Section 2 – Election Management System

File 2-2 EMS Validation

2.2 Describe any software/firmware validation tools built into the device for use in installation, pre-election, and post-election testing to verify that software/firmware has not been modified.

All digital records are encrypted and signed, so the signature is the hash checksum. This applies to any software on the machine, but also to all election data. Should anything be added, the cryptographic hash will immediately be incorrect, which the system will detect and respond appropriately.

Dominion prides itself on the quality and security of our proposed solution for Georgia. Our demonstrated ability to certify and implement successful end-to-end systems begins with ensuring data quality and security from the development to the production phase of our installations.

All products in the Democracy Suite platform follow best software and application development practices, including additional source code quality and security procedures. All software programs satisfy recommended coding standards, as well as code styling guidelines as required by EAC VVSG standards. Automated code review processes are in place, that verify compliance with industry accepted coding standards for programming languages. In addition, proper system and software hardening procedures are clearly defined and regularly tested. Testing is performed on the lower source code level using code analysis tools, and at the system level using Nessus vulnerability testing tool. Data integrity and confidentiality is implemented according to NIST defined and FIPS validate procedures and algorithms.

All the code is stored in a secure manner within our organization and regularly backed up. Dominion’s IT personnel further improve overall security through the usage of firewalls, intrusion detection/prevention systems, comprehensive employee training, and company-wide security policies. Continuous integration is performed on a daily basis along with in-depth testing, which maintains constant code quality. Documentation covers recommended secure configuration scenarios from securing host operating systems (by using antivirus software, firewall configuration, hardening scripts, performing regular updates, and being in an isolated environment) through encryption of application communication mechanisms, hard disk encryption, and election file encryption. Voting locations are physically secured by trained professionals, machines (tabulators) are locked down from modification through the use of appropriate seals and are uniquely identifiable by having appropriate certificates stored for use in authentication.

Dominion uses multi-level assurance and quality control processes to ensure that all elements of our integrated voting system perform properly with every use. Internal acceptance testing is performed on each voting system on receipt from the manufacturer. By the time our products are purchased by the customer, they have gone through three full rounds of acceptance testing. Independent reviews of election databases are conducted to prior Logic and Accuracy testing. We recommend (and support our customers to conduct) precinct-level pre-election testing.

In addition to this rigorous testing and control program designed to catch errors, Dominion Voting regularly conducts process audits of our acceptance testing, and programming processes to ensure that errors never occur.