

Behind the Scenes: A Security Story

When solving the voter access challenge, the most significant objection West Virginia faced concerned security. The State had found the technology partners, a solution that satisfied security criteria, met the standards for voter ease of use, the ability to audit, and full integration with their existing infrastructure.

During the 2018 midterm election pilot, the Voatz system detected and blocked several unsuccessful attempts to gain entry to the West Virginia election. Election officials, the West Virginia leadership and Voatz were ready for these attempts, having implemented a system built on a multi-layered approach to defense.

The West Virginia pilot project not only answered the pressing question of how to provide access to voters, but also successfully identified, thwarted, and reported to the jurisdiction all attempts to tamper with the system. **This proved for the first time that it is indeed possible to build a resilient remote voting system - one that detects, blocks and reports attempted attacks.**

West Virginia Pilot Timeline	
SEP 2018	Voting with Voatz pilot in West Virginia begins
OCT 2018	Voatz blocks, thwarts attempted entry on its live system
NOV 2018	At the completion of the election, Voatz shares all attempted attacks on its live system with West Virginia
NOV 2018	West Virginia refers unsuccessful attempt to law enforcement
OCT 2019	U.S. Attorney's Office releases statement about their investigation
OCT 2019	West Virginia releases statement about their reporting and subsequent investigation
OCT 2019	Media and activists misreport that Voatz reported a researcher to the FBI, and continue to propagate misinformation

The West Virginia pilot has proven to be an ideal test case, setting a standard for election pilots and work across the country. This has quieted many voices of opposition, though a few of the loudest continue to call for an end to all work in this area.

Perhaps the most difficult and staunch opponents went so far as to mischaracterize the successful election pilot and security data points. **It has even been misreported in multiple publications that Voatz reported hackers and researchers to the FBI, or intended to harm researchers. As we have repeatedly **confirmed**, this is blatantly false.**

As stewards of our critical infrastructure, representatives of West Virginia called upon the US

Attorney's Office and held a press conference to issue their report on the attack, which reflected a system that was successful in warding off attempted entry.

At this event, United States Attorney Mike Stuart issued a **strong statement** emphasizing the seriousness of election security.



U.S. ATTORNEY MIKE STUART

“ If you are a party – any party – or an individual – any individual – that intentionally compromises or attempts to intentionally compromise our election systems, the security related to our election systems, or the legitimacy of the votes cast by citizens, **my office will prosecute you to the fullest extent of the law.** Free and fair elections are a critical foundation to the maintenance of liberty.

Whether in the name of an academic exercise, a mere challenge or thrill, or to actually cause harm, we will treat every risk extremely seriously and as a threat to “Critical Infrastructure.” Even a mere attempt is unacceptable. If you do the crime, be ready to do the time. Our election systems are sophisticated with many electronic fingerprints that will lead us exactly to the violators of our secured systems. **Don’t do it. Don’t even think about it.** ”

Throughout all pilots, our commitment has been to the process of learning and sharing information that will chart a way forward to a resilient election system. This is an ongoing challenge that requires collaboration, development, piloting, and auditing.