SENATE BILL REPORT
SB 5843

As of January 4, 2024

Title: An act relating to security breaches of election systems and election-related systems.

Brief Description: Concerning security breaches of election systems and election-related systems.

Sponsors: Senator Nguyen; by request of Secretary of State.

Brief History:
Committee Activity: State Government & Elections: 1/09/24.

Brief Summary of Bill

- Requires every county to install and maintain an intrusion detection system to monitor their network and to disclose certain malicious activity or breaches of security of information technology systems.
- Authorizes the Secretary of State to certify the results of an election if a county canvassing board refuses to certify the results of the election without cause.
- Establishes violations and penalties related to election interference, including prohibited interference by election observers, interference with the operation of a voting center, destruction of certain election supplies and materials, and unauthorized access to election administration locations and systems.

SENATE COMMITTEE ON STATE GOVERNMENT & ELECTIONS

Staff: Greg Vogel (786-7413)

Background: Election System Security. The Secretary of State must annually submit a report to the Governor, State Chief Information Officer, State Fusion Center, and the

---

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

Legislature on any identified instances of security breaches of election systems or election data throughout the state and provide options to increase security and prevent future security breaches. To the extent possible, the Secretary of State must identify whether the source of a security breach is a foreign or domestic entity.

County voting systems must be certified by an independent testing authority and the Secretary of State. Manufacturers or distributors of voting systems or components of voting systems certified by the Secretary of State must disclose to the Secretary of State and attorney general any breach of security of its system immediately following discovery of the breach if:

- the breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election; or
- personal information was, or reasonably believed to have been, acquired by an unauthorized person as a result of the breach and the personal information was not secured.

Shared Voter Registration System. The Secretary of State maintains a centralized statewide voter registration list that is the official list of eligible voters for all elections in the state. County auditors are the chief registrars of voters for every precinct within their county. Voter registration information received by each county auditor is electronically entered into the database.

Election Observers. County auditors must request observers be appointed by the major political parties to be present during the processing of ballots at counting centers. Auditors have discretion to also request observers be appointed by any campaigns or organizations.

Certification of Election Results. Ten days after a special election, ten days after a presidential primary, 14 days after a primary, and 21 days after a general election, a county canvassing board must complete the canvass and certify the results. Each ballot returned before 8:00 p.m. on the day of the election and each ballot postmarked on or before the date of the election and received no later than the day before certification must be included in the canvass report. Members of a county canvassing board include the county auditor, the county prosecuting attorney, and the chair of the county legislative body.

Violations and Penalties. State election laws prohibit certain acts that interfere with the administration of elections, including interfering with a voter's attempt to vote in a voting center; willfully defacing, removing, or destroying voting center supplies or materials; tampering with, damaging, or attempting to damage voting machines or devices; willful neglect or refusal to perform a duty as a person charged with election duties; and knowingly destroying, concealing, or discarding a completed voter registration form or signed ballot declaration. Depending on the violation, it may be prosecuted as gross misdemeanor or class C felony.

Class C felonies may be subject to a prison sentence not to exceed five years, a fine not to

exceed $10,000, or both. Gross misdemeanors may be subject to a prison sentence not to exceed 364 days, a fine not to exceed $5,000, or both.

Summary of Bill: Election System Security. Every county must install and maintain an intrusion detection system that passively monitors its network for malicious traffic by a qualified and trained security team with access to cyber incident response personnel who can assist the county in the event of a malicious attack. The system must support the unique security requirements of state, local, tribal, and territorial governments and possess the ability to receive cyber intelligence threat updates to stay ahead of evolving attack patterns.

A county auditor or county information technology director of any county, participating in the shared voter registration system, or operating a voting system or component of a voting system certified by the Secretary of State, must disclose to the Secretary of State and attorney general any malicious activity or breach of the security of any of its information technology systems immediately following discovery if:

- malicious activity was detected by an information technology (IT) intrusion detection system, malicious domain blocking and reporting system, or endpoint security software;
- a breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of election systems, IT systems used to manage the administration of elections, or peripheral IT systems that support the county auditor's office in day-to-day activities;
- the breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election within the state; or
- personal information of residents in any state was, or is reasonably believed to have been acquired by an unauthorized person as a result of the breach and the personal information was not secured.

For purposes of the Secretary of State's annual report on election security breaches, "domestic entity" is defined as an entity organized or formed under the laws of the United States, a person domiciled in the United States, or a citizen of the United States.

Certification of Election Results. If a county canvassing board refuses to certify the results of an election without cause, the Secretary of State may examine the records, ballots, and results of the election and certify the results of the election. The Secretary of State's certification must be completed within two business days after the certification deadline for the election after the refusal of the county canvassing board to certify the results of the election.

Violations and Penalties. During the processing of ballots, election observers are prohibited from touching any ballots, ballot materials, or election systems. Unauthorized physical contact, or access to ballots or election systems is considered a violation punishable as a class C felony.

No person may interfere with the operation of a voting center. Interfering with the operation of a voting center is a violation punishable as a gross misdemeanor. This prohibition includes unauthorized access or handling of ballots, and unauthorized access to any voting equipment or election systems and also applies to any elected officials or county staff accessing systems in any manner not required by their job function.

Any person who willfully defaces, removes, or destroys any of the supplies or materials the person knows are intended for use in an election office, ballot counting area, ballot storage area, or election system including materials and systems meant for enabling a voter to prepare their ballot is guilty of a class C felony.

Any person who willfully and without authority accesses or assists another person or entity with unauthorized access to a voting center, election office, ballot counting area, ballot storage area, or any election system, or provides unauthorized access to these locations to another person or entity, whether electronic or physical access, is guilty of a class C felony.

Any unauthorized person who accesses or assists another person or entity with unauthorized access to a voting center, election office, ballot counting area, ballot storage, or election system, voting machine, or device to be used in a primary, special, or general election is guilty of a class C felony.

Every person charged with the performance of any duty under state or local election laws, who provides unauthorized access to a person or entity to physical locations or electronic or physical access to election software or hardware used in any element of conduct of an election is guilty of a class C felony and must forfeit their office.

A person who knowingly destroys, alters, defaces, conceals, or discards a voted ballot is guilty of a gross misdemeanor. Any person who intentionally fails to return another person's voted ballot to the proper state or county elections office by the applicable deadline is guilty of a gross misdemeanor.

Appropriation: None.

Fiscal Note: Requested on January 2, 2024.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.