WASHINGTON SECRETARY OF STATE

Elections Division

Access to Voting System Software and Systems

Elections Clearinghouse Notice
Issue #22-05
August 12, 2022

Background

The Office of the Secretary of State has duties, pursuant RCW 29A.12.020, to inspect, evaluate, and publicly test all voting systems or components of voting systems. These reviews include verifying that the voting system conforms to federal and state laws and any regulations or standards regarding confidentiality, security, accuracy, safety, reliability, usability, accessibility, durability, resiliency, and auditability. This is in addition to the Federal testing and certification by an independent testing authority designated by the United States Election Assistance Commission (EAC).

The Help America Vote Act (HAVA) of 2002 was passed by the United States Congress to make sweeping reforms to the nation's voting process. HAVA also established the Election Assistance Commission (EAC) to assist the states regarding HAVA compliance and to distribute HAVA funds to the states. EAC is also charged with creating voting system guidelines and operating the federal government's first voting system certification program. On December 13, 2005, the EAC unanimously adopted the 2005 Voluntary Voting System Guidelines (VVSG), which significantly increased security requirements for voting systems and expanded access, including opportunities for individuals with disabilities to vote privately and independently.

In January 2017, the U.S. Department of Homeland Security designated election infrastructure as critical infrastructure under the “Government Facilities” sector, one of the 16 critical infrastructure sectors in the United States.

Voting System

RCW 29A.12.005 defines a voting system as:

1) The total combination of mechanical, electromechanical, or electronic equipment including, but not limited to, the software, firmware, and documentation required to program, control, and support the equipment, that is used:
   a) To define ballots;
   b) To cast and count votes;
   c) To report or display election results from the voting system;
   d) To maintain and produce any audit trail information; and
   e) To perform an audit under RCW 29A.60.185; and
2) The practices and associated documentation used:
   a) To identify system components and versions of such components;

b) To test the system during its development and maintenance;
c) To maintain records of system errors and defects;
d) To determine specific system changes to be made to a system after the initial qualification of the system; and
e) To make available any materials to the voter such as notices, instructions, forms, or paper ballots.

A component of a voting system can be any specific part of the voting system equipment, software, or firmware.

Third-Party Access to Voting Systems.

Demands have been made to allow third-party entities not directly involved with the conduct of elections to have access to electronic voting systems, specifically to review and copy the internal electronic, software, mechanical, logic, and related components of such systems. These demands have included the desire to image electronic memory spaces, to download operating systems and software, and to copy information that is internal and proprietary. Such access by third parties undermines chain of custody requirements and strict access limitations necessary to prevent both intentional and inadvertent tampering with electronic voting systems.

It also jeopardizes the security and integrity of those systems and will negate the ability of electronic voting system vendors to affirmatively state that such systems continue to meet security standards, are validated as not posing security risks, and are able to be certified to perform as designed by the electronic voting system vendor and as certified by both the U.S. Election Assistance Commission and the Office of the Secretary of State.

Limits on Third-Party Access to Electronic Voting Systems.

WAC 434-335-260 has been amended to clarify that:

a. County Auditors shall not provide physical, electronic, or internal access to third parties seeking to copy and/or conduct an examination of state-certified voting systems, or any components of such systems, including but not limited to: voting software and systems, tabulators, scanners, counters, automatic tabulating equipment, voting devices, servers, ballot marking devices, paper ballot printers, portable memory media devices, and any other hardware, software or devices being used as part of the voting system.

b. If access described in a. occurs, those pieces of voting equipment will be considered no longer secure or reliable to use in subsequent elections. As a result, incidents will be treated as a security breach under RCW 29A.12.180 and the Office of the Secretary of State may decertify the use of the system or component.

Voting System Replacement Costs

The Office of the Secretary of State may not reimburse the cost of replacement voting equipment for which unauthorized access was granted.

Notice

County Auditors shall notify the Secretary immediately upon receipt of any written or verbal request for third-party access to a voting system, or any component thereof.

In addition, County Auditors and voting system vendors are required by RCW 29A.12.180 to disclose of any breach or attempted breach in the chain of custody of its voting system components.

An information publication of the Certification and Training Program, Elections Division, Office of the Secretary of State, P.O. Box 40229, Olympia WA 98504-0229, (360) 902-4180 or ctsupport@sos.wa.govSin