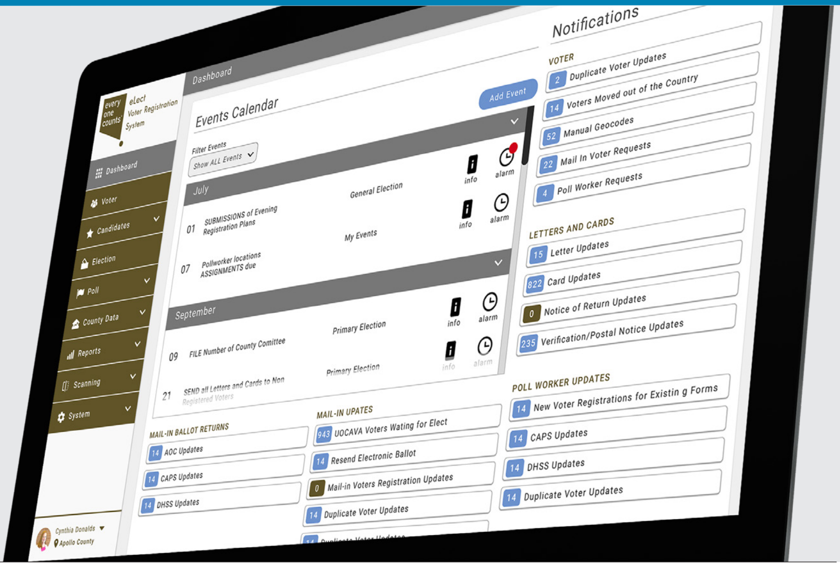
VRS SECURITY

Talking points to engage stakeholders

You've done your research and understand how important it is to have a secure voter registration system, but convincing other stakeholders of the need to upgrade and allocate budget can be challenging.

We've created a list of key points to help define your communications. They are organized starting with basic statements (perfect for introductions or transitions), then a list of ways to secure a VRS, and finally, technical specifications for various areas of VRS security. These can be used to engage all key stakeholders, and empirically justify the procurement of a secure, modern VRS.


every one counts
eLect Voter Registration System
Dashboard
Voter
Candidates
Election
Poll
County Data
Reports
Scanning
System
Cynthia Donalds
Apollo County
Dashboard
Events Calendar
Add Event
Filter Events
Show ALL Events
July
01 SUBMISSIONS of Evening Registration Plans
General Election
info
alarm
07 Pollworker locations ASSIGNMENTS due
My Events
info
alarm
September
09 FILE Number of County Comittee
Primary Election
info
alarm
21 SEND all Letters and Cards to Non Registered Voters
Primary Election
info
alarm
MAIL-IN BALLOT RETURNS
14 AOC Updates
14 CAPS Updates
14 DHSS Updates
MAIL-IN UPATES
943 UOCAVA Voters Wating for Elect
14 Resend Electronic Ballot
0 Mail-in Voters Registration Updates
14 Duplicate Voter Updates
Notifications
VOTER
2 Duplicate Voter Updates
14 Voters Moved out of the Country
52 Manual Geocodes
22 Mail In Voter Requests
4 Poll Worker Requests
LETTERS AND CARDS
15 Letter Updates
822 Card Updates
0 Notice of Return Updates
235 Verification/Postal Notice Updates
POLL WORKER UPDATES
14 New Voter Registrations for Existin g Forms
14 CAPS Updates
14 DHSS Updates
14 Duplicate Voter Updates

JUST THE FACTS:

- » Outdated voter registration systems are vulnerable to attacks—highly-publicized cyber-attacks across the country emphasize the importance of robust, modern security methods. A modern voter registration system keeps data safe and public confidence high with an encrypted database, multi-factor authentication, multiple user and role-based access controls and monitoring, and geo-failover and data recovery.
- » A secure VRS encrypts data at rest and protects that data with role-based access. Data in transit is encrypted using the TLS protocol. Sensitive, non-public data fields are individually encrypted at rest to allow matching against user input without actually storing the data in a readable format.
- » Increased security measures prevent the exfiltration of information that could then be used to submit false voter registration requests, or change current voter information.
- » Technology platforms supporting election administration must meet the current minimum encryption and data protection standards.
- » Regular updates keep security protection current, preventing a massive data breach like the Equifax breach of 2017.

SPECIFIC EXAMPLES:

- » A voter registration system that supports multi factor authentication (MFA) makes it difficult for credentials to be compromised and used by an outside agent.
- » Intelligent automated reporting tools detect abnormal activity by users; if a large set of data is changed, it's easy to tell which user made the changes and when.
- » A modern voter registration system features automated integration with external data sources such as the Department of Corrections (DOC), Department of Motor Vehicles, and National Death Index. Data is directly transferred back and forth, eliminating human error and increasing data integrity. However, those touchpoints need to be secure in order to prevent hacks. There are multiple ways to secure these processes in a modern VRS.

VRS SECURITY

Talking points to engage stakeholders

- Failure-resistant architecture allows for independent modules, which ensure no single component of the system can adversely impact the performance of the others. If there's an update to petition management, it won't slow down other components like the voter facing site. A properly-functioning, reliable system helps ensure public trust.
- A VRS built on an NoSQL database supports automatic database replication to maintain availability with automated failover and recovery, in case of outages or planned maintenance.
- Role-based access controls manage permissions to limit a user's access to resources and actions that are only necessary to performing their job. User roles are configurable to match ideal workflow or security use cases.

IF YOU WANT TO GET TECHNICAL ABOUT IT:

- VRS security should follow NIST Cybersecurity Framework, created as a result of Executive Order 13636, improving critical infrastructure cybersecurity and NIST SP 800-63 Digital Identity Guidelines. By using industry open standards and implementing additional controls on top, conformance is exceeded.
- The most secure voter registration systems use data validation methods such as insecure direct object referencing, and cross-site request forgery.
    - With insecure direct object reference controls, application code always checks for access prior to accessing an object on any and all requests.
    - Cross-site request forgery uses a short time-to-live token strategy for each request generated. If the token provided is valid, the request is allowed. If the token is not valid, a 403 (Forbidden) error is returned.
- VRS servers should utilize a web application firewall (WAF) to prevent common vulnerabilities, including SQL injection, cross-site scripting (XSS), remote file injection (RFI), and local file injection (LFI). A WAF applies rules to properly-formed HTTP requests and confidently filters out common attacks.
    - VRS networks should also use a network firewall and network intrusion protection system to block any unsolicited traffic to the system's network.
- Databases protected with Client and Member x.509 certificates ensure operations are authenticated prior to being executed on the database level.

If you would like to learn more about any of the above points in greater detail, or if there is another component of VRS you'd like to understand better, let us know and we'd be happy to provide you with more information!

For additions to this document or ideas for other resources, email contact@everyonecounts.com.

For additional tools and resources, visit resources.everyonecounts.com.