Voting Security and Preventing Fraud

Security

The American Arbitration Association® provides a stable and secure environment for electronic voting. The processes and procedures in place make it very difficult, if not impossible, for fraudulent votes to be cast.

Using a two-tier approach for both Internet and telephonic voting, the system architecture physically separates the data entry mechanism (Internet or Telephone) from the actual storage of data. The two-tier architecture provides a security layer (protected by user authentication) at the machine level. The data itself is stored using separate authentication.

In order to obtain direct access to secure data, one must be able to access the physical machine (web server) with an appropriate user ID and password. Then one must identify the physical machine on which the data resides, access that machine (again with an appropriate user ID and password), then provide the correct user ID and password to access the data itself.

For Internet voting, we also employ a secured mechanism of communicating between the voter's browser and our web server. This mechanism encrypts the data that is transmitted across the Internet while in transit to and from the web browser. The encryption method uses keys up to 256 characters in length. Standard encryption uses only 7 character keys and is hard to break even for seasoned cryptologists, so our method of encryption is next to impossible to break.

This mechanism prevents arbitrary 'sniffing' of the Internet traffic from obtaining user authentication or voting data that is being transmitted. All machines are equipped with the latest virus protection available to prevent malicious attempts to breach security. The machine used to access the system by the voter is an unknown for us. However, if voters are uncomfortable with the security or reliability of the machine they want to use, then they should not use it. Telephonic voting is an even more secure voting mechanism.

Fraud Prevention

The AAA® voting system stores voter information separately from the vote. During the election an encrypted link exists between the voter record and the vote transaction record. Upon official certification of an election, the link is removed as required by the U.S. Department of Labor.

The system (both Internet and telephonic) is constantly monitored for anomalies. Daily voting rates are monitored, as well as too many changes to a member's vote, too many votes coming from the same source, or too many failed attempts over a given period of time. These anomalies will trigger an investigative response. The original source (IP address or ANI-Caller ID number) is recorded for all attempts at contacting the system. These sources can then be traced back to their origin.

User authentication also provides a high level of security for these systems. Voters must first supply an ID—typically the employee ID or the last four digits of their SSN. Voters are also assigned a unique Personal Identification Number by the American Arbitration Association. Votes can only be cast when both identifiers are correctly supplied. Being assigned by two separate entities also ensures that the client does not have the information available to them. The system can also prevent votes from ever being changed. Clients do have an option of allowing changes to a vote once it has been cast, however this option can be set to not allow a change thereby further minimizing the threat of fraud.

One final note: in every election, the American Arbitration Association is a disinterested third party and has no ties to the outcome of the election results.