RCW 29A.12.180 Disclosure of security breaches—Use of intrusion detection system. (1) A manufacturer or distributor of a voting system or component of a voting system that is certified by the secretary of state under RCW 29A.12.020 shall disclose to the secretary of state and attorney general any breach of the security of its system immediately following discovery of the breach if:

(a) The breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election in any state; or

(b) 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 this subsection, "personal information" has the meaning given in RCW 19.255.010.

(2) Every county must install and maintain an intrusion detection system that passively monitors its network for malicious traffic 24 hours a day, seven days a week, and 365 days a year by a qualified and trained security team with access to cyberincident 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 cyberintelligent threat updates to stay ahead of evolving attack patterns.

(3) A county auditor or county information technology director of any county, participating in the shared voter registration system operated by the secretary of state under RCW 29A.08.105 and 29A.08.125, or operating a voting system or component of a voting system that is certified by the secretary of state under RCW 29A.12.020 shall disclose to the secretary of state and attorney general any malicious activity or breach of the security of any of its information technology (IT) systems immediately following discovery if:

(a) Malicious activity was detected by an information technology intrusion detection system (IDS), malicious domain blocking and reporting system, or endpoint security software, used by the county, the county auditor, or the county election office;

(b) A breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of election systems, information technology systems used by the county staff to manage and support the administration of elections, or peripheral information technology systems that support the auditor's office in the office's day-to-day activities;

(c) The breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election within the state; or

(d) 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 this subsection, "personal information" has the meaning given in RCW 19.255.005.

(4) For purposes of this section:

(a) "Malicious activity" means an external or internal threat that is designed to damage, disrupt, or compromise an information technology network, as well as the hardware and applications that reside on the network, thereby impacting performance, data integrity, and the confidentiality of data on the network. Threats include

viruses, ransomware, trojan horses, worms, malware, data loss, or the disabling or removing of information technology security systems.

(b) "Security breach" means a breach of the election system, information technology systems used to administer and support the election process, or associated data where the system or associated data has been penetrated, accessed, or manipulated by an unauthorized person. The definition of breach includes all unauthorized access to systems by external or internal personnel or organizations, including personnel employed by a county or the state providing access to systems that have the potential to lead to a breach.

(5) Notification under this section must be made in the most expedient time possible and without unreasonable delay. [2024 c 28 s 1; 2018 c 218 s 6.]

Intent—2018 c 218: See note following RCW 29A.60.185.