U.S. ELECTION ASSISTANCE COMMISSION
Voting System Testing and Certification Program
1335 East West Highway, Suite 4300
Silver Spring, MD. 20910

Notice of Clarification

NOC 16-02: Trusted Build

Issued by Program Director, 04/19/2016

Section of Certification Manual to Be Clarified:

Voting System Test Laboratory Program (VSTL) Manual, Version 2.0

2.18. VSTL Verification of Trusted Build. At the conclusion of each test campaign, VSTLs shall verify the trusted build and associated materials required to be escrowed in the EAC Repository (See Section 5.5 of the Testing and Certification Program Manual). The verification process shall include:

2.18.1. Catalog all files contained in the escrow package and confirm the ability to read the media.
2.18.2. Test the functionality of the compile to be deposited.

Testing & Certification Program (Cert) Manual, Version 2.0

5.6. Trusted Build Procedure. A trusted build is a three-step process: (1) the build environment is constructed, (2) the executable code and installation disks are created, and (3) the VSTL verifies that the trusted build was created and functions properly. The process may be simplified for a modification to a previously certified system. In each step, a minimum of two witnesses from different organizations are required to participate. These participants must include a VSTL representative and a manufacturer representative. Before creating the trusted build, the VSTL must complete the source code review of the software delivered from the manufacturer for compliance with the VVSG and must produce and record file signatures of all source code modules. Hashes shall use a current FIPS 140-2 level 1 or higher validated cryptographic module. After the trusted build is completed, there shall be no other "final" build. As the final step, the trusted build must be submitted to the EAC on two separate forms of media.

5.6.1.Constructing the Build Environment. The VSTL shall construct the build environment in an isolated environment controlled by the VSTL, as follows:

5.6.1.1. The device that will hold the build environment shall be completely

erased, in accordance with Department of Defense or NIST approved methods. The VSTL shall ensure a complete erasure of the device.
5.6.1.2. The VSTL, with manufacturer observation, shall construct the build environment.
5.6.1.3. After construction of the build environment, the VSTL shall produce and record a file signature of the build environment.
5.6.1.4. A clone of the build environment computer's main storage media shall be created. File signatures shall be taken by the VSTL for verification purposes.

5.6.2.Creating the Executable Code and Installation Disks. After successful source code review the VSTL shall:

5.6.2.1. Check the file signatures of the source code modules and build environment to ensure they are unchanged from their original form.
5.6.2.2. Load the source code onto the build environment and produce and record the file signature of the resulting combination.
5.6.2.3. Produce the executable code, and produce and record file signatures of the executable code. A clone of the computer's main storage on which the executable code was created shall be created, with the file signatures verified by the VSTL.
5.6.2.4. The VSTL shall create installation disk(s) from the executable code, and produce and record file signatures of the installation disk(s).

5.6.3.Verification of the Created Media. Upon completion of all the tasks outlined above, the VSTL shall perform the following tasks:

5.6.3.1. Install the executable code onto the system submitted for testing and certification before the completion of system testing.
5.6.3.2. Produce and record file signatures of each voting system file resident on each device.
5.6.3.3. Verify that all media to be included in the Trusted Build and submitted to the EAC functions properly.

5.6.4.Trusted Build for Modifications. The process of building new executable code when a previously certified system has been modified can be somewhat simplified, if the build environment of the modification's original certification can be obtained.

5.6.4.1. The build environment used in the original certification is removed from storage and its file signature verified.
5.6.4.2. After source code review, the modified files are placed onto the verified build environment and new executable files are produced.
5.6.4.3. If the original build environment is unavailable or its file signatures cannot be verified against those recorded from the original certification,

then the full process of creating the build environment must be performed. Further source code review may be required to validate that files are unmodified from the originally certified versions.

Purpose:

The Trusted Build is used by EAC to ensure that manufacturers provide the EAC with a witnessed software build. This build helps ensure that the executable code is a verifiable and faithful representation of the source code and is stored in the EAC repository.

Clarification:

Based upon VSTL feedback and recommendations, EAC shall receive Virtual Machines (appliances) from the VSTL for the trusted build.

Trusted builds shall include this virtual machine and any related items, so that the system can be constructed or restored on another machine.

Trusted builds shall be in the Open Virtualization Format (OVF).

Conclusion:

This clarifies what the VSTLs shall provide for Trusted Builds.