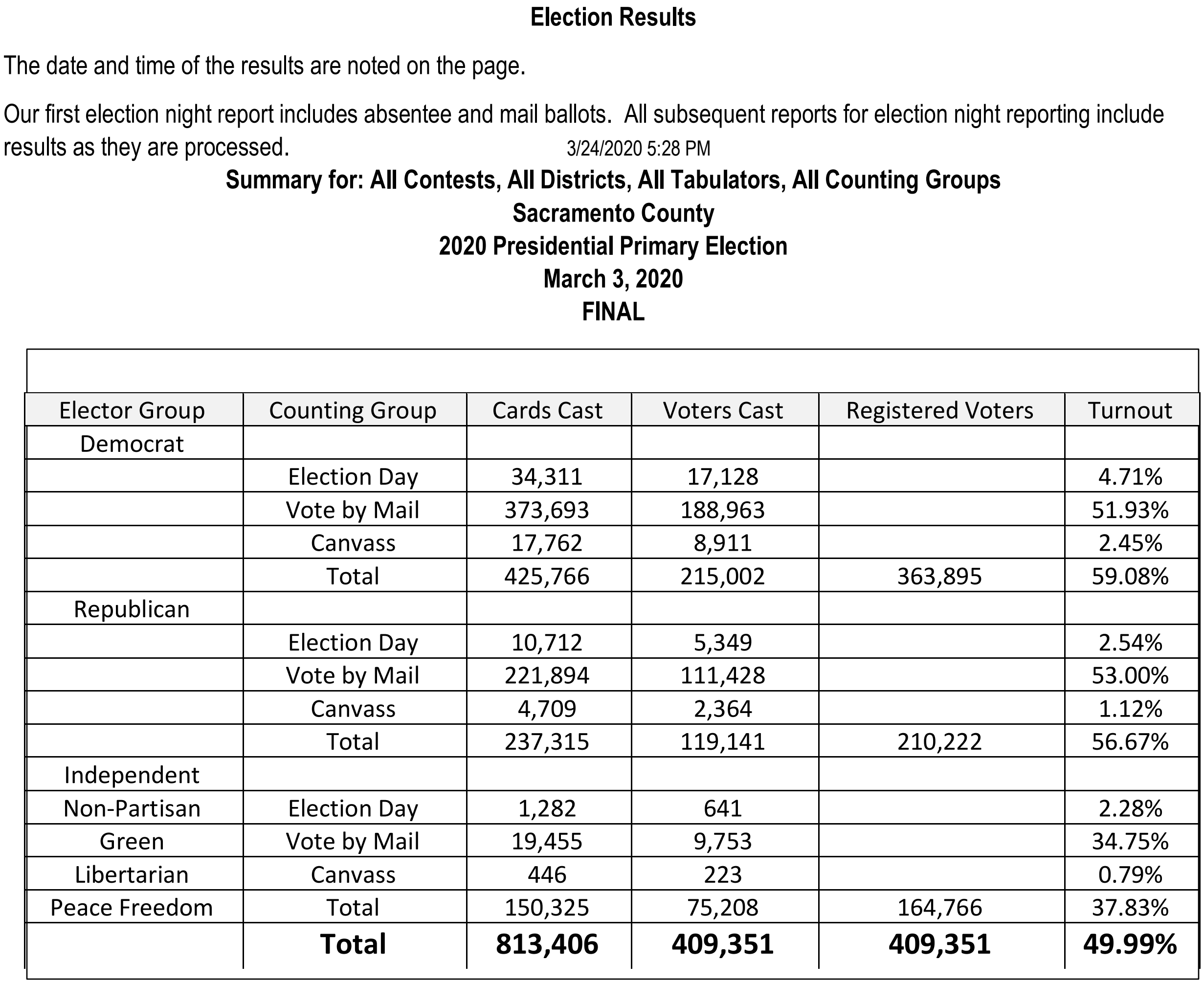
Election Security in Sacramento County



ELECTION SECURITY IN SACRAMENTO COUNTY



Election Results

The date and time of the results are noted on the page.

Our first election night report includes absentee and mail ballots. All subsequent reports for election night reporting include results as they are processed. 3/24/2020 5:28 PM

Summary for: All Contests, All Districts, All Tabulators, All Counting Groups
Sacramento County
2020 Presidential Primary Election
March 3, 2020
FINAL

Elector Group	Counting Group	Cards Cast	Voters Cast	Registered Voters	Turnout
Democrat					
	Election Day	34,311	17,128		4.71%
	Vote by Mail	373,693	188,963		51.93%
	Canvass	17,762	8,911		2.45%
	Total	425,766	215,002	363,895	59.08%
Republican					
	Election Day	10,712	5,349		2.54%
	Vote by Mail	221,894	111,428		53.00%
	Canvass	4,709	2,364		1.12%
	Total	237,315	119,141	210,222	56.67%
Independent					
Non-Partisan	Election Day	1,282	641		2.28%
Green	Vote by Mail	19,455	9,753		34.75%
Libertarian	Canvass	446	223		0.79%
Peace Freedom	Total	150,325	75,208	164,766	37.83%
	Total	**813,406**	**409,351**	**409,351**	**49.99%**

Source: Election Results Sacramento County Website

SUMMARY

In 2010, hackers hijacked San Mateo's Registrar of Voters Election website and in 2016 cyberthieves successfully breached several employee email accounts using phishing techniques. A 2018-19 San Mateo County Grand Jury (SMCGJ) report, "Security of Election Announcements," focused on the vulnerabilities of their county's email and online communication platforms to hijacking and propagating disinformation in the guise of election instructions and/or announcements, and included a series of recommendations which proposed short-term fixes to address the immediate risk to upcoming elections and longer-term changes to assess the broader cybersecurity threats to election information.

In 2019, the Sacramento County Grand Jury (SCGJ) received a citizen inquiry regarding whether Sacramento's Voter Registration System could benefit from the recommendations adopted in San Mateo. The SCGJ forwarded this report to the Sacramento County Registrar of Voters (SCRV) to ask if these recommendations applied to Sacramento and, if so, whether they were being implemented. The SCGJ found that most of the San Mateo recommendations had either been adopted by or were in the process of being adopted by the Sacramento County Department of Technology (DTech) and the Voter Registration and Elections Department (VRE).

However, the SCGJ also determined that DTech was not regularly performing vulnerability scans and penetration testing of Sacramento County information technology systems. We, therefore, recommend that DTech develop a plan to perform regular vulnerability scans and penetration testing.

BACKGROUND

In 2008 after a $1 million comprehensive review of the voting system, the Secretary of State of California decided that several of California's electronic voting machines were faulty and required that all electronic voting machines must leave a paper trail. VRE uses a state-of-the-art paper ballot system and an air gap computer system to tally results. Air gapping is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.

The 2016 Voter's Choice Act dramatically changed the voting process in California. The 2020 Primary Election is the second time the new process has been used in Sacramento County and the first time for most of the other counties in California, giving Sacramento County a lead role in implementation both in the U.S. and statewide. The Department of Homeland Security's (DHS) website notes, "A secure and resilient electoral process is a vital national interest and one of our highest priorities." A 2018-19 SMCGJ report focused on the vulnerabilities of its county's email and online communication platforms to hijacking and propagating disinformation in the guise of election instructions and/or announcements and issued a series of recommendations to strengthen the security of its Voter Registration system. The report concluded with findings and recommendations which represented short-term fixes to address the immediate risk to upcoming elections and longer-term changes to assess the broader cybersecurity threats to election information.

In 2019, the SCGJ received an inquiry regarding the Sacramento Voter Registration System and whether it had or needed to adopt the same kinds of recommendations that were presented to San Mateo County. SCRV was provided a copy of the report and was requested to provide an assessment and determination regarding the applicability of the San Mateo County recommendations to Sacramento and, if appropriate, plans for remediation.

VRE invited DTech to conduct a series of meetings to assess the recommendations, and if necessary, the plans for remediation. VRE collated their joint recommendations and provided the summary of actions taken or contemplated to the SCGJ. That comparative summary is included in the “Discussion” section.

METHODOLOGY

The SCGJ interviewed both senior and line staff of the VRE, the SCRV, DTech and CyberDefenses. It also reviewed system documentation, including the system's assessment of recommendations and actions, and conducted onsite reviews of the VRE and their onsite information technology system. VRE and DTech currently have a contract with CyberDefenses, Inc. to evaluate information technology security throughout Sacramento County. SCGJ had a team onsite at the VRE offices during the March 3, 2020, primary election during which time a question and answer session was held with the SCRV, two employees of DTech and the managing director of CyberDefenses, Inc.

DISCUSSION

In response to the Grand Jury's inquiry, the SCRV, in cooperation with DTech conducted a series of meetings in 2019 to determine how Sacramento County's Voter System measured up to the standards as documented in the SMCGJ 2018-2019 Report "Security of Election Announcements."

The SCGJ reviewed the recommendations adopted by and actions taken by the VRE and DTech to determine the security of the current system and to determine if further recommendations or actions were required. The Grand Jury found that most of the San Mateo County recommendations had either been adopted by or were in the process of being adopted by the DTech and the VRE.

The SCGJ’s decision to initiate this investigation may have helped bring the deficiency of multi-factor authentication forward as a threat to the current election cycle. A series of meetings with the department heads of DTech and VRE to address all the concerns of the SMCGJ report was undertaken. The implementation of Domain-based Message Authentication Reporting and Conformance (DMARC) may also have been accelerated because of the inquiry. DMARC limits the ability of hackers to use phishing techniques to steal passwords and other personal information to breach computing systems. The SCGJ was unable to determine when the last external audit was done to evaluate the security of Sacramento County Election systems or what entity had done the penetration testing.

SMCGJ's proposed security measures outlined in the table below are technical in nature. They were divided by the Sacramento County Grand Jury into categories for ease of presentation.

- Security measures 1, 2: Address the need to update the County's election security policies and to publish the revised results.
- Security measure 3: Addresses DMARC, (Domain-based Message Authentication, Reporting and Conformance) an email authentication, policy, and reporting protocol It verifies linkage to the author ("From") domain name to ensure that the sender is properly identified and helps improve and monitor the protection of the domain from fraudulent email.
- Security measures 4 - 9: Address the management of account passwords and the enforcement of the County of Sacramento supported multi-factor authentication methods. Cell phones are specifically excluded as the SIM cards can be switched between phones.
- Security measures 10, 11, 12: The Election Security Working Group identifies and addresses security concerns for all aspects of the election system. A cyber hygiene awareness program is being implemented this year to educate and train new hires as well as existing staff in safe online practices.

SMCGJ Report

Proposed Security Measures	**VRE and DTech Responses**
1: Incorporate Communications into Election Security Definition: VRE should adopt a policy that defines election security to include the security of the VRE website, VRE staff email accounts, social media accounts used for VRE announcements, and other platforms VRE uses for publishing election announcements.	Policy adjustments are in progress to specifically call out security controls for election systems that deal with communications, registration, vote casting and results from the tabulation. Estimated completion June 30, 2020.
2: Publish Updated Security Policy: VRE should update the VRE website's written	Written descriptions of election security for VRE websites are in development.

descriptions of the election security to incorporate the policy resulting from R1 on the security of election communications in addition to the current focus on the security of (a) registration, (b) vote casting, and (c) election results. .	These descriptions will call out security controls for election systems that deal with communications, registration, vote casting and results from tabulation in an appropriate format for external dissemination. Estimated completion by March 15, 2020.
3: Prevent Spoofing with DMARC. DTech, the Communication and Media Office (CMO), and VRE should improve email security for employees involved in election announcements by configuring and enabling DMARC for at least the smcvre.org and smcgov.org domains.	DMARC is now fully implemented in all Sacramento County email domains.
4: Combat VRE Email Account Phishing with FIDO Keys: VRE should provide FIDO physical security keys to each of its permanent elections employees and require the use of those FIDO keys as part of their multi-factor authentication for accessing their County email accounts.	The County of Sacramento has begun a county-wide employee and contractor initiative to implement Duo to provide Multi-Factor Authentication for systems and applications. FIDO tokens are an available option but are not enforced as the only authentication method. The County of Sacramento will support the following: Duo multi-factor authentication types Duo Push, U2F (FIDO) and tokens (limited to Duo application and organizational desk phones). Cell phone texting and call verification methods are blocked to prevent SIM swapping. This project is currently in a limited pilot and is being rolled out in segments over 16 months, with critical infrastructure and

	departments like VRE deploying first.
5: Fast Identity Combat Other Email Account Phishing with FIDO keys: VRE should identify County employees outside of VRE that have a role in election announcements (e.g., Chief Communications Officer, senior DTech employees, etc.) and ask that the departments of the identified employees provide FIDO physical security keys to each of the identified employees and require the use of those FIDO keys as part of their multi-factor authentication for accessing their County email accounts.	The County of Sacramento has begun a county-wide employee and contractor initiative to implement Duo to provide Multi-Factor Authentication for systems and applications. FIDO tokens are an available option but are not enforced as the only authentication method. The County of Sacramento will support the following: Duo multi-factor authentication types Duo Push, U2F FIDO and tokens (limited to Duo application and organizational desk phones). This project is currently in a limited pilot and is being rolled out in segments over 16 months, with critical infrastructure and departments like VRE deploying first. VRE should complete this recommendation by December 31, 2020
6: Combat Island Hopping with FIDO key Vendor Requirement: VRE and DTech should require employees and contractors of any vendor that hosts the VRE website to use FIDO physical security keys as part of their multi-factor authentication.	The County of Sacramento has begun a county-wide employee and contractor initiative to implement Duo to provide Multi-Factor Authentication for systems and applications. FIDO tokens are an available option but are not enforced as the only authentication method. The County of Sacramento will support the following: Duo multi-factor authentication types Duo Push, U2F FIDO and tokens (limited to Duo application and organizational desk phones). This project is currently in a limited pilot and is being rolled out in segments over 16

	months, with critical infrastructure and departments like VRE deploying first.
7: Stop Sharing Social Media Account Passwords: VRE and Communication and Media Office (CMO) should implement procedures whereby communications staff manage official County social media accounts with multi-user administration, and no employees share social media account passwords.	Social Media Accounts are managed by the CMO and adhere to the County of Sacramento Social Media Policy. This policy is currently under review to address the management of account passwords and the enforcement of the County of Sacramento supported multi-factor authentication methods. The estimated completion date of January 15, 2021.
8: Request FIDO key Feature If Not Available: VRE and CMO should jointly draft and send a FIDO key feature request citing this report to the social media companies used by the County to broadcast election announcements, but that do not currently offer FIDO account security protections—especially Instagram and Nextdoor.	Social Media Accounts are managed by the CMO and adhere to the County of Sacramento Social Media Policy. This policy is currently under review to address the management of account passwords and the enforcement of the County of Sacramento authentication methods. The estimated completion date is June 30, 2020. Additionally, due to the limitations and diversity of Social Media Accounts authentications, a review of Social Media Management software will be conducted. The estimated completion date is January 15, 2021
9: Combat VRE Social Media Account Phishing with FIDO Keys: VRE should require any employee social media accounts capable of administering the official VRE social media pages listed in	Social Media Accounts are managed by the CMO and adhere to the County of Sacramento Social Media Policy. This policy is currently under review to address the management of account

Table 1 to use FIDO physical security keys as part of their multifactor authentication.	passwords and the enforcement of the County of Sacramento supported multi-factor authentication methods. The estimated completion date is June 30, 2020. Additionally, due to the limitations and diversity of Social Media Accounts authentications, a review of Social Media Management software will be conducted. The estimated completion date is January 15, 2021
10: Coordinate Election Security with Interdepartmental Working Group: VRE and DTech should create an election security working group that meets periodically and is responsible for evaluating and improving the security of elections (a) registration, (b) vote casting, (c) results from tabulation, and (d) communication within San Mateo County.	The County of Sacramento holds monthly meetings between the VRE department, infrastructure support teams and information security teams. This Election Security Working Group identifies and addresses security concerns for all aspects of the election system. Additionally, this group leverages independent security consultants to audit security control effectiveness and recommend improvements.
11: Evaluate Free DHS Elections Security Assistance Programs: VRE and DTech election security working group should evaluate the benefits of having all members of the election security working group participate in any of the free DHS elections security assistance programs listed in Table 2.	A vendor is scheduled to audit the next election from a people process and technology standpoint. A DHS assessment is in the roadmap after another organizational segment completes its audit. Report back by September 30, 2020

12: Offer Behavioral Cyber Hygiene Audits: DTech and the County Controller's Office should develop a behavioral auditing program consisting of sampling the day-to-day routines and security practices of employees, contractors, and/or vendors and offer to audit each department within the County periodically to (1) evaluate compliance with existing cyber hygiene policies and (2) provide proactive advice on cyber hygiene improvements that could inform new policies.	In support of the County's focus on cybersecurity, a new cyber awareness program is being rolled out this year to educate, evaluate, and enhance its security posture. This program includes activities like new hire training, annual computer-based training, site visits, promotional poster and email distributions, and cyber hygiene audits. Report back by September 30, 2020

FINDINGS

F1. Sacramento County Department of Technology (DTech) is not currently practicing regular, consistent vulnerability scans and penetration testing. Vulnerability scanning and penetration testing are often confused. The two security procedures are quite different and are used for different purposes. At the most basic level, vulnerability scanning aims to identify any systems that are subject to known vulnerabilities while a penetration test aims to identify weaknesses in specific system configurations and organizational processes and practices that can be exploited to compromise security.

F2. Voter Registration and Elections Department (VRE) considers election security a major concern and has given it a very high priority. The Sacramento County Registrar of Voters (SCRV) and her staff were very cooperative and began almost immediately to implement changes and corrective measures for identified shortcomings.

F3. Media policy is currently under review to address the management of account passwords and the enforcement of the County of Sacramento supported multi-factor authentication methods. The estimated completion date is June 30, 2020. Social Media Accounts are managed by the Communication and Media Office (CMO) and adhere to the County of Sacramento Social Media Policy.

Due to the limitations and diversity of Social Media account authentications, a review of Social Media Management software will be conducted by the Sacramento County Department of Technology (DTech). The estimated completion date is January 15, 2021.

F4. Sacramento County Department of Technology (DTech) has begun a 16-month county-wide initiative to implement multi-factor authentication. Multi-factor authentication is one of the best deterrents to keep unauthorized users from hacking into computer networks. Voter Registration and Elections Department (VRE) will be one of the first departments to deploy this methodology.

RECOMMENDATIONS

R1. Sacramento County Grand Jury (SCGJ) recommends the Sacramento County Department of Technology (DTech) institute frequent penetration testing performed by a third party twice per year at a minimum. SCGJ further recommends DTech perform vulnerability scans each time the following occurs within the IT ecosystem.

- Security patches are applied,
- Significant changes are made to the infrastructure or network,
- New infrastructure or web applications are added,
- An office location changes, or an office is added to the network.

R2. Sacramento County Grand Jury (SCGJ) recommends the Communication and Media Office (CMO) adjust its election security policy to include security of the Voter Registration and Elections Department (VRE) website, communication, registration, voting and results from tabulation by June 30, 2020 in preparation for the November 2020 general election.

R3. Sacramento County Grand Jury (SCGJ) recommends that the Sacramento County Department of Technology (DTech) and Voter Registration and Elections Department (VRE) need to implement multi-factor authentication procedures before the November 2020 general election.

R4. Sacramento County Grand Jury (SCGJ) requests that the Sacramento County Department of Technology (DTech) report back to the SCGJ the results of the CyberDefenses, Inc. review and the U.S. Department of Homeland Security (DHS) audit of the election security by September 30, 2020.

GLOSSARY

CMO:	Communication and Media Office
DHS	U.S. Department of Homeland Security
DMARC	Domain-based Message Authentication Reporting and Conformance
Duo	Multi-factor authentication and device trust security platform
DTech	Sacramento County Department of Technology
FIDO	Fast Identity Online Alliance
Multi-factor Authentication	Proof of identity at login using a combination of unique identifiers
Phishing	The fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.
SCGJ	Sacramento County Grand Jury
SCRV	Sacramento County Registrar of Voters
VRE	Voter Registration and Elections Department

REQUIRED RESPONSES

Pursuant to Penal Code sections 933 and 933.05 the grand jury requests responses as follows:

Responses from the following Sacramento County officials within 60 days:

- Courtney Bailey-Kanelos
  Registrar of Voters
  Voter Registration and Elections
  7000 65th Street, Suite A
  Sacramento, CA 95823

- Rami Zakaria,
  Chief Information Officer
  Department of Technology
  799 G Street
  Sacramento, CA 95814

Mail or deliver a hard copy response to:

- Hon. Russell Hom
  Presiding Judge
  Sacramento County Superior Court
  720 9th Street
  Sacramento, CA 95814

Please email a copy of this response to:

- Paul Thorn
  Jury Commissioners
  ThornP@saccourt.ca.gov

- Ms. Erendira Tapier-Bouthillier
  Grand jury
  TapiaE@saccourt.ca.gov

INVITED RESPONSES

- Janna Haynes
  County Communication and Media Office
  c/o Voter Registration and Elections
  7000 65th Street, Suite A
  Sacramento, CA 95823

Mail or deliver a hard copy response to:

- Hon. Russell Hom
  Presiding Judge
  Sacramento County Superior Court
  720 9th Street
  Sacramento, CA 95814

Please email a copy of this response to:

- Paul Thorn
  Jury Commissioner
  ThornP@saccourt.ca.gov

- Ms. Erendira Tapia-Bouthillier
  Grand Jury
  TapiaE@saccourt.ca.gov

Reports issued by the Grand Jury do not identify individuals interviewed. Penal Code section 929 requires that reports of the Grand Jury not contain the name of any person or fact leading to the identity of any person who provides information to the Grand Jury.

DISCLAIMER

One Grand Juror was recused from participating in all aspects of the investigation, including interviews, deliberations, and the writing and the approval of this report due to that Grand Juror's service as an election clerk in Sacramento County.