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

September 23, 2024

The Honorable Bryan Steil
Chairman
Committee on House Administration
1309 Longworth House Office Building
Washington, D.C. 20515

Dear Chairman Steil:

Thank you for your September 13, 2024, letter to the U.S. Election Assistance Commission (EAC) Chair Ben Hovland and Vice Chair Donald Palmer regarding *DeKalb County Republican Party, Inc. v. Brad Raffensperger*.[1] While the Help America Vote Act of 2002 (HAVA) limits EAC authority as primarily voluntary, the EAC continues to provide all allowable assistance to election officials and voters. We appreciate your continued oversight and will provide any technical information as the Committee requires.

The Voluntary Voting System Guidelines (VVSG) are a set of specifications and requirements against which voting systems can be tested to determine if they meet required standards. Factors examined under these tests include functionality, accessibility, and security capabilities. While HAVA mandates the EAC to develop and maintain these requirements, adhering to the VVSG is voluntary except in select states where it is required by their own state law.[2]

A voting system receives EAC certification when the system has been tested by a federally accredited voting system test laboratory (VSTL) and has successfully met the requirements of the VVSG and any other claims made by the voting system manufacturer. The EAC issues a certification once all steps required by the program have been completed. EAC certification of a voting system does not expire, and a system can only lose its certification if the EAC formally decertifies it.

To assist in your review, you have asked the EAC to answer several questions. Each question is restated below and addressed individually.

1. What are encryption keys, and what role do they play in safeguarding voting machines from ballot tampering or other interference?

   Encryption keys are utilized by the Dominion Democracy Suite 5.5-A voting system to ensure that data stored and transmitted both internal and external to the system are encrypted, making it unreadable to unauthorized parties. This prevents malicious actors from accessing

[1] *See DeKalb County Republican Party, Inc. v. Brad Raffensperger*, No 24-cv-011028 (Ga. Sup. Ct. Aug. 30, 2024) ("Complaint").
[2] Help America Vote Act of 2002," (HAVA), Pub. L. No. 107-252, 116 Stat. 1666 (2002).

or manipulating system data. The Dominion Democracy Suite 5.5-A voting system utilizes a Federal Information Processing Standards (FIPS) 140-2 cryptographic module for transmission of data between system components as required by the Voluntary Voting System Guidelines 1.0 (VVSG 1.0).

2. Would releasing voting-machine encryption keys through public information requests violate any aspect of the EAC's best-practices protocol or the "Voluntary Voting System Guidelines" ("VVSG")?

   The EAC has no authority to dictate state sunshine or public records laws. Further, the EAC cannot provide legal guidance to states on how to respond to state public records requests. However, as a result of an influx of records requests to local election offices in 2020, the EAC collected best practices from across the country. Additionally, the EAC receives regular inquiries from state and local election officials regarding Federal records protections for personal information. In response to these inquiries, the EAC compiled information to provide Federal practices for protecting personal or sensitive information in the context of public records requests.

   The EAC's best practices for election technology references key management on page three. It is important to establish and follow procedures to ensure that all encryption keys are properly managed, including following all state, manufacturer, or IT department guidance and best practices. Well-defined policies and procedures should be used to control access to the voting system, the circumstances under which users can access the system, and the functions users are allowed to perform. These procedures should specify that all users utilize unique login names and passwords and that they are only authorized to perform the minimum functions required to complete their duties Given that this guidance is voluntary and only a compilation of best practices, the EAC cannot view release of information under a state or local process as a violation.

   The VVSG 1.0 does not explicitly or indirectly address public information requests. Therefore, a release would not violate the VVSG.

3. Would public release of a voting-machine encryption key heighten the risk of tampering or interference with voting machines?

   The integrity and security of encryption keys are essential in ensuring the protection of data transmitted between system components. While public release of encryption keys allows for the possibility of manipulation of data specific to the election that the key is obtained from, the resulting risk should be considered in the context of timing. Encryption keys that are obtained for a specific election after ballots have been counted and the election has been certified poses negligible risk that manipulation of data will have any negative consequences on an outcome after-the-fact. Further, encryption keys should be uniquely generated per election. This best practice significantly reduces risks posed by cryptographic secrets released from a prior election.

   Defense-in-depth is employed in EAC certified voting systems which is a security strategy integrating people, technology, and operations capabilities to establish barriers across

multiple layers of the system. Voting system manufacturers must document all system features used in securing the system and mitigating cybersecurity risks. This includes administrative access controls, internal security procedures, adherence to operational procedures, security of physical facilities, and organizational responsibilities. To further mitigate risk, the EAC recommends published best practices for equipment chain-of-custody, post-election audits, voting system security measures, and the EAC's Election Management Guidelines chapters 6 and 7 on voting system security.

4. Has the EAC previously certified the Georgia voting system as compliant with the VVSG?

   Georgia utilizes Dominion Democracy Suite 5.5-A, which was certified by the EAC to VVSG 1.0 on January 19, 2019.

5. Has the EAC ever certified that Georgia is or was compliant with mandatory practices for cryptographic keys under the VVSG?

   The EAC does not have authority under HAVA to certify state processes. The EAC certifies voting systems as compliant with the VVSG, and implementation is specifically left to the states.

6. Does the EAC mandate or recommend ongoing compliance with the VVSG?

   The EAC does not have authority to mandate state compliance with VVSG. As a matter of policy, the EAC Testing and Certification division's Quality Monitoring Program (QMP) provides a set of post-certification tools to help enable the EAC to independently monitor the continued compliance of certified voting systems. The QMP methodology includes inspection of fielded systems upon invitation, or with permission of the state or local election authority.

   Effective monitoring for continued compliance with the VVSG across thousands of jurisdictions requires significant personnel and resources that have not been available to the Commission until recently. With the help of Congress, the EAC created a Field Services Program (FSP) in 2023 to assist states and local jurisdictions by providing a combination of virtual and onsite services when requested by a state. The FSP team has a deployable, full-time staff of six subject matter experts to accomplish this mission. We are enthusiastic to have this new team to assist election officials, however, the capability of the program is severely constrained by the limited number of staff. Additional funding from Congress would allow the EAC to hire more full-time employees and grow the program to effectively assist many more jurisdictions than we currently have capacity to serve.

7. If so, does the EAC play any oversight role in continuing certification of voting machines?

   The EAC does not have oversight authority once a voting machine is fielded. However, as noted above, the EAC FSP provides voluntary assistance as requested by a state. When a non-conformance to VVSG is identified in a certified and fielded system, the primary enforcement mechanism at the EAC's disposal is decertification of the system. Decertification is only used as a final resort when a manufacturer is unable or unwilling to

remediate an issue as it significantly affects state and local governments, election administrators, and the public.

8. What precautions does EAC recommend or require governments take to safeguard voting-machine encryption keys?

   The EAC best practices document on public information requests encourages state and local election officials to develop a public records policy that follows applicable state and local laws and regulations, including information that is generally made available, and denial or redaction of sensitive information. It is important to assess any potential security and privacy risks in publishing system data. The EAC recommends localities communicate directly and coordinate with state and local legal representatives on disclosing technical data in response to public records requests. The EAC also recommends that everyone in an elections office should be provided with general training on state public records laws.

9. What steps, if any, has the EAC taken to ensure state and local election officials are aware of risks to public disclosure of voting-machine encryption.

   The EAC worked with the Cybersecurity and Infrastructure Security Agency (CISA) to provide disclosure and mitigations regarding the vulnerabilities identified in the Dominion Democracy Suite 5.5-A voting system.

   Dominion submitted an updated system Democracy Suite 5.17 to the EAC for conformance testing to VVSG 1.0 which addresses vulnerabilities disclosed in the CISA advisory. Democracy Suite 5.17 was certified by the EAC on March 16, 2023.

Over the course of 2024, the EAC has worked diligently to fulfill our responsibilities under HAVA. As part of extensive preparations for the November general election, the EAC continues to meet with election officials across the country, develop guidance, offer support to election administrators, and educate voters. Commissioners and staff frequently organize and participate in conferences, meetings with stakeholder organizations, and events concerning developments that impact election administration. Jurisdictions of all sizes and in all parts of the country have emphasized the urgent need for ongoing support, including consistent and increased federal funding.

As election offices work to address evolving challenges, the EAC provides much-needed information and guidance in areas ranging from cyber- and physical security to grants assistance to poll worker support. Please do not hesitate to contact us with any additional questions or concerns that you may have.

Sincerely,

Ben Hovland
Chairman

Donald Palmer
Vice Chair