Electronic methods potentially secure for sending blank ballots overseas

December 23 2008

Electronic technologies could be deployed immediately and reliably to augment slower postal mail for distributing ballots to U.S. citizens living abroad, but using telephone, e-mail, and the Web to transmit completed ballots still faces significant, unresolved issues, according a new report* released today.

Prepared by the Commerce Department's National Institute of Standards and Technology with funding from the Election Assistance Commission (EAC), the report provides the first wide-ranging look at the security threats associated with potential electronic technologies for overseas voting and identifies possible ways of mitigating these threats.

The need to verify that each completed ballot comes from a registered voter while preserving voter privacy and has not been changed in transit makes the threats to the return of voted ballots by e-mail and Web "difficult to overcome," according to the NIST report.

The report discusses how postal mail and four electronic transmission options (telephone, fax, e-mail, and Web sites) could be used in the overseas voting process. It identifies issues and threats associated with using these methods to register voters, distribute blank ballots and return voted ballots. In addition, the report suggests control measures that can mitigate some of the specific threats identified.

For example, the report noted that automated computer systems could allow voters to cast ballots using a telephone or on a Web site. However,

such systems are difficult to audit, so attacks and malfunctions could go unnoticed. Voters might also be tricked into submitting votes on fraudulent Web sites using common spoofing and phishing tactics.

Another issue raised by the report is that e-mail and Web-based methods send election information through computer systems outside the control of election officials. Encryption could be used to protect communications between voters and Web sites, and this technology is widely deployed. E-mail encryption is also possible but less widely available.

Distributing blank ballots to overseas voters by fax, e-mail, and Web methods "do not pose significant risks to the integrity of elections" as long as appropriate measures are taken, according to the report. While some states already use these methods, wider use would allow more voters to receive electronically transmitted ballots in a fraction of the time required to send ballots via postal mail.

To ensure that voters receive unaltered ballots, the NIST report recommended specific control measures, such as cryptography and back up communications lines, depending on the electronic method chosen. Voter registration could also be accomplished electronically, it said, using these technologies.

The EAC is responsible under the Help America Vote Act (HAVA) of 2002 (Public Law 107-252) to examine the technical challenges associated with overseas voting.

In 1986, Congress enacted the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), which states that U.S. citizens who are part of the uniformed services, merchant marines, and citizens residing overseas are allowed to register and vote absentee for Federal office.

Overseas citizens follow the rules of their home states, which typically have their own specific laws covering how overseas citizens register and vote. Overseas voting generally relies upon postal and military mail as the mechanism to distribute and receive election materials though some states have begun to distribute blank ballots by fax or e-mail.

At this time there are no guidelines that document best practices for fax, e-mail or Web-based distribution of ballots. Developing such best practices, according to the report, could help states develop methods for distributing ballots using these transmission methods and potentially improve the procedures and technical controls already in place in the states currently using these systems.

Note:
* Regenscheid, A. and Hastings, N., A Threat Analysis on UOCAVA Voting Systems, National Institute of Standards and Technology, Dec. 2008, full report at vote.nist.gov/uocava-threatanalysis-final.pdf .

Source: National Institute of Standards and Technology