Umatilla County
Primary 2020
Post-Election Review

National Cybersecurity Center
Secure the Vote
Executive Summary

Democracy Live, an online electronic ballot return platform, recently contracted with Umatilla County, Oregon to offer electronic ballot return service to overseas voters registered in the county. The work took place between April 2020 – May 2020, covering the timeline between when absentee ballots went out and the date of the primary election.

Umatilla County has a total of **44,830** registered voters, and a total of **16,505** votes were cast for the primary. Of the total registered voters, **101** were eligible UOCAVA voters; **11** eligible UOCAVA voters returned their ballots through the Democracy Live OmniBallot platform. Umatilla County counted all **11** ballots submitted, as there were no signature discrepancies. Official results of the Umatilla 2020 County Primary Election can be found [here](#).

There appears to have been no external or internal threat of interference to the election. The National Cybersecurity Center (NCC) reviewed Democracy Live’s security logs during the election, which include an internal and external security audit. No interference with the integrity of the election was identified.

***

Introduction to Democracy Live & Electronic Voting

Democracy Live is a voting technology company and the largest provider of cloud and tablet-based voting technologies in the U.S. Democracy Live has been used in over 1,000 elections covering nearly 600 jurisdictions.

Democracy Live has developed a platform for delivering and returning electronic ballots via an online portal, hosted by Amazon’s cloud. Ballots are encrypted and stored in the cloud until they are downloaded and printed by the respective election administrators. The printed ballots are then scanned and tabulated like any other paper ballots.

Electronic Voting Security Risks

The electronic transmission of ballots is currently used in a variety of states, primarily for uniformed and overseas voters (UOCAVA). Instead of using mail, those voters can elect to receive a ballot as a fax or email attachment. They then print the ballot, and email or fax it back to the election office that serves the jurisdiction in which they are registered to vote.
As technology advances, the electronic transmission of ballots has become the seeding grounds for more progressive technological solutions. Much like how technology has transformed public and private sector service delivery, there is promise that electronic voting methods over an application or secured site might offer a more secure alternative than current email or fax methods, and can enhance voter accessibility.

However, concerns remain that these newer voting options are not sufficiently secure.¹ The National Cybersecurity Center offers a high-level view of the risks, and also describes the existing criteria for assessing whether vendors are appropriately addressing those issues.

**Risk Overview**

There is no purely risk-free election. Through intentional or unintentional errors, paper ballots can be misplaced, mail-in ballots can get stuck in ballot drop-off locations, or an election judge may not accurately catch a signature discrepancy that results in voter fraud. In addition to the risks of human error or nefarious actors, less tangible risks exist such as the risk of not making elections as accessible as possible to all registered voters.

Trade-offs exist at every level of election administration – election administrator’s efforts to be more transparent may translate to a less efficient process, or vice versa.

When it comes to the electronic transmission of ballots, the following are some of the key risks:

- **Vulnerabilities associated with network connections between the election administration and the electronic ballot image storage unit (may be a cloud, or blockchain system)**
- **Any use of removable storage devices (such as a USB) to transfer data (ballot images, for example)**
- **Underlying errors in the coding that lead to the user not being able to use the product**
- **End-to-end verifiability**
- **Security vulnerabilities inherent to the technology being used (e.g. lack of strong internal security protocols, lack of rigorous testing, lack of strong external defenses)**²

National Cybersecurity Scope

The National Cybersecurity Center’s work focused primarily on reviewing security reports conducted on Democracy Live’s technology and reviewing security policies and procedures.

Security Reviews

Democracy Live has worked with federal government agencies and the Election Assistance Commission (EAC) on improving overall election infrastructure, and is therefore well aware of the many voting system guidelines and best practices.

The Amazon Web Services Object Lock used to securely store the ballots transmitted via OmniBallot are used by several federal agencies for securing sensitive documents, so the technology is accepted.

An MIT and University of Michigan joint report was recently published that offered critiques to improve the security of the OmniBallot tool.

The MIT report, published June 7, 2020, identified the following key risks:

- Susceptibility to malware and other infections on a user’s device
- More stringent security for personally identifiable information

Democracy Live has offered the following response to the security concerns:

- **Voter ID to Google Analytics** – This was a legacy workaround which is no longer needed. They are removing in the next release.
- **Do not load Google Analytics or PDF.js (they say Cloudflare for this) from remote servers** – They are looking into this for the next release.
- **Privacy Policy** – Democracy Live has posted a Privacy Policy to their website and the next release of their voter portal includes a reference to it along with a custom privacy policy for the counties with whom they work.

Security Policies & Procedures Review

The National Cybersecurity Center reviewed the incident response log for Democracy Live during the primary election.

Internal Security Review

The internal security review included an overview of access to the root account (main access point to the secured storage of ballots); employee downloads of ballots; employee modification or deletion of voter ballots or packages; and modifications to the audit logs.
Democracy Live has created alerts for the use of the root account; disabled access on the part of employees to download any voter ballots or packages; and relies on the Object Lock's Write Once, Read Many model to mitigate against modification and deletions of files.

Finally, Democracy Live limits employee access to any audit logs, restricting access to root account users.

There were no incidents of internal security breaches found during the primary election period.

*External Security Review*

Democracy Live monitors for external security threats such as Denial of Service (DOS/DDOS) attacks and SQL injection attacks. During the Umatilla County Primary Election, the system detected probe attacks against OmniBallot. The attacks were relatively simplistic, and did not exhibit features of targeted attacks. The attacks did not result in any system downtime or data loss.

The OmniBallot system detected potential SQL injection attacks; however, all requests were blocked by the firewall.

The National Cybersecurity Center recommends that Democracy Live continue to supplement its policies and procedures, and security protections with an added layer of auditability that lies in an external capability to compare the ballot images of the ballot voted by the voter, the ballot stored in the cloud, and the ballot printed and tabulated.

**Key Findings & Recommendations**

The National Cybersecurity Center **did not find any issues with the audit logs that would lead to concerns that there was any internal or external tampering of the results.**

We are also committed to furthering the security and transparency of the electronic transmission of ballots, and therefore make the following recommendation for ongoing progress:

- **Identifying a way to confirm that the ballot images are the same within the system and without; essentially a way to externally verify a full end-to-end process.**
<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forrest Senti</td>
<td><a href="mailto:Forrest.Senti@cyber-center.org">Forrest.Senti@cyber-center.org</a></td>
<td>931-249-8245</td>
</tr>
<tr>
<td>Mattie Gullixson</td>
<td><a href="mailto:Mattie.Gullixson@cyber-center.org">Mattie.Gullixson@cyber-center.org</a></td>
<td>703-943-7128</td>
</tr>
</tbody>
</table>