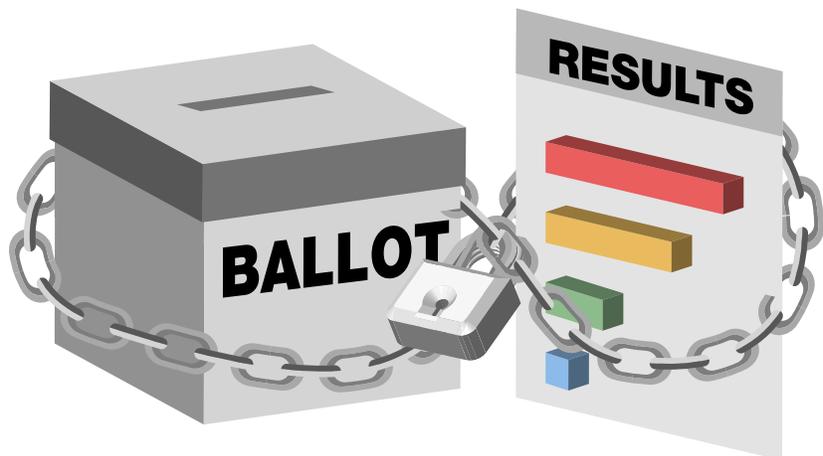


Protecting Your Elections through a World-Class Security Infrastructure



3	Introduction from Michael Tuteur, President and Chief Executive Officer, Votenet Solutions
4	Election Data Security
7	Application Security
9	Network Security
10	Physical Security
12	Continuous Security Upgrades and Monitoring

Dear Election Administrator,

Clients often ask me what it takes to have a strong, successful organization governance program. Of course many factors play into it, but one of the key aspects is the trust and confidence of your constituents that your elections are secure and reliable, enabling them to participate without concern that their personal information, voting choices, or other data will be improperly accessed or used.

Our team at Votenet Solutions understands the importance of security in maintaining constituent trust, and is 100% dedicated to the proactive protection and success of our customers. Our eBallot™ web-based election solution stands alone as the only online election solution designed from the ground up to be secured at the physical, network, application, and individual data levels. Independently validated by 6 leading third-party security authorities, and partnering only with independently certified service providers, eBallot provides complete, multi-layer defenses against physical or electronic attack on election or confidential information, and performs reliably 24/7/365, even during emergencies.

After eight years with zero security intrusions, 10,000 elections for 700 customers and 7 million voters served, eBallot is the proven choice for organizations concerned about establishing and maintaining the trust of their constituents and conducting a successful governance program.



To your election success,

Michael Tuteur

President and Chief Executive Officer
Votenet Solutions, Inc.

8 years of election security success:

- ✓ Zero security intrusions
- ✓ 700 customers
- ✓ 10,000 elections
- ✓ 7 million voters served

7 independent 3rd party security certifications:



All partners independently certified to verify highest levels of security





eBallot has extensive security measures in place to protect against the loss, misuse, and alteration of data. eBallot is a SAS-70 (Statement on Auditing Standard 70) Type I certified solution. Developed and maintained by the American Institute of Certified Public Accountants, the AICPA audited eBallot to ensure compliance with the SAS-70 Information Security Controls standards. This certification also verifies that eBallot is a neutral third-party solution, eliminating any perception of election tampering. These industry best practices, procedures and controls, coupled with industry-leading database technologies, ensure that your election information is secured.

eBallot offers a true multi-tenant architecture, meaning that individual customer “deployments” of the eBallot application occupy virtual partitions, rather than requiring separate physical stacks of hardware and software. Customers share the same physical infrastructure and identical code lines, but all customer and election data is stored separately. This ensures that one customer cannot access another customer’s election results and voter lists.

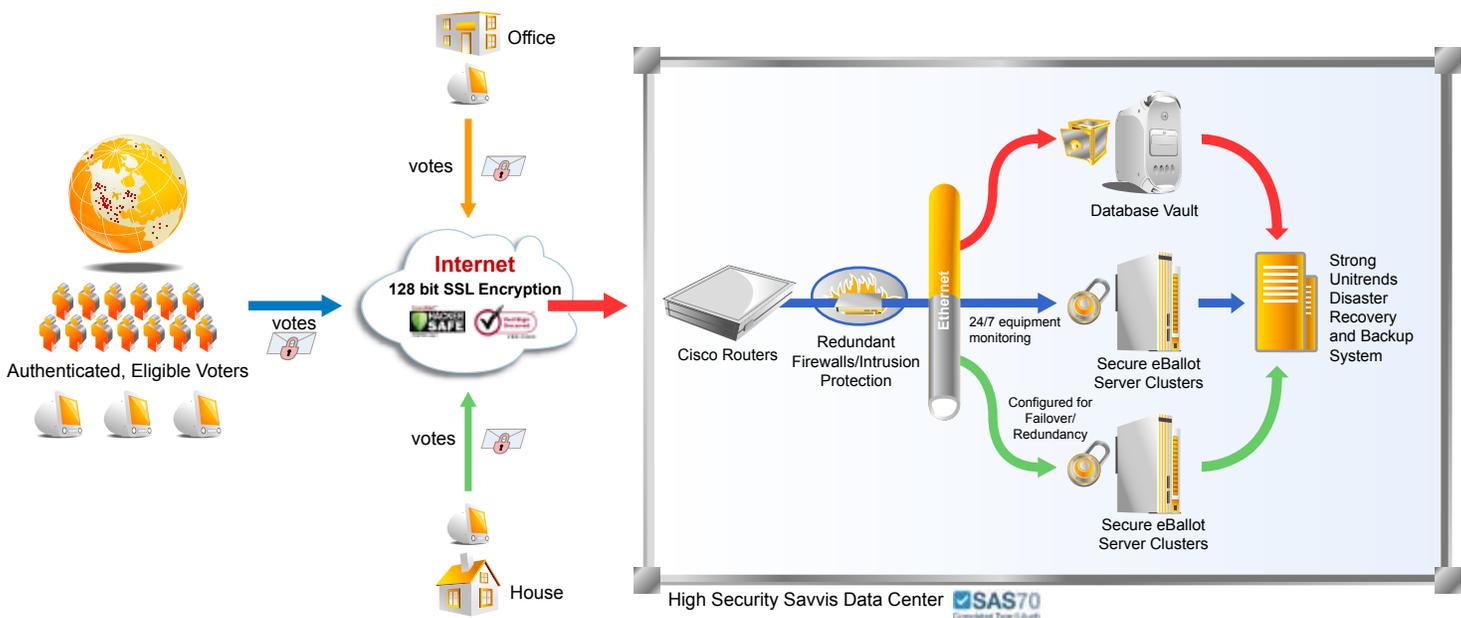
Powerful databases enable high volume vote processing at any time during an election, ensuring against system slowdowns and lost votes even if large numbers of voters cast ballots simultaneously.

Database Security

Database technologies and procedures are in place to safeguard and secure your voter lists and election results, preventing unauthorized access and maintaining accuracy.

- **Database is restricted** to a very limited number of authorized technicians
- **Databases are password-protected**, and passwords are changed regularly
- **Database access is logged via electronic entry logs** with a time and date stamp, providing a history of each login and possible irregularities
- **Voter lists are stored securely** in our protected database

eBallot™ stands alone as the only online election solution designed from the ground up to be secured at the physical, network, application, and individual data levels





Business Continuity and Disaster Recovery

Business continuity is the ability of an organization to continue to function at its normal operational levels, even after a disastrous event or during an electrical outage.

A comprehensive, proven backup and recovery strategy is imperative to achieving business continuity, leading Votenet Solutions to partner with Unitrends, leading provider of backup and rapid recovery systems rated #1 by industry analyst firm Gartner.

Unitrends provides data protection, system recovery, and application recovery capabilities from a single appliance, the Data Protection Unit (DPU), ensuring that no election data is lost in the event of a disaster and enabling eBallot to fully recover from a system crash in less than half an hour.

All eBallot web and database servers are connected to the Unitrends system and all data is backed-up every hour. All backups are encrypted, and any unused, obsolete, or end-of-life media is destroyed to prevent third-party data retrieval.

Additionally, Votenet Solutions business partner SAVVIS provides state-of-the-art hosting facilities for Votenet's data and servers. Rated #1 by industry analyst firm Gartner and trusted by the U.S. Department of Defense, AOL/Time Warner, Google and many FORTUNE 500 companies, each SAVVIS datacenter is engineered to include multiple levels of data protection. A large team of highly trained, certified on-site engineers continuously monitor Votenet's servers 24/7/365. From physical defense measures to network architecture, HVAC services, redundancy and failover, security, performance reliability, and disaster recovery has been fully accounted for in all areas.

- **Uninterruptible Power Supplies (UPS)** – Caterpillar 1000 KW diesel generators. Multiple UPS systems eliminate fluctuations and electrical irregularities, delivering continuous power to all critical systems.
- **N+1 Redundancy** – All systems are configured to be N+1 redundant. Electricity backup capabilities at SAVVIS datacenters are essentially unlimited. Short-notice refueling contracts for the diesel generators are maintained with multiple vendors at each datacenter location.
- **Environmental Controls** – All SAVVIS datacenters are built on raised floors and have high-volume, zoned temperature control systems. Multiple air conditioning units are configured to ensure proper heat dissipation. SAVVIS maintains multiple (N+1) Heating, Ventilation, Air Conditioning (HVAC) units within each data center. The HVAC units are powered by both normal and emergency electrical systems, and are monitored 24x7x365 by on-site personnel.
- **Fire Suppression** – "Sniffer" systems that detect smoke from the earliest stages of combustion. This detection system is augmented by heat detection and dry-pipe sprinkler systems.
- **Seismic Engineering** – Design elements include seismic isolation equipment to cushion facilities against movement, as well as earthquake bracing on all equipment racks. All datacenters have racks anchored to a concrete slab below the raised floor.



Rates Unitrends #1 Backup and Rapid Recovery Systems Provider



Rates SAVVIS #1 Managed Security Services Provider



SAVVIS team of highly-trained, certified on-site engineers monitor eBallot servers 24/7/365



SAVVIS Included in InformationWeek 500 Best IT Companies



Votenet Solutions Corporate Privacy Promise

We take privacy seriously and are committed to establishing and maintaining policies and procedures which protect the privacy of personal information gathered from our customers, prospective customers, and partners. Our comprehensive privacy promise means:

- Your voter lists are protected and safeguarded using secure servers and a secure hosting environment
- Your membership or voter data is never sold to 3rd parties
- Voter credentials or pass codes are never provided to individuals who contact us unless authorized by the designated Election Administrator
- Military-grade email encryption is used when routing your voter lists to technicians for scrubbing and uploading into your eBallot system
- Strict Non-Disclosure Agreements signed by partner firms assisting Votenet in maintaining our hosting facility
- Your election results are never disclosed to anyone at anytime

TRUSTe Certification

We are a member of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build trust and confidence in the Internet by promoting the use of fair information practices. Because we want to demonstrate our commitment to your privacy, we have agreed to disclose our information practices and have our privacy practices reviewed for compliance by TRUSTe. For more information about the TRUSTe certification process, and what TRUSTe certification means, please look at the TRUSTe website at www.truste.com.

E.U. Safe Harbor Certification

We comply with the E.U. Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal data from the European Union. The Department of Commerce Safe Harbor certification program is a way for U.S. based companies to ensure that they comply with E.U. regulations regarding the safekeeping of private data. You can see our Department of Commerce certification at <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>





eBallot was designed from the ground up with security in mind, using the Cold Fusion platform. Cold Fusion utilizes the Web Services Security (WS-Security) standard and World Wide Web Consortium (W3C) specifications for industry-standard authentication, encryption, authorization, XML signature, attachments, and routing with Web services.

128-Bit SSL Security

VeriSign, the world's leading provider of SSL encryption certificates, equips eBallot with the strongest commercial-grade 128-bit SSL encryption available. This ensures data and votes cannot be stolen, intercepted or manipulated while in transit from an administrator's or voter's computer to our election servers. A comprehensive encryption system ensures that only eBallot servers can decrypt data.

Administrator Security

- **Log-in Safeguards** – Election administrators may access eBallot only with a valid username and password. Safeguards exist to ensure intruders cannot gain access simply by trying numerous different passwords.
- **Intrusion Detection** - Administrator entry logs show a time and date stamp as well as IP address log, providing a history of each login and possible irregularities
- **Encrypted Election E-mail Reminders** – eBallot utilizes JangoMail, leading secure e-mail service provider, to enable administrators to send election e-mail reminders via 51 powerful, encrypted servers, ensuring rapid delivery. JangoMail participates in several whitelist programs, ensuring e-mails are delivered to their recipients' in-boxes, including participation in third-party initiatives such as Return Path's Sender Score Certified program.

Ballot Security

- **Ballot Scanning** – Before a ballot has been activated, the ballot is reviewed for logic errors and incomplete sections
- **Ballot Lockdown** – Prevents ballots from being altered or edited once they are active, eliminating inaccurate election results
- **Advanced Error Checking** – Ballot selections that do not adhere to ballot-level rules prompt instant notification of voter, preventing them from moving forward in the voting process until errors are resolved

Results Security

- **IP Tracking and Restriction** – eBallot tracks the Internet Protocol (IP) address for every vote, aiding election administrators in uncovering irregularities or illegal block voting, and enabling administrators to restrict votes to specific IP addresses only
- **Multiple Viewing Options** – Real-time election results can be viewed during the election or hidden from view until voting has closed, enabling organizations to choose a setting that complies with their bylaws
- **Receipts and Time and Date Stamps** – Each vote has a receipt and time and date stamp, ensuring results can be audited
- **SAS-70 Certified Tabulation** – Independent auditors have inspected eBallot to ensure each vote is counted correctly and election results are 100% accurate



VeriSign is the world's leading provider of SSL encryption verification certificates, assuring eBallot customers that voter data cannot be stolen, intercepted or manipulated while in transit from voter computer to the election servers



Voter Security

• Log-in Safeguards

- Voters may access eBallot only with a valid username and password
- Election administrators create username and password for each voter, using randomly generated codes, or existing membership information
- eBallot automatically authenticates voters, for example verifying membership dues are up-to-date, ensuring only eligible voters access the election voting area, and guarding against double voting and ballot stuffing
- eBallot safeguards against multiple failed attempts to log-in to the election voting area, ensuring intruders cannot gain access simply by trying numerous different passwords
- **Anonymous voting option** – If desired, eBallot can separate voter identity from vote selection, ensuring complete privacy
- **Session Limits** – Limiting the length of time that a voter can view the ballot reduces the possibility that another voter could view the voter's ballot choices
- **Paper Receipts** –The option to print a paper receipt provides voters with proof and peace-of-mind that their vote is counted

eBallot automatically authenticates voters when they log-in to your election voting area, ensuring only eligible voters gain access, and guarding against double voting and ballot stuffing

Thank you for voting in the NVAR Board of Directors Election.

This is your vote confirmation receipt. You may print this receipt for your records. [Click here to print](#)



Vote Confirmation: 2052008285613577	Date: February 20, 2008	Time: 08:56 EST
---	--------------------------------	------------------------

NVAR Board of Directors Election

Position	Votes cast for
Board of Directors	Genie Clark-Houston
NVAR Treasurer	Sandra Velasquez
Referendum Question 1: Enable the NVAR leadership to increase member dues for the implementation of a new membership management software system. The approximate cost of this software is \$150,000 and will be paid for with a \$12.50 increase in annual dues.	Approve Referendum
Survey Question 1: Related to the annual conference that took place in June, we would like to gather your feedback. Was the conference helpful for your business?	Very Helpful
Survey Question 2: This year, NVAR used an online service to facilitate the conference registration process. The aim of going to the online service was to cut down the time taken by the members to register and go through packet pick-up at the conference. Compared to the registration experience at prior conferences, how do you rate your experience at this years conference?	Much better than past years

Printable receipts reassure voters that their ballot has been cast correctly

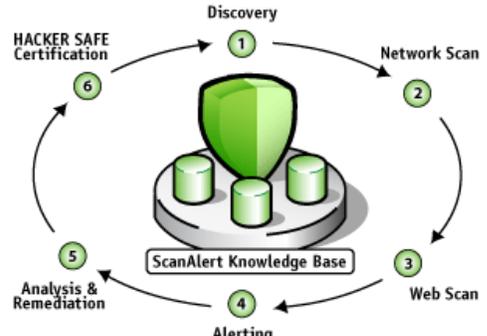


Votenet Solutions maintains the most robust, secure, and reliable network infrastructure in the online election software market, with hosting partner SAVVIS guaranteeing 99.9% network uptime. Our multi-layer network perimeter further protects your voting application, data, and results.

- **OC-12, OC-3, and T-3 bandwidth**
- **Belden Media Twist 350 Category 6 cable**
- **Private IP address** eliminates the possibility for the outside world to establish a connection directly to a machine running eBallot
- Network complies with the **RFC 1918 Internet standard**
- Constant **Trend Micro anti-virus scanning**
- **Intrusion Detection System** sensors placed through all network segments
- **Multiple robust, enterprise-class redundant firewalls and constant intrusion detection monitoring** powered by Fortinet
- **Web Application Vulnerability Testing** with 24/7/365 alert notifications if vulnerabilities detected
- **Swift issue remediation** using extensive vulnerability management portal and comprehensive technical support
- **Load balancing server configuration** evenly divides traffic, ensuring ballots and election content loads quickly and performs at optimal levels
- **Full Redundancy/Fail Over** - All networking components, VeriSign 128-bit Secure Sockets Layer (SSL) accelerators, Coyote Point equalizer, load balancers, Web servers and application servers operate in a mirrored, multi-redundancy configuration. If an eBallot Web server were to go down, another server would immediately handle the traffic, ensuring no downtime during an election.
- **24/7/365 Election Monitoring** - eBallot servers are automatically monitored 24 hours/day, every day of the year by a team of election specialists
- **HACKER SAFE certification** from ScanAlert achieved by passing rigorous daily network security audits
- **Dynamic Port Scanning** including Port-level Network Services Vulnerability Testing
- Votenet Solutions utilizes **IceSECURE, a corporate email network from IceWEB with military-grade encryption and security protocols**. IceWEB employs multiple firewalls and technologies, including anti-virus scanning, to protect confidential information transferred via email, such as voter lists sent from administrators to Votenet election consultants, from Internet predators, denial of service attacks, and hackers.



Trend Micro is a world leader in network anti-virus scanning and protection



ScanAlert protects, audits and certifies the security of the eBallot network infrastructure



Office Security

eBallot customers are protected by world-class physical security measures normally only found at global FORTUNE 500 companies and government agencies. Ensuring that every measure is taken to guard against physical intrusion to their office locations, Votenet Solutions proactively consulted with Interfor, Inc., an independent international investigation and security firm with over 25 years of experience in comprehensive domestic and foreign intelligence services to the legal, corporate, and financial communities. Votenet received Interfor's highly-regarded Physical Security Certification after intense scrutiny of their security protocols, including:

- **On-site building security guard**
- **Building visitor sign in/sign out**
- **Electronic alarm/motion detection system** monitored by 3rd party
- **24-hour video surveillance** of lobby, elevator, and suite entrances
- **Electronic access ID badge** required to enter office suite
- **Visitor sign-in/sign-out** witnessed by receptionist
- **Extremely limited access to IT systems**, encrypted password for authorized executive use only
- **Criminal background checks** conducted on each staff member and vendors at both the federal and local levels prior to hiring



Votenet Solutions, Inc.
Headquarters
Washington, D.C.



On-site security guard, electronic alarm/motion detection system, 24-hour video surveillance, electronic access ID badges just a few of the state-of-the-art physical security measures protecting eBallot customer data



Hosting Security

Ensuring the highest levels of network protection, SAVVIS datacenters provide market-leading physical security measures including:

Building Exterior

- **Unmarked, anonymous buildings**
- **Bullet-resistant exterior walls and embassy-grade concrete posts and planters** around the perimeter
- **24-hour video surveillance cameras** with digital recorders, Pan-Tilt-Zoom capabilities
- **False entrances**
- **Vehicle blockades**
- **Biometric scan, including palm scan, of personnel prior to building entrance**
- **Exterior entrances feature silent alarm systems** that notify law enforcement in the event of suspicion or intrusion

Building Interior

- **Cipher-encoded personnel ID access badges**
- **On-premise uniformed guards** to control access
- **Bulletproof glass/walls**
- **All of Votenet Solutions' equipment**, including servers, routers, switches, and storage devices are stored in locked steel Internet Data Cages (IDC)
- **Authorized personnel must pass through five levels of biometric scanning** to reach the Votenet Solutions IDC
- **Access to the IDC is monitored by time-stamped logs for historical retrieval**

Rates SAVVIS #1 North American Web Hosting



SAVVIS IDC

All eBallot servers, routers, switches, and storage devices are stored in locked steel Internet Data Cages (IDC), with access to the IDC monitored by time-stamped logs for historical retrieval



eBallot is the only online voting solution that guarantees continuous security and solution improvements to every customer. Customers are not required to manually install disks or download patches, they are available instantly and delivered automatically through their existing eBallot software.

Independent audits continuously affirm that the eBallot security infrastructure goes to great lengths to protect customer elections and confidential data. Using the latest firewall protection, encryption, and proprietary security products, eBallot gives customers the peace of mind that only a world-class security infrastructure can provide.

Our team of over 20 eBallot security experts and election technicians constantly monitor your elections and new security threats. Year after year, they succeed in upgrading our security infrastructure to ensure that every election is backed by the highest possible levels of protection.

For more information, please contact salesconsultant@votenet.com or 1-800-VOTENET.

**You Will Always Have the
Best Online Election
Security with eBallot**