Comments of Col. Shawn Smith (United States Air Force, retired) on Iowa's voting systems and standards

"Iowa Code Title II, Section 1, Chapter 52.5.2. states that all optical scan voting systems approved for use in Iowa after April 9, 2003 shall meet voting systems performance and test standards, as adopted by the Federal Election Commission on Apr 30, 2002 (find those standards here, under 2002 Voting System Standards (VSS) (https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines)).

The internet was pretty new in 2002, so the VSS didn't prohibit its use (in fact, it discussed Direct-Recording Electronic (DRE) over telephone line or internet), BUT, the VSS has a section on security standards (6) and a sub-section 6.5 for Telecommunications and Data Transmission, and that sub-section requires, e.g. that voting systems must:

1. "6.5.3.b. Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System," and
2. "6.5.4..."Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible," and
3. "6.5.4.2...Voting systems that use public telecommunications networks shall use protective software at the receiving-end of all communications paths to:
   a. Detect the presence of a threat in a transmission;
   b. Remove the threat from infected files/data/
   c. Prevent against storage of the threat anywhere on the receiving device;
   d. Provide the capability to confirm that no threats are stored in system memory and in connected storage media; and
   e. Provide data to the system audit log indicating the detection of a threat and the processing performed." - It goes on and describes what vendors have to do to monitor and protect against threats to the system.

Title 52 does have some requirements for voting systems under Chapters 201-209, but it's silent on internet connections.

Iowa is using a combination of ES&S, Dominion, and Unisyn voting systems; any of them might have networking capabilities that would allow connection to the internet, and none of those will have been tested, at all, to ensure they meet the telecommunications security requirements in the 2002 VSS.

For example, Iowa allows use of ES&S' EVS 6.1.1.0;

a) in the first place, Pro V&V conducted this certification testing (to determine whether EVS 6.1.1.0 conformed to VVSG 1.0 (2005 standards); VVSG 1.0 is NOT the same as 2002 VSS.
b) Second, Pro V&V was not actually accredited at the time (their accreditation expired in 2017 and was not renewed until 2021 - the EAC (Election Assistance Commission) has conspired to hide this fact, because it means the EAC certfication of the voting systems Pro V&V tested in that period are not valid, and therefore the state cert dependent on EAC cert or EAC-accredited VSTL (formerly ITA - interim test authority) are also not valid).
c) Third, although ES&S previously sold cellular modem-equipped DS200 tabulators to multiple U.S. customers, claiming that they were "EAC Certified"

(ES&S actually put "EAC Certified!" stickers on the DS200s), those DS200s were not tested/certified, nor was any ES&S voting system suite tested/certified with them. There's a good chance Iowa actually has cell modem-equipped DS200s in use), they are not legal to use in Iowa (because they weren't tested/certified by a Fed lab (the VSTL) to certify their conformance to 2002 VSS.

d) Fourth, EVS 6.1.1.0 uses multiple third-party products (like MS Server 2016 and Win 10 LTSC) which have numerous published, known vulnerabilities, for which the EVS installs are not protected/mitigated (and therefore not compliant with the 2002 VSS). E.g., EVS 6.1.1.0 test report from Pro V&V was issued June 2020; any vulnerability for 3rd party software (e.g. Windows) published AFTER June '20 is NOT mitigated in EVS 6.1.1.0 (if it was, you'd have to have an Engineering Change Order (ECO) from the vendor to EAC, which would refer the ECO to a VSTL for evaluation and recommendation (either a) de minimis (makes no difference) and no test required or b) some retest required, or c) full retest required; the VSTLs are paid by the vendor, so they always recommend "de minimis" and EAC always accepts; regardless, there is no ECO for EVS 6.1.1.0 reflecting mitigation of [vulnerabilities] in 3rd party software. There were 156 vulnerabilities to Windows Server 2016 alone, published in 2022 alone.

To wit: there is no Fed or State (IA) statute that prohibits internet connection, per se, but 2002 VSS is mandated by IA code, and cannot possibly be satisfied by any vendor's voting system, including telecommunication security requirements.

SO, if any vendor proposes to use telecommunications (internet or otherwise), they must have both test reports showing those capabilities have been tested for compliance w/2002 VSS, and 2002 VSS requirements that the security of those systems be maintained by proactive defense against both threats known at the time of cert/testing and threats which emerge.

Ergo, if the vendor can't prove the voting system mitigates all emerging threats and known vulnerabilities (e.g. all the threats published at CVE Details (https://www.cvedetails.com/) affecting 3rd party software/hardware listed in their system configuration (in some detail in test report at (https://www.eac.gov/sites/default/files/voting_system/files/ESS%20EVS6110%20Test%20Report-01.pdf), then they can't use telecommunications without violating the 2002 VSS standards and therefore IA Code, Chapter 52 (.5.2). That's what's true. It's probably not what will have been explained to or be consensus to the Board of Examiners.

September 25, 2023
Cause of America
Col. Shawn Smith, United States Air Force, retired.