EAC Decision on Request for Interpretation 2012-05 (Public Telecommunications and Cryptography)

2005 VVSG Volume I, Section 7.5.1.b

Date:
October 1, 2012

Question:
Which 2005 VVSG encryption requirements apply to systems using public telecommunications technologies?

Section of Guidelines:
2005 VVSG Volume 1, Section 7.5.1.b - Maintaining Data Integrity
Voting systems that use telecommunications to communicate between system components and locations before the polling place is officially closed shall:

i. Implement an encryption standard currently documented and validated for use by an agency of the U.S. government
ii. Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System

Discussion:
2005 VVSG Volume 1, requirement 7.5.1.b is unclear on the following items:

1. What is meant by telecommunications?
2. When is a polling place officially closed?
3. Which technologies does this requirement apply to?

The definition of telecommunications provided by the first paragraph of 2005 VVSG Section 6 states:

2005 VVSG Section 6

For the purpose of the Guidelines, telecommunications is defined as the capability to transmit and receive data electronically using hardware and software components over distances both within and external to a polling place.

The phrase "*external to a polling place*" leads the EAC to conclude all devices that are part of the voting system's network residing inside and/or outside the polling place, including the

central election office, are subject to this requirement. The applicability of requirement 7.5.1.b to all locations is further demonstrated by references in the requirement to communication between "system components and locations."

The second point needing clarification in the requirement references the time at which a "*polling place is officially closed*." The requirement is difficult to enforce as this is a legal matter decided by states and election jurisdictions. Closing the polling place is a multi-step process including the following:

1. Closing the polls on each individual voting component or system;
2. No longer allowing voters to cast votes at a polling site;
3. Concluding all post-election activities at the polling site; and
4. Closing the physical location of the polling site.

While the first method of closing the polling place is a technical solution, it does not directly align with all voting channels, such as early voting. The second method is extremely variable from election to election, and in some scenarios differs by polling place. Many polling sites share a location with centralized vote centers at election offices, further complicating the official close because the election office may not close until much later that night.

For the purposes of this requirement, polling places are officially closed when *all election-related duties conclude at the polling site.* This ensures that voting systems adhere to the 2005 VVSG and can be used in election jurisdictions regardless of state or local laws related to the close of polls. Therefore, voting systems using telecommunications before the polling place is officially closed shall implement an encryption standard currently documented and validated for use by an agency of the U.S. government. This interpretation is consistent with the next iteration of the VVSG.

There are many open source solutions available to assist in implementing these requirements, and if implemented properly, should appear transparent to the voting system's users. Voting systems using public telecommunications usually operate as part of a larger network owned and operated by the county. When new systems are connected to public telecommunications networks, there are new threats introduced into the entire network. Protecting data in this manner is one of many standard risk mitigating practices present in systems using public telecommunications technologies.

The 2005 VVSG differentiates between wired and wireless technologies by applying different security requirements for each medium. As expected, more stringent requirements exist for systems with wireless capabilities. However, requirement 7.5.1.b does not mention technology specific requirements; it applies to all systems utilizing public telecommunications technology.

Conclusion:

This decision ensures EAC certified voting systems conform to the 2005 VVSG in any configuration election officials choose to use the voting system. The requirements and information discussed here leads the EAC to conclude that all aspects of the system that are

exposed to the threats of a public/private network need to be protected using FIPS 140-2 or the most current FIPS certified cryptographic modules. These shall be used in FIPS-compliant mode for all portions of the voting system, including precinct and central locations, and for both public and private networks.

Effective Date:

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