Voatz Election Audit

Utah Republican Party Convention

National Cybersecurity Center
Secure the Vote

TABLE OF CONTENTS

Executive Summary

The COVID-19 pandemic has created extraordinary circumstances under which election offices and political parties must administer elections. Social distancing and stay-at-home orders have complicated the accessibility and safety of elections, requiring organizations to look to alternative voting methods other than traditional in-person, or even mail-in voting.

The Utah Republican Party opted to operationalize an electronic mobile voting application for the state party convention, which occurred April 25, 2020. The vendor selected for the electronic mobile voting application is Voatz, Inc. The National Cybersecurity Center (NCC) was selected to conduct a third-party, independent review of the votes cast and tabulated, and to review the overall security procedures to assess any issues.

A total of **3,580 votes** were cast during the convention; of those **3,340** were cast via the Voatz mobile application and **240** were cast through Vote by Voice call. Results of the convention election may be found here.

After review, there appears to be no external or internal threat of interference to the convention. The NCC coordinated the public citizen's audit of the votes cast through the Voatz application through poll workers.

The NCC deems this election successful based on the criteria of no interference with the application (internal or external), and in this convention election, a confirmation that stored ballot images match a voter's verified ballot receipt.

***

Introduction to Voatz & Electronic Voting

Voatz, Inc. is a "mobile elections platform"[1] developed to allow voters to cast their ballots via mobile devices such as smartphones and tablets. Voatz was founded in 2015 and began formal operations in 2016; over 80,000 ballots have been cast using the blockchain-based technology since its inception.

The Voatz application may be downloaded onto a individuals' personal smart device. Devices must have newer technologies to be used effectively; for iPhones, users must have the iPhone 5s or newer, and Android handsets from 2016 on are supported.

[1] https://voatz.com/faq.html

Once the application is downloaded, voters confirm their identity by scanning their driver's license or passport, taking a 'selfie' with their phone or tablet, and then using the fingerprint scanner to confirm the submission of the identity. The voter's identity is then confirmed with the respective state's voter records to ensure the individual is a registered voter in the jurisdiction. As an additional mode of verification for entities that don't require ID scan, the Voatz platform enables alternative methods of identity verification.

Once the voter has verified their identity, candidate choices or ballot questions appear one contest at a time; selections are made by tapping the desired choice. The voter submits their ballot, and the information is anonymized and posted to the blockchain. For governmental elections, the results are then generated into a paper ballot that is scanned and tabulated by the respective elections office.

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.[2] 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

[2] https://www.nationalacademies.org/news/2018/09/securing-the-vote-new-report

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)[3]

National Cybersecurity Scope

The National Cybersecurity Center's work focused primarily on reviewing security reports conducted on Voatz's technology, coordinating a citizen audit of the system, and reviewing security policies and procedures. Therefore, our work focused primarily on assessing the risk of the first, third and fourth security framework points. Our findings are as follows.

Security Reports & Notable Revisions

Voatz has worked with several technical security firms to review their product for testing and feedback. The National Cybersecurity Center reviewed the findings of the Trail of Bits report as the primary source of open feedback in addition to the CISA's Hunt and Incident Response Team (HIRT) overview. The NCC recognizes that a team from MIT published a report as well. However, given that their efforts do not appear to have been in collaboration with the company, we are concerned that the approach taken by MIT undermines the rigor of their findings.

[3] These risks are generally applied to conversations surrounding the electronic transmission of ballots; we specifically reference the following document as an outline: https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

Trail of Bits

The Trail of Bits report, published March 11, 2020 identified three high-level priority areas requiring attention that are listed below:

- More stringent cryptographic protocols
- More stringent data protection protocols
- More aggressive data validation protocols

Voatz has addressed several of these issues, and identified those changes here.

HIRT Report

The HIRT team specifically worked to identify vulnerabilities surrounding threat actor behaviors, and identified some areas for strengthening defenses. These issues, and Voatz' response, may be found here.

Security Policies & Procedures Review

The National Cybersecurity Center reviewed the incident response and security policies and procedures for Voatz. The purpose for this review is to assess the comprehensive security culture, which enables the vendor to prevent, detect and respond to internal and external security interference.

Voatz has implemented a detailed incident response checklist, along with policies and procedures that define and categorize various security issues and the appropriate responses and mitigation efforts. Voatz also has a third-party vendor vetting system in place to ensure that any subsequent vendors meet the security standards Voatz has established.

The National Cybersecurity Center recommends that Voatz continue to supplement these policies and procedures with a broader elections context to help ensure that the security procedures match what would be expected in more traditional election systems.[4]

[4] An ongoing challenge with electronic voting systems is developing a means for third-party auditors to review ballot images outside of the vendor's system. With that added level of transparency, the National Cybersecurity Center is confident that electronic voting systems would be able to enhance public trust and the accountability of their systems.

Voatz Mitigation Activities - UT GOP Convention

The NCC reviewed Voatz' threat mitigation report after the convention election. There were limited threats detected and mitigated.

- Man-in-the-middle attacks – There were 35 incidents of exposure to malicious attacks on the transmission of data from the voter to the cloud; these incidents were the result of voters' connections to insecure Wi-Fi, and were detected immediately and resolved by encouraging the users to switch to a secure Wi-Fi connection. The issue was detected for both iOS and Android users prior to votes being cast such that the application does not work unless there is a secure network connection.
- Device pin not set – Some voters did not have a pin set on their device, which was again detected by the Voatz software prior to a vote being cast. The voters were asked to set a device pin (thereby enhancing their overall security), and the application proceeded to allow the voter to vote
- Device malware – Some devices were identified to have separate applications downloaded that contained malware. Again, the application did not allow the voter to vote until the separate applications containing malware were deleted, and the phone was rebooted.

The security protocols within the Voatz application highlighted security vulnerabilities on voters' devices, meaning that the application has inherent security features that instinctively prevent its use in insecure environments. The security features, coupled with the internal policies and procedures translates, to a substantially secure ecosystem for votes cast in the Utah GOP Convention.

Audit Overview

The National Cybersecurity Center worked with the Utah GOP Party to recruit poll workers to assist with the citizen audit. The audit will remain open until June 30, 2020 to allow for ongoing participation and review, and a full addendum will be released at that time.

The audit for this political convention includes reviewing the ballot receipts generated for each voter with the ballot's stored blockchain data. This enables auditors to confirm that all ballot results remained consistent from the voter to the tabulation conducted on blockchain.

One auditor reviewed 140 ballots, another reviewed 48 ballots in a different batch, and a final reviewer reviewed 50 ballots in another batch of ballots, which equals 7 percent of the total ballots cast via the mobile application.

While risk limiting audits are a tool used to assess the accuracy of votes tabulated, we believe the approach taken to conduct the audit may have some applicability with regards to citizen's audits of votes cast electronically.

Due to the higher-than-normal volume of the votes cast in this election, the votes have been 'batched' to allow auditors to review different groupings of ballots for any issues. The audit process is therefore conducted in a way that allows for ballot comparison (a comparison between the image of the voter's verified ballot receipt and the blockchain data for tabulation).

In this citizen audit, no issues were reported thus far. National Cybersecurity Center staff also audited batches and found no discrepancies.

As noted in a previous footnote, these citizen audits offer voters the chance to review anonymized ballots to ensure consistency between the ballot images and blockchain data. However, one of the ongoing challenges with all electronic voting systems is developing a method to compare ballot images outside of the vendor's system. The National Cybersecurity Center looks forward to that step being implemented in order to create additional confidence and transparency.

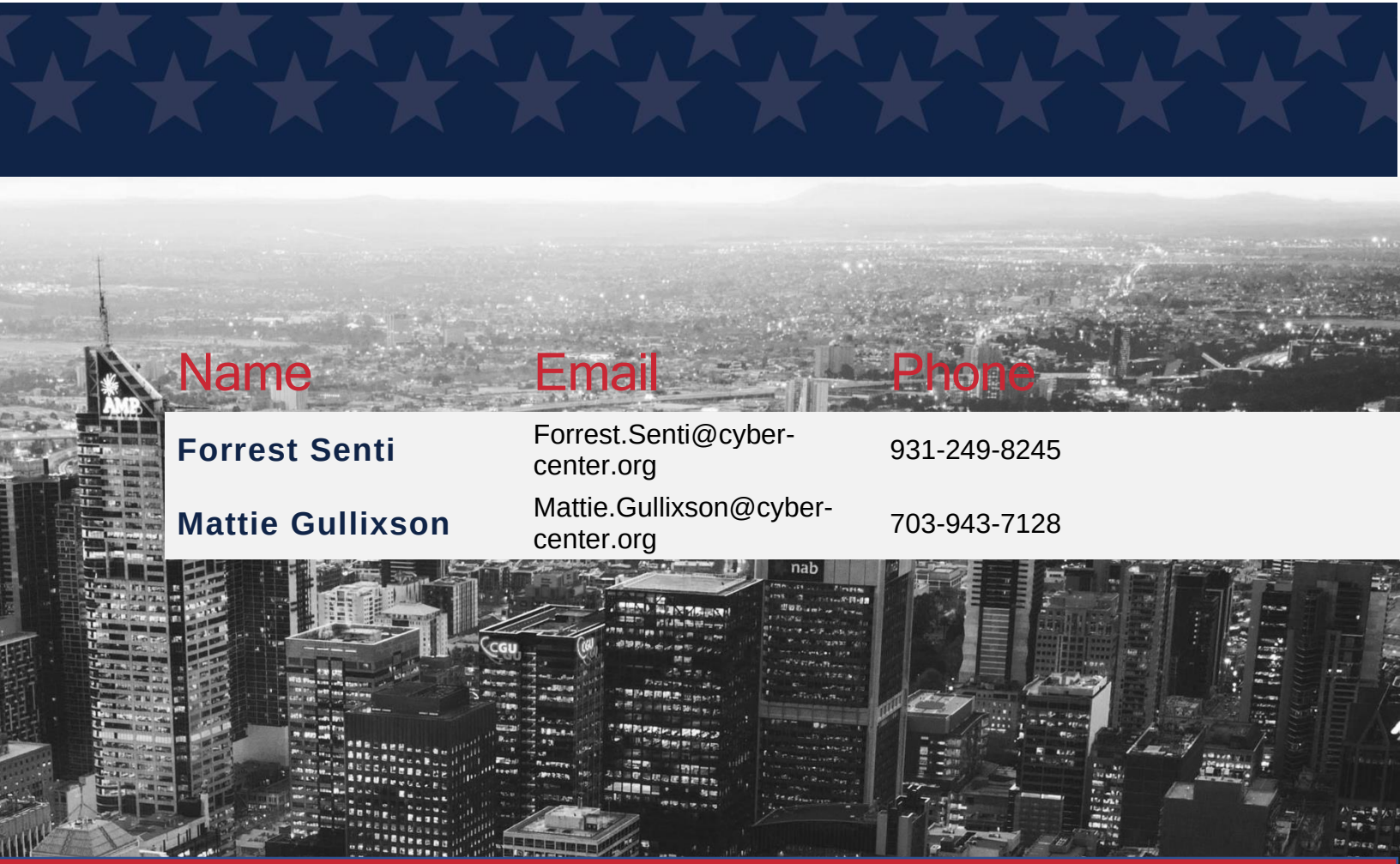
Key Findings & Recommendations

The National Cybersecurity Center has conducted citizen audits for Voatz on a variety of pilot projects. **We do not find any issues with the audit that would lead to concerns that there was any internal or external tampering of the results.**[5]

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

- An independent node for a third party to review
- Provide additional information and resources for auditors to discuss results
- 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.

[5] It should be noted that this audit includes a review of ballot images contained within the Voatz system, such that the results of the audit are only able to confirm that there was no discrepancy between the image of the ballots cast, recorded, and the resulting paper ballot tabulated. The NCC is working to identify additional verification opportunities that will strengthen the results of the audit.



Name	Email	Phone
Forrest Senti	Forrest.Senti@cyber-center.org	931-249-8245
Mattie Gullixson	Mattie.Gullixson@cyber-center.org	703-943-7128

National Cybersecurity Center

Contact Information