NEW YORK STATE Board of Elections

40 NORTH PEARL STREET, SUITE 5
ALBANY, N.Y. 12207-2109

Douglas A. Kellner
Co-Chair

MEMORANDUM

To: **Peter S. Kosinski**
Andrew J. Spano
Gregory P. Peterson

From: **Douglas A. Kellner**

Date: **March 7, 2019**

Subject: **Dominion ImageCast Evolution 4.14.25**

Two respected professors of computer science have provided reports that the Dominion ImageCast Evolution voting machine has a "design flaw." Andrew W. Appel, the Eugene Higgins Professor of Computer Science in the Department of Computer Science at Princeton University,[1] has written, "***after you mark your ballot, after you review your ballot, the voting machine can print more votes on it!***"[2] (emphasis in original). Richard A. DeMillo, Charlotte B. and Roger C. Warren Distinguished Professor of Computing in the Department of Computer Science at the Georgia Institute of Technology,[3] has opined that Professor Appel has identified "a vulnerability in Dominion's ICE and that--absent a thorough and convincing design and code review--there is no way to be confident that the system is immune from the ballot stuffing attack he describes."

Election Law § 7-201 requires that the State Board of Elections examine and approve each type of voting machine or voting system before it can be used in New York State. The examination criteria for certification of voting equipment are set forth in Regulation 6209.6.[4] The regulation requires that the vendor include detailed documentation regarding software security:

---

[1] https://www.cs.princeton.edu/~appel/
[2] https://freedom-to-tinker.com/2018/10/16/design-flaw-in-dominion-imagecast-evolution-voting-machine/
[3] https://www.cc.gatech.edu/people/richard-demillo
[4] 9 NYCRR § 6209.6

> Security requirements and security provisions of the system's software shall be identified for each system function and operating mode. The voting system must be secure against attempts to interfere with correct system operation. The vendor shall identify each potential point of attack. For each potential point of attack, the vendor shall identify the technical safeguards embodied in the voting system to defend against attack, and the procedural safeguards that the vendor has recommended be followed by the election administrators to further defend against that attack. Each defense shall be classified as preventative, if it prevents the attack in the first place; detective if it allows detection of an attack; or corrective if it allows correction of the damage done by an attack. Security requirements and provisions shall include the ability of the system to detect, prevent, log and recover from the broad range of security risks identified. These procedures shall also examine system capabilities and safeguards claimed by the vendor to prevent interference with correct system operations. The State Board, with the assistance of its ITA, shall conduct tests to confirm that the security requirements of these Regulations have been completely addressed. Notwithstanding any other provisions of these Regulations, the State Board shall determine whether all or a portion of such security requirements and security provisions shall be available for public inspection, but shall exclude any information which compromises the security of the voting system.[5]

In particular, "the vendor shall identify each potential point of attack," and "for each potential point of attack, the vendor shall identify the technical safeguards embodied in the voting system to defend against attack."

I have carefully reviewed Dominion's "Democracy Suite System Security Specification" version 4.14E::436, which I understand was used to satisfy the documentation required by Regulation § 6209.6(f)(3)(xiv). I do not see anything in the submission that addressed the point of attack or threats identified by Professors Appel and DeMillo.

In addition Regulation § 6209(e) provides that:

> Prior to certifying a voting system, the state board shall designate an independent expert to review, all source code made available by the vendor pursuant to this section and certify only those voting systems compliant with these Regulations. At a minimum, such review shall include a review of security, application vulnerability, application code, wireless security, security policy and processes, security/privacy program management, technology infrastructure and security controls, security organization and governance, and operational effectiveness, as applicable to that voting system.

It is my understanding that SysTest Labs Inc. (SLI) was retained to conduct the required security review as well as the review of source code required by the

[5] 9 NYCRR § 6209.6(f)(3)(xiv)

State Board's regulation. New York State Technology Enterprise Corporation (NYSTEC) was designated to review the test plans and to verify the security requirements reviewed by SLI. Both SLI[6] and NYSTEC[7] issued reports for the State Board that formed the basis for the State Board's approval and certification of the Dominion ImageCast Evolution optical scan voting system.[8] None of these reports, however, addressed the vulnerabilities described by Professors Appel and DeMillo.

Election Law § 7-202(1)(j) requires that every voting machine or system "retain all paper ballots cast or produce and retain a voter verified permanent paper record." The provision goes on to confirm the purpose of the voter verified permanent paper record: "such ballots or record shall allow a manual audit." Election Law § 9-211, also added as part of the Election Reform and Modernization Act of 2005,[9] sets forth the requirement for a random audit of the voter verifiable records. Every expert regarding computer security recognizes that it is literally impossible to prevent all potential threats of the installation of malware that could alter the operation of equipment used to count votes. Indeed, both the SLI and NYSTEC reports acknowledge that possibility. One of the principal mitigations to these malware threats is the audit of the voter verified paper ballots.

If there is a serious possibility that an insider could install malware that could program the printer to add marks to a ballot without the possibility of verification by the voter, then the entire audit process is compromised and circumvented. If it was possible for the machine to add a voting mark to the ballot without verification by the voter, the audit is not meaningful because it cannot confirm that the ballot was counted in the manner intended by the voter.

At a meeting of the Budget & Appropriations Committee of the Westchester County Legislature, Dominion spokesman Gio Constantiello explained that a blind voter, after using the ImageCast Evolution as a ballot marking device has the option to eject the ballot for inspection and then reinsertion, or alternatively to cast the ballot without ejecting it.[10] Professor Appel notes that this means that the software has a mode to cast a ballot into the ballot box directly from the printer without verification by the voter. SLI's source code review does not indicate that it examined whether the ballot configuration software could trigger this mode without the need to install malware that would alter the operating system.

---

[6] "NYSBOE Dominion Source Code Review Findings ImageCast Evolution Only" and "NYSBOE Dominion Security, Accessibility and TDP Review ImageCast Evolution Only"

[7] "NYSTEC Review of the Dominion ImageCast Evolution 4.14.25 SBOE Upgrade Testing"

[8] State Board Resolution 18-13, adopted October 25, 2018

[9] L. 2005, c. 181

[10] Minute 42 of the video posted at: http://westchestercountyny.iqm2.com/Citizens/SplitView.aspx?Mode=Video&MeetingID=5245

Election Law § 7-201(3) provides that:

> If at any time after any machine or system has been approved,…the state board of elections has any reason to believe that such machine or system does not meet all the requirements for voting machines or systems set forth in this article, it shall forthwith cause such machine or system to be examined again.

In view of the omission of the security threats identified by Professors Appel and DeMillo in the submission by Dominion in support of its application for certification of the ImageCast Evolution, and in view of the absence of any analysis of this issue in the SLI and NYSTEC reports, I request that the Election Operations Unit of the State Board examine again the ImageCast Evolution to consider the vulnerability of the voting system because the printer could be programmed to add marks to ballots without verification by the voter, and that SLI and NYSTEC supplement their reports with respect to these issues.

Copies To: **Robert A. Brehm**
Todd D. Valentine
Thomas E. Connolly
Brendan M. Lovullo