DRAFT LETTERS

[Updated Sunday, 3/12 with minor changes to the previous Friday, 3/10 version: three changes to the first two letters and one to the last letter, all shown using underline & ~~strikeout~~.]

Letter #1 (to California Secretary of State)

EMAIL TO: votingsystems@sos.ca.gov

March 15, 2023

The Honorable Shirley Weber
Secretary of State
1500 11th Street
Sacramento, CA 95814

RE: DVSorder privacy flaw in Dominion's voting system

Dear Secretary of State Weber:

I am writing on behalf of the San Francisco Elections Commission to seek answers to questions related to the DVSorder privacy flaw in Dominion Voting Systems' ImageCast Evolution tabulators, which your office was notified about last October. The Elections Commission voted at its March 15, 2023 meeting to authorize me to send this letter. Our questions are listed at the end.

On January 9, 2023, Dr. J. Alex Halderman of the University of Michigan wrote to the Elections Commission about the DVSorder[1] privacy flaw in Dominion's voting system that his team discovered and then informed your office about on October 10, 2022.[2] His team included Dr. Halderman, Dr. Drew Springall of Auburn University, and student researchers.

Although Dominion, the U.S. Election Assistance Commission (EAC), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), and your office were all notified by his team about the vulnerability well in advance of the November 8, 2022 election, none of these organizations notified the San Francisco Department of Elections about the vulnerability or told us that our system was vulnerable, even though it was. If the Department had been told about the vulnerability, the Department could have taken steps to protect San Francisco's voters by using one of the available mitigations.

[1] DVSorder website: https://dvsorder.org/
[2] Email from Dr. Halderman to Elections Commission, with attachment: https://sf.gov/sites/default/files/2023-02/Halderman_Email_to_Commission.pdf

The Commission invited Dr. Halderman to give a short presentation about DVSorder at our February 15, 2023 meeting during agenda item #9. The agenda item, along with Dr. Halderman's presentation, can be viewed starting 2 hours, 20 minutes, and 35 seconds into the video for the meeting.[3] The agenda packet documents for the item can be found under the agenda item on the web page for the meeting.[4] The packet documents include the email that Dr. Halderman sent to the Commission, the letter his team sent to your office in October, and a memo one of our Commissioners wrote about his findings related to DVSorder.

It appears from California's voting system certification regulations that the presence of the DVSorder privacy flaw means that Dominion's voting system did not meet California's voting system standards:[5]

> **20700. Certification of Voting Systems and Voting System Equipment.**
> (a) In deciding whether to certify, decertify, or withhold certification of a voting system, voting system procedures, or part of a voting system under Division 19 of the Elections Code, the Secretary of State shall apply the standards entitled "California Voting System Standards (October 2014)," which are hereby incorporated by reference.
> …
> **20705. Examination.**
> The Office of Voting Systems Technology Assessment of the Secretary of State's office shall conduct the examination of new voting systems seeking initial certification as well as for modified versions of systems that have been certified. The Office of Voting Systems Technology shall use a state-approved testing agency or expert technicians as provided in Division 19 of the Elections Code. The examination shall meet the standards established in the "California Voting System Standards (October 2014)."

Specifically, the system appears not to meet requirements discussed on the following three pages. On page 49, in Section 3. Usability, Accessibility, and Privacy Requirements—

> **3.1. Purpose**
> …
> The voting process must preserve the secrecy of the ballot. The voting process should preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation. If such a determination is made against the wishes of the voter, then his or her privacy has been violated.

On page 54, also in Section 3—

---

[3] Video of agenda item #9 ("Reporting of Voting System Security Issues") of February 15, 2023 Commission meeting: https://youtu.be/WZkghfligHg?t=8435

[4] February 15, 2023 meeting agenda and packet documents: https://sf.gov/meeting/february-15-2023/elections-commission-regular-meeting

[5] California Voting System Certification Regulations: https://www.sos.ca.gov/administration/regulations/current-regulations/elections/voting-system-certification-regulations

3.2.4 Privacy

The voting process must preclude anyone else from determining the content of a voter's ballot without the voter's cooperation. Privacy ensures that the voter can cast votes based solely on his or her own preferences without intimidation or inhibition.

Finally, on page 131, in Section 7. Security Requirements—

7.7.3 Electronic and Paper Record Structure

a. Electronic ballot images **shall** be recorded in a randomized order by the voting system for the election. NIST Special Publication 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators specifies techniques for the generation of random numbers that can be used to randomize the order of ballot images in a cryptographically sound way. …

Incidentally, the existence of the DVSorder privacy flaw, along with the fact that it was not caught by California's certification processes, provides another reason for California to move more quickly towards open source voting. As Dr. Halderman told the Commission at our February meeting (see starting 2:39:37 into the meeting video), this flaw would have been easy for security researchers to notice if the code were open source. Indeed, as he also told the Commission (see starting 2:26:15 into the video), the random number generator used by the Dominion system is a linear congruential generator (LCG)[6], which ~~and~~ has been known since the 1970's to be unsuitable for cryptographic purposes.

San Francisco first expressed an interest in moving towards open source voting in 2007, with subsequent resolutions and legislation from the Board of Supervisors in 2008, 2014, 2018, 2019, and 2022. The Elections Commission has also passed several resolutions in support of open source voting, starting in 2007.

At the state level, the California Legislature adopted SB-360 ("Certification of voting systems") in 2013.[7] This legislation said, in part—

19006. It is the intent of the Legislature that:

...

(c) The Secretary of State study and encourage the development of voting systems that use nonproprietary source code and that are easy to audit.

[6] Wikipedia page for "linear congruential generator":
https://en.wikipedia.org/wiki/Linear_congruential_generator#Advantages_and_disadvantages
The page also says, "LCGs are not intended, and must not be used, for cryptographic applications …."

[7] SB-360 Certification of voting systems (2013-2014):
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB360

Also, in April 2021 California's own bipartisan Little Hoover Commission "call[ed] on the state to adopt an open source election system," writing in its executive summary:[8]

> The state currently relies on for-profit producers of election equipment. An open source system would be more transparent, save money, increase versatility for counties, and align with a state goal to use open source software across government.

Below are the questions the Elections Commission would like answers to:

- Why didn't California's testing and certification process, which includes source code review and security testing,[9] catch this error?
- How will California validate Dominion's purported fix?
- Will California improve its testing practices to determine if equipment from other vendors you might consider in the future has similar vulnerabilities? If so, how?
- Does California have a process in place to share relevant security information with local jurisdictions?
- Why did your office not share information about the vulnerability in this case? Dr. Halderman's October letter to your office specifically mentioned how San Francisco could be affected. In addition, Dominion's October 7, 2022 notification[10] to its customers didn't provide information about the privacy flaw or acknowledge that it existed, making only cryptic reference to a researcher's claim about an earlier version of the system.
- ~~By what mechanism~~ How should our Department learn about vulnerabilities like this that are reported to you in the future?

Thank you.

Sincerely,

[8] Little Hoover Commission, Report #259 (April 2021), "California Election Infrastructure: Making a Good System Better": https://lhc.ca.gov/report/california-election-infrastructure-making-good-system-better
[9] California Secretary of State Election Security page: https://www.sos.ca.gov/elections/ovsta/security
[10] Dominion's October 7, 2022 "UPDATE: Customer Notification: Cast Vote Selections" (see under agenda item #9): https://sf.gov/meeting/march-15-2023/elections-commission-regular-meeting

Letter #2 (to EAC)

U.S. Election Assistance Commission
633 3rd Street NW, Suite 200
Washington, DC 20001

To: Chairperson Christy McCormick
Vice Chair Benjamin W. Hovland
Commissioner Donald L. Palmer
Commissioner Thomas Hicks
Executive Director Steven Frid

Dear Chairperson McCormick, Commissioners, and Director Frid:

[Insert letter body below]

Letter #3 (to CISA)

[Jen Easterly is the Director of CISA, and Geoffrey Hale is the Director of CISA's Election Security Initiative.]

Cybersecurity and Infrastructure Security Agency Stop 0380
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

To: Director Jen Easterly
CC: The Honorable Dianne Feinstein
The Honorable Alex Padilla
The Honorable Nancy Pelosi
Director Geoffrey Hale

Dear Director Easterly:

[Insert letter body below]

March 15, 2023

RE: DVSorder privacy flaw in Dominion's voting system

[Insert greeting above]

I am writing on behalf of the San Francisco Elections Commission to seek answers to questions related to the DVSorder privacy flaw in Dominion Voting Systems' ImageCast Evolution tabulators, which your office was notified about last September. The Elections Commission voted at its March 15, 2023 meeting to authorize me to send this letter. Our questions are listed at the end.

On January 9, 2023, Dr. J. Alex Halderman of the University of Michigan wrote to the Elections Commission about the DVSorder[1] privacy flaw in Dominion's voting system that his team discovered and then informed your office about on September 2, 2022 (see the second paragraph of their letter to the California Secretary of State).[2] His team included Dr. Halderman, Dr. Drew Springall of Auburn University, and student researchers.

Although Dominion, the U.S. Election Assistance Commission (EAC), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), and the California Secretary of State's Office were all notified by his team about the vulnerability well in advance of the November 8, 2022 election, none of these organizations notified the San Francisco Department of Elections about the vulnerability or told us that our system was vulnerable, even though it was. If the Department had been told about the vulnerability, the Department could have taken steps to protect San Francisco's voters by using one of the available mitigations.

The Commission invited Dr. Halderman to give a short presentation about DVSorder at our February 15, 2023 meeting during agenda item #9. The agenda item, along with Dr. Halderman's presentation, can be viewed starting 2 hours, 20 minutes, and 35 seconds into the video for the meeting.[3] The agenda packet documents for the item can be found under the agenda item on the web page for the meeting.[4] The packet documents include the email and attachment that Dr. Halderman sent to the Commission, and a memo one of our Commissioners wrote about his findings related to DVSorder.

Incidentally, the existence of the DVSorder privacy flaw, along with the fact that it was caught by neither the EAC's nor California's certification processes, provides support for voting systems being open source. As Dr. Halderman told the Commission at our February meeting (see starting 2:39:37 into the meeting video), this flaw would have been easy for security researchers to notice if the code had been open. Indeed, as he also told the Commission (see starting 2:26:15 into the video), the random number generator used by the Dominion system is

[1] DVSorder website: https://dvsorder.org/
[2] Email from Dr. Halderman to Elections Commission, with attachment: https://sf.gov/sites/default/files/2023-02/Halderman_Email_to_Commission.pdf
[3] Video of agenda item #9 ("Reporting of Voting System Security Issues") of February 15, 2023 Commission meeting: https://youtu.be/WZkghfligHg?t=8435
[4] February 15, 2023 meeting agenda and packet documents: https://sf.gov/meeting/february-15-2023/elections-commission-regular-meeting

a linear congruential generator (LCG)[5], which ~~and~~ has been known since the 1970's to be unsuitable for cryptographic purposes.

The City and County of San Francisco has long been interested in moving towards open source voting. There has also been interest from the California state legislature in 2013,[6] as well as support for open source voting from the state's bipartisan Little Hoover Commission in April 2021.[7]

There is also an awareness of open source software's advantages at the federal level. For example, the U.S. Department of Defense's (DoD's) Open Source Software FAQ quotes a 2003 MITRE study saying that open source software "plays a far more critical role in the DoD than has been generally recognized... (especially in) Infrastructure Support, Software Development, Security, and Research."[8] The same DoD web page goes on to say that hiding source code does not confer any security advantages, and that open source software has conditions that reduce the risks from unintentional vulnerabilities.

The questions the Elections Commission would like answers to are as follows:

- Why did the EAC and CISA not coordinate disclosure of this vulnerability to affected jurisdictions like ours? Dominion's October 7, 2022 notification[9] to its customers didn't provide information about the privacy flaw or acknowledge that it existed, and it made only cryptic reference to a researcher's claim about an earlier version of the system.
- Why didn't EAC's certification process uncover this vulnerability?
- Can you confirm whether the vulnerability violates either or both the VVSG 1.0 and 2.0 standards? If it does not, do you think the standards should be updated to ensure that voting systems used in the United States preserve the secrecy of the ballot?
- ~~By what mechanism~~ How should our Department learn about vulnerabilities like this that are reported to you in the future?

Thank you.

Sincerely,

---

[5] Wikipedia page for "linear congruential generator": https://en.wikipedia.org/wiki/Linear_congruential_generator#Advantages_and_disadvantages
The page also says, "LCGs are not intended, and must not be used, for cryptographic applications …."
[6] SB-360 Certification of voting systems (2013-2014): https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB360
[7] Little Hoover Commission, Report #259 (April 2021), "California Election Infrastructure: Making a Good System Better": https://lhc.ca.gov/report/california-election-infrastructure-making-good-system-better
[8] DoD Open Source Software FAQ: https://dodcio.defense.gov/open-source-software-faq/#q-doesnt-hiding-source-code-automatically-make-software-more-secure
[9] Dominion's October 7, 2022 "UPDATE: Customer Notification: Cast Vote Selections" (see under agenda item #9): https://sf.gov/meeting/march-15-2023/elections-commission-regular-meeting

Letter #4 (to Dominion)

EMAIL TO: security@dominionvoting.com

March 15, 2023

Mr. John Poulos
Chief Executive Officer
Dominion Voting Systems, Inc.
1201 18th Street, Suite 210
Denver, CO 80202

RE: DVSorder privacy flaw in Dominion ImageCast Evolution (ICE) scanner

Dear Mr. Poulos:

I am writing on behalf of the San Francisco Elections Commission to seek answers to questions related to the DVSorder privacy flaw in your ImageCast Evolution tabulators, which your company was notified about last August. The Elections Commission voted at its March 15, 2023 meeting to authorize me to send this letter. Our questions are listed at the end.

On January 9, 2023, Dr. J. Alex Halderman of the University of Michigan wrote to the Elections Commission about the DVSorder[1] privacy flaw in your ImageCast Evolution equipment that his team discovered and then informed your company about on August 23, 2022 (see the second paragraph of their letter to the California Secretary of State).[2] His team included Dr. Halderman, Dr. Drew Springall of Auburn University, and student researchers.

Although the U.S. Election Assistance Commission (EAC), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the California Secretary of State's Office, and your company were all notified by his team about the vulnerability well in advance of the November 8, 2022 election, none of these organizations notified the San Francisco Department of Elections about the vulnerability or told us that our system was vulnerable, even though it was. If the Department had been told about the vulnerability, the Department could have taken steps to protect San Francisco's voters by using one of the available mitigations.

The Commission invited Dr. Halderman to give a short presentation about DVSorder at our February 15, 2023 meeting during agenda item #9. The agenda item, along with Dr. Halderman's presentation, can be viewed starting 2 hours, 20 minutes, and 35 seconds into the video for the meeting.[3] The agenda packet documents for the item can be found under the

[1] DVSorder website: https://dvsorder.org/
[2] Email from Dr. Halderman to Elections Commission, with attachment: https://sf.gov/sites/default/files/2023-02/Halderman_Email_to_Commission.pdf
[3] Video of agenda item #9 ("Reporting of Voting System Security Issues") of February 15, 2023 Commission meeting: https://youtu.be/WZkghfligHg?t=8435

agenda item on the web page for the meeting.[4] The packet documents include the email and attachment that Dr. Halderman sent to the Commission, and a memo one of our Commissioners wrote about his findings related to DVSorder.

The questions the Elections Commission would like answers to are as follows:

- Can you confirm whether the flaw exists largely as Dr. Halderman's team described?
- Will you work with researchers to validate your fix?
- Why did your October 7, 2022 notification[5] to our Department of Elections not provide information about the privacy flaw or acknowledge that it existed?
- Why have you not yet sent a more detailed advisory, now that the vulnerability is public and a fix is undergoing certification?
- Can our Department expect to find out the next time a vulnerability is reported to you that affects us?

Thank you.

Sincerely,

[4] February 15, 2023 meeting agenda and packet documents: https://sf.gov/meeting/february-15-2023/elections-commission-regular-meeting

[5] Dominion October 7, 2022 "UPDATE: Customer Notification: Cast Vote Selections" (see under agenda item #9): https://sf.gov/meeting/march-15-2023/elections-commission-regular-meeting