EAC Decision on Request for Interpretation 2008-03
(Operating System Configuration)

2002 VSS Volume1: 2.2.5.3, 4.1.1, 6.2.1.1, Volume2: 3.5
2005 VVSG Volume1: 2.1.5.2, 5.1.1, 7.2.1, Volume2: 3.5

Date:
October 3, 2008

Question:

What is required and appropriate for determining and validating operating system configuration settings?

Section of Standards or Guidelines:

VSS 2.2.5.3 COTS General Purpose Computer System Requirements
VVSG 2.1.5.2 Use of Shared Computing Platforms

Further requirements must be applied to Commercial-off-the-Shelf operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations, including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these systems is vulnerable to unintended effects from other user sessions, applications, and utilities executing on the same platform at the same time as the election software.

"Simultaneous processes" of concern include: unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.

To counter these vulnerabilities, three operating system protections are required on all such systems on which election software is hosted. First, authentication shall be configured on the local terminal (display screen and keyboard) and on all external *connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running*

Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.

Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.

VSS V1: 4.1.1 Software Sources
VVSG V1: 5.1.1 Software Sources

The requirements of this section apply generally to all software used in voting systems, including:

- *Software provided by the voting system vendor and its component suppliers*
- *Software furnished by an external provider (for example, providers of COTS operating systems and web browsers) where the software may be used in any way during voting system operation*
- *Software developed by the voting jurisdiction*

Compliance with the software requirements is assessed by several formal tests, including code examination. Unmodified software is not subject to code examination; however, source code provided by third parties and embedded in software modules for compilation or interpretation shall be provided in human readable form to the accredited test lab. The accredited test lab may inspect source code units to determine testing requirements or to verify that the code is unmodified and that the default configuration options have not been changed.

Configuration of software, both operating systems and applications, is critical to proper system functioning. Correct test design and sufficient test execution must account for the intended and proper configuration of all system components. Therefore, the vendors shall submit a record of all user selections made during software installation as part of the Technical Data Package. The vendor shall also submit a record of all configuration changes made to the software following its installation. The accredited test lab shall confirm the propriety and correctness of these user selections and configuration changes.

VSS V1: 6.2.1
VVSG V1: 7.2.1 General Access Control Policy

The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security.

Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for:

- *a. Software access controls*
- *b. Hardware access controls*
- *c. Communications*
- *d. Effective password management*
- *e. Protection abilities of a particular operating system*
- *f. General characteristics of supervisory access privileges*
- *g. Segregation of duties*
- *h. Any additional relevant characteristics*

VSS V1: 6.2.1
VVSG V1: 7.2.1.1 Individual Access Privileges

Voting system vendors shall:

- *a. Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access*
- *b. Specify whether an individual's authorization is limited to a specific time, time interval or phase of the voting or counting operations*
- *c. Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes*

VSS V1: 6.2.2
VVSG V1: 7.2.1.2 Access Control Measures

Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include:

- *a. Use of data and user authorization*
- *b. Program unit ownership and other regional boundaries*
- *c. One-end or two-end port protection devices*
- *d. Security kernels*
- *e. Computer-generated password keys*
- *f. Special protocols*
- *g. Message encryption*
- *h. Controlled access security*

Vendors also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.

VSS V2: 3.5
VVSG V2: V2: 3.5 Testing for Systems that Operate on Personal Computers

For systems intended to use non-standard voting devices, such as a personal computer, provided by the local jurisdiction, the accredited test lab shall conduct functionality tests using hardware provided by the vendor that meets the minimum configuration specifications defined by the vendor.

Section 4 provides additional information on hardware to be used to conduct functionality testing of such voting devices, as well as hardware to be used to conduct security testing and other forms of testing.

Discussion:

VSS 4.1.1./VVSG 5.1.1., third paragraph clearly describes what is required of the vendor and the VSTL for configuration of software including COTS Operating System. It concludes with the statement "The accredited test lab shall confirm the propriety and correctness of these user selections and configuration changes."

As a benchmark to determine if user selections are correct the EAC will utilize guidelines that have been established by an activity that has a broad participation of software providers, application developers, security professionals, users, standards developers, government representatives etc. This provides an unbiased, vetted, stable but current, and trusted information base to use as the benchmark.

The characteristics of the benchmark are consistent but the specific program that will be used will be selected to match the technology in question. For example the SCAP program and specifically the FDCC checklists for specific Operating System configuration settings will be used as the benchmark for assessing the adequacy of the testing, both in coverage as well as the appropriateness of specific settings.

Three examples of the 295 from the National Checklist Repository (SCAP) for Windows XP, set to FDCC (Federal Desktop Configuration Checklist) guidance.

CCE-315 Audit account logon events Set to: Success, Failure
Determines whether to audit each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account. If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when an account logon attempt succeeds. Failure audits generate an audit entry when an account logon attempt fails. To set this value to no auditing, in the Properties dialog box for this policy setting, select the Define these policy settings check box and clear the Success and Failure check boxes. If success auditing for account logon events is enabled on a domain controller, an entry is logged for each user who is validated against that domain controller, even though the user is actually logging on to a workstation that is joined to the domain.

CCE-233 Network security: Do not store LAN Manager hash value on next password change
Determines if, at the next password change, LAN Manager is prevented from storing hash values for the new password. It is important to enable this setting since the LAN Manager Hash is a prime target of many hackers.

CCE-55 System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
Determines if the TLS/SSL Security Provider supports only the LS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. In effect, this means that the provider only supports the TLS protocol as a client and as a server (if applicable). It uses only the Triple DES encryption algorithm for the TLS traffic encryption, only the RSA public key

algorithm for the TLS key exchange and authentication, and only the SHA-1 hashing algorithm for the TLS hashing requirements. For Encrypting File System Service (EFS), it supports only the Triple DES encryption algorithm for encrypting file data supported by the Windows NTFS File System. By default, the Encrypting File System Service (EFS) uses the DESX algorithm for encrypting file data. Setting to “Enabled” causes problems documented in MS KB article “Can't browse to SSL sites after enabling FIPS compliant cryptography”.

Conclusion:

The Manufacturer and the VSTL may use whatever metrics they wish to establish the correct configuration of operating systems. It is incumbent on the VSTL to evaluate the configuration documentation provided by the manufacturer in order to determine completeness, clarity and consistency with the checklist criteria. The VSTL shall provide additional information if some inconsistency exists with the checklist criteria. This information must include any rationale supporting a contention that any inconsistencies with the checklist are either not applicable or have been mitigated.

In review of the VSTL evaluation of the operating system(s) configuration, the EAC will use the NIST SCAP FDCC checklist, if available (some OS’s may not currently be in the repository), as the benchmark for appropriate settings. If all the settings are not identifiable in the report or selections have been made to be other than the FDCC recommendation, a justification for the variance may be requested. It is recognized that in some cases variance may be required or desired for optimum security and functionality.

Effective Date:

Immediate- for all voting system test plans submitted after the date of this document.