SHIRLEY N. WEBER, Ph.D.
CALIFORNIA SECRETARY OF STATE
Office of Voting Systems Technology Assessment | 1500 11th Street, 6th Floor
Sacramento, CA 95814 | **Tel** 916.695.1680 | www.sos.ca.gov

June 3, 2022

County Clerk/Registrar of Voters (CC/ROV) Memorandum # 22131

TO: All County Clerks/Registrars of Voters

FROM: /s/ Susan Lapsley
Deputy Secretary of State, HAVA and Counsel

RE: CISA Advisory: Dominion Democracy Suite Voting System Version 5.5A

The Cybersecurity and Infrastructure Security Agency (CISA) recently released an advisory regarding the ImageCast X (ICX) component of the Dominion Democracy Suite Voting System Version 5.5A. The ICX is an accessible ballot marking device. This advisory was in response to vulnerabilities reported to CISA by J. Alex Halderman, University of Michigan and Dre Springall, Auburn University. The official CISA advisory can be found here at CISA website - https://www.cisa.gov/uscert/ics/advisories/icsa-22-154-01 .

In the advisory, CISA identifies vulnerabilities with the ICX, that would require bad actors to have physical access to the individual devices, access to the Election Management System (EMS), or the ability to modify election files prior to them being uploaded to the ICX, to exploit such vulnerabilities. CISA states that they have no evidence that these identified vulnerabilities have been exploited in any election and has recommended mitigations for jurisdictions using the Dominion 5.5A System to prevent the exploitations of the vulnerabilities. Many of CISA's recommended mitigations are standard practice with use of the voting devices and cover technical, physical, and operational control that limit unauthorized access to the voting system, all of these are long-standing processes, procedures, and practices in California.

The California Secretary of State's Office of Voting Systems Technology Assessment (OVSTA) is charged with the testing and certification of voting technology used within the state of California. Our testing process is the most strenuous in the country, and involves a multi-phase approach consisting of the following:

1. Functional Testing
2. Accessibility, Usability, and Privacy Testing
3. Volume Testing
4. Hardware Testing
5. Software Testing / Source Code Review

6. Security Testing
7. Telecommunications Testing
8. Quality Assurance Assessment

For every system, we bring in independent security experts to do open ended vulnerability testing, penetration testing, source code review, and security testing. Through each of the phases, to the extent vulnerabilities are identified, OVSTA works with the vendors to implement process, procedural or security fixes, to mitigate those vulnerabilities. Our office publishes the findings of our testing, including vulnerabilities and mitigations on our website - https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/dominion-voting.

Dominion's Democracy Suite 5.5A voting system has never been tested or certified for use in California. Dominion Democracy Suite Voting System Version 5.10A is certified for use in California elections and is the current version that jurisdictions in California may purchase or contract for, pursuant to California Elections Code Section 19202(d). OVSTA has reviewed CISA's advisory and concluded the findings discussed are either not applicable to California as they are not resident on version 5.10A or they have already been identified by us through our testing and mitigations are in place. Specifically, of the nine findings by CISA, seven are not applicable to California because they are not resident on version 5.10A. Those that are not applicable are:

1. Improper Verification of Cryptographic Signature
2. Hidden Functionality
3. Improper Protection of Alternate Path
4. Traversal: '../filedir'
5. Execution with Unnecessary Privileges
6. Incorrect Privilege Assignment
7. Origin Validation Error

The remaining two findings were previously identified through the Secretary of State's testing and certification. Mitigations were put into place as part of our certification:

1. Mutable Attestation or Measurement Reporting Data. The tested version of ImageCast X's on-screen application hash display feature, audit log export, and application export functionality rely on self-attestation mechanisms. An attacker could leverage this vulnerability to disguise malicious applications on a device. In California we require that a third-party HASH utility be utilized to validate voting systems to mitigate the finding.

2. Authentication Bypass by Spoofing. The authentication mechanism used by technicians on the tested version of ImageCast X is susceptible to forgery. An attacker with physical access may use this to gain administrative privileges on a device and install malicious code or perform arbitrary administrative actions. In California we require strict polling place and physical security procedures, and the

use of the Election Event Designer (EED) to create individual passwords for technician cards to mitigate the finding.

As part of the advisory, CISA recommends election officials implement specific mitigations to further enhance defensive measures to reduce the risk of exploitation of the vulnerabilities mentioned in the report. For each CISA recommendation, the California Secretary of State has a matching requirement or mitigation already in place. The CISA recommended mitigations and their corresponding SOS requirement and/or mitigation are as follows:

1. Contact Dominion Voting Systems to determine which software and/or firmware updates need to be applied. Dominion Voting Systems reports to CISA that the above vulnerabilities have been addressed in subsequent software versions.
    - As identified above, California uses version 5.10A and the findings are either not applicable to California as they are not resident on version 5.10A or they have already been identified by us through our testing and mitigations are in place.

2. Ensure all affected devices are physically protected before, during, and after voting.
    - This is standard practice in California and required by the California Voting System Standards (CVSS).

3. Ensure compliance with chain of custody procedures throughout the election cycle.
    - Jurisdictions are required to follow strict chain of custody procedures before, during and after an election. This is a best practice and a required condition of certification.

4. Ensure that ImageCast X and the Election Management System (EMS) are not connected to any external (i.e., Internet accessible) networks.
    - Pursuant to Elections Code Section 19205, no part of a voting system shall be connected to the internet at any time. Our testing verifies that systems do not connect or have the capability to connect to the internet.

5. Ensure carefully selected protective and detective physical security measures (for example, locks and tamper-evident seals) are implemented on all affected devices, including on connected devices such as printers and connecting cables.
    - This is a standard practice in California and required by the California Voting System Standards (CVSS), system Use Procedures and certification.

6. Close any background application windows on each ImageCast X device.
    - This is a standard practice in California and required by the California Voting System Standards (CVSS).

7. Use read-only media to update software or install files onto ImageCast X devices.
    - This is a standard practice in California and required by the California Voting System Standards (CVSS).

8. Use separate, unique passcodes for each poll worker card.
    - This is a standard practice in California and required by the California Voting System Standards (CVSS).

9. Ensure all ImageCast X devices are subjected to rigorous pre- and post-election testing.
    - California Elections Code section 15000 requires logic and accuracy testing no later than seven days prior to any election. As a part of this testing, the elections official shall conduct a test or series of tests to ensure that every device used to tabulate ballots accurately records each vote. Additionally, as a safeguard to ensure votes are accurately read and tallied, county elections officials are required by law to conduct a manual tally of one percent of the precincts or a risk limiting audit as part of the official canvass of election results.

10. Disable the "Unify Tabulator Security Keys" feature on the election management system and ensure new cryptographic keys are used for each election.
    - This is a standard practice in California and required by the California Voting System Standards (CVSS).

11. As recommended by Dominion Voting Systems, use the supplemental method to validate hashes on applications, audit log exports, and application exports.
    - Our office generates HASH values during the Trusted Build process, utilizing third party utilities, and provides verification to jurisdictions. In addition, jurisdictions are encouraged to perform post-election HASHing.

12. Encourage voters to verify the human-readable votes on printout. NOTE: this mitigation is not applicable if the ImageCast X is used in paperless direct recording electronic (DRE) mode.

    - Voters in California receive a paper ballot, with selections printed in human-readable format. Voters with visual disabilities can have their selections read to them, using the accessible features of the ballot marking device.

13. When barcodes are used to tabulate votes, they may be subject to attacks exploiting the listed vulnerabilities such that the barcode is inconsistent with the human-readable portion of the paper ballot. To reduce this risk, jurisdictions

should, where possible, configure the ImageCast X to produce traditional, full-face ballots, rather than summary ballots with QR codes.

- ImageCast X ballots are printed in human-readable format in California. All barcodes and QR codes are tested and verified to match the human-readable text. In addition, where they are used for tabulation the following is required:
  - Jurisdictions shall develop procedures and conduct training for poll workers, prior to every election, regarding voter verification of barcodes or QR codes used for tabulation.
  - In conducting pre-election testing pursuant to Elections Code section 15000, the jurisdiction shall validate the logic and accuracy of the barcodes or QR codes used for tabulation. In conducting a one percent manual tally pursuant to Elections Code section 15360 or a risk limiting audit pursuant to Elections Code section 15367, the jurisdiction shall perform a further review of any ballot examined pursuant to those sections that contains a barcode or QR code used for tabulation. The further review shall verify that the information contained in the QR code or barcode matches the voter verified, human readable text.

14. Conduct rigorous post-election tabulation audits of the human-readable portions of physical ballots and paper records, to include reviewing ballot chain of custody and conducting voter/ballot reconciliation procedures.

- County elections officials are required by law to conduct a manual tally of one percent of the precincts or a risk-limiting audit as part of the official canvass of election results.

Jurisdictions seeking additional technical information, documentation or further guidance regarding this information should contact OVSTA at (916) 695-1680 or votingsystems@sos.ca.gov.