Getting the facts straight about modems and Minnesota

In a few states, including Minnesota, it is a legal practice to use cellular modems to transmit unofficial election results after the polls are officially closed and all voting has ended. These early, unofficial results help the news media report results quickly on election night. Below are the most frequently asked questions about modems and election firewall security.

1. Do ES&S DS200 tabulators in Minnesota have modems?

Six of the 78 Minnesota counties using ES&S equipment use modems to transmit unofficial election results after the polls are officially closed and all voting has ended. In these counties, ES&S uses private network connectivity, industry best practices, and numerous security safeguards to protect the transfer of these unofficial election night results. The physical ballots and printed results tapes are always protected. Final official results are physically uploaded at election headquarters prior to the final certification of elections.

2. How do we know modems aren't in DS200s in all jurisdictions in Minnesota?

Modem components are not resident on the DS200 by default, but rather a separate board that is only installed in DS200s in those jurisdictions which choose this technology and where a state may permit their legal use. A configuration report printed by the DS200 will indicate whether a modem has been installed. Additionally, DS200s without a modem component do not include the technology or the network architecture required to support modeming and allow a modem to operate on the machine.

3. How has ES&S made the modeming of unofficial election night results in Minnesota secure?

The modem solution for Minnesota jurisdictions that wish to send unofficial results on election night has been tested by federally accredited Voting System Test Laboratories (VSTLs), certified by multiple states, and proven in elections. ES&S voting systems are designed and built with multiple layers of protection, including physical controls, system hardening, data integrity validation and data encryption.

Certified versions of modems used in Minnesota use private network connectivity, adding an additional layer of security to the transfer of unofficial results. ES&S' private network configurations are specifically designed for high-security applications in critical infrastructure environments. In this configuration, all transmissions are segregated from the public internet. By using a dedicated, private connection, the public internet's best-effort routing paths are avoided, and concerns over data security are reduced.

Again, unofficial election results are only able to be transferred after polls close and results tapes are printed. The physical ballots and printed results tapes are always protected. Final official results are physically uploaded at election headquarters prior to the final certification of elections.

4. How is the Election Management System (EMS) protected?

EMS programs, including Election Reporting Manager (ERM) and Electionware, run on hardened computer workstations, meaning they are locked down with allowed access only to the functions required to conduct an election. Unused ports can be blocked and unnecessary services are removed. In jurisdictions using modems to transmit unofficial election results following the close of polls, only the Data Communications (SFTP) server, which sits behind the firewall in what's known as the DMZ, has any connection to the cellular network.

5. What can jurisdictions do to further increase the security of unofficial modem transmissions?

ES&S strongly recommends that jurisdictions maintain the Minnesota state certified and hardened configuration on their EMS network and system components. Access to systems should be restricted both physically as well as technically to prevent unauthorized access. Furthermore, EMS systems should only be powered on and connected to the firewall and external telecommunication networks when being tested or when in actual use.