Electronic Ballot Return – Overview

Professor Jonathan Katz, Department of Computer Science, University of Maryland

Why Electronic Ballot Return?

Every state in the country is required by federal law to offer electronic ballot delivery to eligible voters serving in the military and living abroad. 31 states require eligible voters to have the option for electronic ballot return.

Beyond voters covered under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), there are many voters with disabilities who cannot see, hold, or mark a paper ballot. Electronic ballot return offers a way for such voters to vote privately and independently from home.

Additionally, natural disasters such as hurricanes, wildfires, pandemics, domestic terrorism, or other unknown emergencies may once again make in-person voting difficult or impossible. Electronic ballot return may be the only option for voters in that case.

The opinion of many (but not all) cybersecurity experts about electronic ballot return is simply "don't do it." However, that ignores the reality that many state laws mandate electronic ballot return, and that many states already offer electronic ballot return via fax and/or email. It also discounts the needs of disabled voters, and the potential for another voting emergency in the middle of an election year.

Current Electronic Ballot Delivery and Return Options

As noted above, all 50 states require electronic ballot delivery, while 31 states also require the option for electronic ballot return. The majority of states comply with these laws by mandating fax or email as the only allowed methods of electronic ballot return. A few states are starting to use Web portals to comply with their state electronic ballot return laws. This paper aims to highlight the differences between email, fax, and Web-portal mechanisms for electronic ballot return, while suggesting best practices that apply to these approaches.

[1] The author is a professor in the Department of Computer Science, University of Maryland, and may be reached via email at jkatz@cs.umd.edu. This report was written under a consulting agreement with Democracy Live. The opinions expressed herein do not necessarily represent the positions or opinions of the University of Maryland or the State of Maryland.

Comparison Table: Email, Fax, and Web-Portal Ballot Return

(The column for a web portal corresponds to the OmniBallot system from Democracy Live, however other systems may offer similar functionality.)

	Email	Fax	Web Portal
Paper Ballot Trail	**X**	**X**	**X**
Uses Internet or Other Public Network	**X**	**X**	**X**
Accessible for Voters with Disabilities			**X**
Voter Verified Ballot	**X**	**X**	**X**
Security Audits Available			**X**
Follows NIST Cybersecurity Framework			**X**

A comparative analysis of different techniques for electronic ballot return was conducted in May, 2020.[2] The following summarizes some conclusions of that analysis.

Fax	"Fax has no security protections unless sent over a secured phone line and is generally not considered suitable for sensitive communications."
Email	"Email provides limited security protections and is generally not considered suitable for sensitive communications. Email may be viewed or tampered with at multiple places in the Return process…"
Web Portal	"While web applications support stronger security mechanisms than email, they are still vulnerable to cyberattacks…."

The above chart indicates that any electronic ballot return method carries some level of risk. No voting system (including in-person voting and paper tabulation) is 100% secure. Therefore, state and local elections authorities must carry out their own risk/benefit analysis when determining which electronic ballot return method to use.

Electronic Ballot Return - Best Practices

Where electronic ballot return is being used, elections officials should consider the following best practices:

[2] The entire report is available at https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf

1) Ensure a full independent security review has been conducted on the ballot return system.

2) Ensure the ballot return process meets basic security guidelines such as the NIST Cybersecurity Framework.

3) Ensure the system meets accessibility requirements for blind and disabled voters.

The following best practices relate specifically to ballot return through a web portal:

1) The portal should be hosted in a FedRamp-compliant cloud.

2) The portal should offer a ballot verification option to allow voters to confirm their ballot was accurately returned using an independent device.

3) It is recommended that further pilots, tests, and security reviews be conducted before the portal is expanded beyond voters who cannot independently vote a paper ballot by mail or at a polling location.

Summary

Many states are currently using email and fax for ballot return. However, email and fax systems are likely less secure than solutions using a web portal hosted in a FedRamp-compliant cloud. Given that it takes only one compromised ballot to cause doubt or uncertainty on an election, it is recommended that state and local elections officials look beyond outdated fax and email ballot return methods. Cloud-based solutions that meet the best practices listed in this document, offer a viable, potentially more secure option for electronic ballot return.