

# **Use of Cryptography in Securing On-line Voting**

**By**

**Beth Ann Surber and Jackie Harris**

## **MOTIVATION**

There are several issues associated with providing individuals the ability to cast ballots electronically from a remote location, but most significant are the demands of maintaining a secure voting environment. The Military and Overseas Voters Empowerment Act has focused expedited ballot delivery and return efforts on the Overseas and Military Voters population. Though providing an affordable, secure and administratively feasible web-based voting solution presents numerous challenges, it is a goal worthy of pursuit.

## **METHODS/ PROCEDURES/ APPROACH**

West Virginia piloted online voting for military/overseas voters in the 2010 General Election. Two systems were used: 1) hosted data on a remote server, and 2) hosted data on redundant servers located in the Secretary of State's Office. In essence, each of the two solutions made use of private "Cloud" solutions.

There were four primary objectives: 1) allow voters sufficient time to receive and cast an absentee ballot; 2) secure voter's non-public information; 3) assure the vote cast is the vote tallied without linking ballot content to the voter; and 4) count all eligible ballots.

Both systems used secure methods to provide authentication and connectivity to the systems. Each was tested to assure the votes cast were tallied without the contents being attached to the individual voters. Each voter received confirmation of the ballot being received by the local election official.

## **RESULTS/ FINDINGS/ PRODUCT**

Both processes used in WV were considered successful by those using and administering the systems. The greatest criticism was voiced by academicians stating the processes used were not sufficiently secure to prevent vote-tampering or denial of service if used during a high-profile election.

## **CONCLUSION/ IMPLICATIONS**

As election administrators, vendors, and security experts continue to proactively address the cybersecurity concerns utilizing cryptography for end-user devices, telecommunications, and application development for the cloud, this initiative will move closer to full realization.