Andrea Gyger

From: Ralph Shnelvar [redacted]
Sent: Thursday, August 21, 2014 4:09 PM
To: SoS Rulemaking
Cc: Mary Eberle
Subject: 1.1.40 & SHA-1

Suggested rewrite of 1.1.40

1.1.40 "Trusted build" means the write-once installation disk or disks for software and firmware for which the Secretary of State has established the chain of evidence CHAIN-OF-CUSTODY to the building of the disk(s), which is then used to establish or re-establish the chain-of-custody of any component of a voting system that contains firmware or software. The trusted build is the origin of the chain of evidence CHAIN-OF-CUSTODY for any software and firmware component of the voting system.

1.1.40.1 All non-firmware components shall have cryptographically secure (e.g. SHA-2) signatures computed and such hash values are to be kept by the office of the Secretary of State for each build and made available on the Internet.

1.1.40.2 A build is considered trusted when all hash values compare equally.

1.1.40.3 Only trusted builds are allowed to be used in any computer equipment in any election or Logic and Accuracy Test.

- - - - -

SHA-1 has been found to be cryptographically insecure. SHA-2 should replace SHA-1

Ralph Shnelvar
[redacted]

Libertarian Candidate for Boulder County Clerk and Recorder
www.ralphyforclerk.org

Chair, Libertarian Party of Boulder County
www.lpboulder.org www.facebook.com/lpboulder