



EAC Decision on Request for Interpretation 2010-04 (Functional Requirements with respect to Security)

2002 VSS Volume I: 2.2.1 Security
2005 VVSG Volume I: 2.1.1 Security

Date:

June 24, 2010

Question:

Does the first sentence in the Functional Requirements Section with respect to Security allow the security requirements, a through f, in that section to be adhered to solely by administrative practices/procedural safeguards?

Section of Standards or Guidelines:

2002 VSS VI: 2.2.1

2.2.1 Security

System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems shall:

- a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.
- b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.
- c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met.

- d. Provide safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure.
- e. Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation.
- f. If access to a system function is to be restricted or controlled, the system shall incorporate a means of implementing this capability.
- g. Provide documentation of mandatory administrative procedures for effective system security.

2005 VVSG VI: 2.1.1

2.1.1 Security

System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems shall:

- a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability
- b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions
- c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met
- d. Provide safeguards in response to system failure to protect against tampering during system repair or interventions in system operations
- e. Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation
- f. Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled
- g. Provide documentation of mandatory administrative procedures for effective system security

Discussion:

The posed question centers on the meaning and impact of the statement “System security is achieved through a combination of technical capabilities and sound administrative practices.” The above statement is a statement of fact and contains no normative language. On the other hand, statements a through g (within Section 2.2.1 of the 2002 VSS and Section 2.1.1 of the 2005 VVSG) are preceded by the keyword SHALL and are, in fact, normative. Administrative practices are used to ensure that technical/system capabilities that provide security are

implemented properly. It is considered poor security practice to use policy and procedures in lieu of system capabilities/functions that can prevent, deter, or detect security violations.

Conclusion:

“System security is achieved through a combination of technical capabilities and sound administrative practices” is not normative and shall not be used to justify using policy and/or administrative procedures, in lieu of voting system capabilities/functions, to meet requirements in a through f above. In conforming to all requirements in the VSS/VVSG, including the requirements cited above, voting systems, through system capabilities/functions, or (only for documentation requirements) via its associated documentation (TDP), shall be capable of meeting the specific requirements in the applicable standard. These system capabilities/functions may be supported with administrative procedures or procedural safeguards that are, or are planned to be, in place, as required by requirement g. However, administrative practices/procedural safeguards are not solely sufficient to fulfill the normative requirements a through f. It is only with both system security features and administrative procedures that effective system security can be achieved.

Applicability:

This is effective for all Test Plans approved after this date.