EAC Decision on Request for Interpretation 2012-06 (Use of Public Telecommunications Networks and Data Transmission)

2005 VVSG Volume I, Section 7.6.1

Date:

October 1, 2012

Question:

Two primary questions are intended to be addressed in this RFI:

- Do the Data Transmission requirements of the 2005 VVSG apply to voting systems that transmit aggregate vote totals?
- How should Voting System Test Laboratories and Voting System Manufacturers interpret these requirements?

Section of Guidelines:

2005 VVSG Volume 1, Section 7.6.1 - Data Transmission

All systems that transmit data over public telecommunications networks shall:

a) Preserve the secrecy of voter ballot selections and prevent anyone from violating ballot privacy

b) Employ digital signatures for all communications between the vote server and other devices that communicate with the server over the network

c) Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes

Discussion:

In discussing the Data Transmission requirements with Voting System Test Laboratories (VSTLs) and voting system manufacturers, multiple parties asserted that voting systems transmitting aggregate vote totals are not subject to these requirements. 2005 VVSG Volume 1, Section 7.1.2 states the following about the "Use of Public Communications Networks" section:

Use of Public Communications Networks: *These standards address security for systems that communicate individual votes or vote totals over public communications networks.*

Because this section explicitly states "*for systems that communication individual votes or **vote totals,***" [emphasis added] the EAC concludes the requirements of section 7.6.1 apply to voting systems transmitting aggregate vote totals over public telecommunications networks. As the 2005 VVSG public telecommunications requirements have not been evaluated against any voting system to date, the EAC will provide guidance for these three requirements.

Requirement 7.6.1.a pertains to confidentiality. Transmitting aggregate vote totals can potentially safeguard the secrecy of an individual voter's ballot selections and prevent violations of ballot privacy. VSTLs shall devise tests to ensure the format of the aggregated vote totals does not violate this requirement.

Requirement 7.6.1.b requires manufacturers to digitally sign individual votes or vote totals (e.g., aggregate totals) before they are transmitted. The vote server must verify the digital signature of the vote or vote totals. In an effort to not limit the innovation and design of voting systems, the EAC will not define the term "vote server." Vote server may refer to a single server, but multiple devices could also work together to provide this functionality. VSTLs shall confirm votes or vote totals are digitally signed, and work as intended. Digital signatures are cryptographic functions which, per RFI 2012-05, are to be FIPS 140-2 certified.

Requirement 7.6.1.c applies to critical operations of processing returns received via data transmission from various precincts. The action of processing these votes or vote totals must be a deliberate action performed by only election officials authorized by the voting system.

Additionally, Section 6.1 of the 2005 VVSG states:

> A wide area network (WAN) public telecommunications component consists of the hardware and software to transport information, over share public (i.e., commercial or governmental) circuitry or among private systems. For voting systems, the telecommunications boundaries are defined as the transport circuitry, on one side of which exists the public telecommunications infrastructure, outside the control of voting system supervisors. On the other side of the transport circuitry are the local area network (LAN) resources, workstations, servers, data and applications controlled by voting system supervisors.

Finally, Section 6.1.2 of the VVSG States:

> This section applies to voting-related transmissions over public networks, such as those provided by local distribution and long distance carriers. This section **also** applies to private networks regardless of whether the network is owned and operated by the election jurisdiction. (emphasis added)

Conclusion:

The requirements of section 7.6.1 apply to all voting systems with public telecommunications capabilities. The guidance provided here by the EAC is intended to assist VSTLs and voting system manufacturers in determining the applicability, implementation, and testing of these requirements to verify their operation within the voting system.

Effective Date:

Effective immediately for all voting systems without an approved application for testing.

.