



Security Surrounding the Trusted Build

Each vendor must deliver, or make arrangements for delivery of the “witnessed compile in an audited compilation environment,” or Trusted Build, for the software created during federal testing to be used for Colorado Department of State testing pursuant to Secretary of State Election Rule 45.4.6.

Upon receipt of the Trusted Build, the Secretary of State will secure the media containing the information and ensure the chain of evidence is included. The trusted build’s media will be placed in a suitcase, with at least two tamper-evident seals on the suitcase, and an audible alarm. The chain of custody document will be updated and placed, along with the suitcase, in a secure safe.

The safe is secured in a limited access room with 24x7 surveillance monitoring. The safe has a key and combination lock. Only one staff member will have access to the key and another staff member will have the combination. The combination is changed once every 24 months.

During the documentation period (Phase II) of each voting system, the State will work with each vendor to install the Trusted Build version(s) of the software and firmware onto the devices in preparation for testing.

During Phase II, the Secretary of State’s office will also identify procedures for both installing and verifying the Trusted Build for the system being tested. These procedures will later be used by the State to install or verify the Trusted Build for all certified machines of the tested system in each county across the state.