**Section 7 – Electronic Poll Book (EPoll)**

**File 7-3 EPoll Validation**

**7.3 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.**

The Poll Pad has built-in software and firmware validation tools that enable the device to verify that it has not been modified and demonstrate this via comprehensive audit logs that timestamp and display every single event or interaction on the device. The application is code signed using our Apple enterprise development license and will not run on any device if it has been modified in any way. For more info, please see the "App code signing" section in the Apple iOS 12 Security paper attached to section 7-4.

Firmware tools inherent to the iPad include “sandboxed” applications which prevent applications from interacting with one another or accessing another application’s data. Data encryption on the device is certified FIPS 140-2. Additionally, the iPad and the Poll Pad application prevent unauthorized access from removable drives or any other physical medium. The device and application require an Apple developer signature to connect, which the iSync drives have to interact.

Amazon Web Services (AWS) GovCloud provides a network audit log of all threats and activity, including unauthorized access attempts using AWS Cloudwatch. This means that any unauthorized attempts to interact with ePulse EPDMS will be provided in a printable, exportable audit log.

Meraki Mobile Device Manager does not require a cloud network to enroll devices and maintain logs. Software updates or other modifications can be pushed out until after the close of an election. Similarly, if a device is stolen, it can be locked and disabled to prevent data from being accessed or modified.

**Clarification Question**

1. **Does the capability exist to validate the Epoll software/firm using hash validation?**

No, the ePulse/Poll pad solution does not use or make Hash Validation available. iOS platforms instead use Code Signing. Whereas Hash Validation simply validates that the file size has not changed, Code Signing uses Hash Verification inside its security procedures and also verifies against ANY file modification, and will stop the application from functioning should any change be detected.

**B. If yes, what are the steps needed to obtain a HASH value in the following scenarios? Please specify:**

**- Initial Acceptance Testing,**

**- County Warehouse Pre-Election,**

**- Polling Place Setup, and**

**- Post Election review (saved as archived documentation).**

With the utilization of Code Signing, the need for a front facing easily accessible Hash value is not as prevalent, so in the current configuration of the Poll Pad Solution it is not available.  If this is a need, then it can be disseminated upon request.

More information on code signing if available from Apple here: <https://developer.apple.com/support/code-signing/>