



UNIVERSITY OF WASHINGTON

CIAC

CENTER FOR INFORMATION ASSURANCE AND CYBERSECURITY

November 28, 2021

RE: Beyond Fax and Email: Securing Electronic Ballot Transmission

The purpose of this letter is to illustrate the need to modernize and secure the electronic transmission of ballots, both to and from eligible voters, as required by federal and state laws. This paper encourages state and local elections officials to replace outdated methods of electronic ballot transmission such as fax machines and email attachments. This brief reviews alternatives to fax and email ballot transmission, such as cloud solutions, that fully meet NIST cybersecurity framework standards.

“Online Voting” versus “Electronic Ballot Transmission”

Terminology matters. From our review, cloud-based ballot transmission technologies often get intertwined with “online voting systems”, or “Internet voting systems”. The National Institute of Science and Technologies (NIST) defines a voting system as a software that “programs, controls, and supports the equipment that is used to define ballots; to cast and count votes; to report and/or display election results.” The cloud-based electronic ballot transmission portal reviewed for this brief, does not include any of the items required to be listed as a “voting system” and thus cannot be defined as an online, or Internet voting system.

Below is a list of key differences between “online voting systems” and the cloud-based, electronic ballot transmission system we reviewed for this brief.

- Electronic ballot transmission does not tabulate any ballots.
- 100% of the ballots submitted via the cloud generates a paper ballot which is printed directly onto ballot stock, eliminating manual ballot duplication, protects voter privacy and ensures a paper trail.
- The voter must verify the ballot before submitting via electronic submission.
- Every voter has the option to print the ballot and return by mail. (If postal services exist in their region of the world.)
- Voters must submit a handwritten signature, or other proof of identity as proscribed by law.
- The ability to conduct a full recount of paper ballots is always available.

How Cloud-based, Electronic Ballot Transmission Works

Cloud computing is leveraged to transmit a ballot electronically to the voter and back to the election office. The voter’s signature, or voter credentials are reviewed and if approved, the ballot is printed. This digital-to-paper process results in a voter verified paper ballot that may be used for a full paper re-count of the election if necessary.

The federally approved cloud acts as the equivalent of the post office. For the purposes of this brief, we reviewed OmniBallot by Democracy Live, fully hosted in the Amazon (AWS) cloud.

Executive Director, Center for Information Assurance and Cybersecurity
Professor, University of Washington
endicott@uw.edu

Fax, Email, or Cloud Ballot Transmission

Where most elections jurisdictions are currently using fax and email to comply with ballot transmission laws, cloud-based document (ballot) transmission has strong potential to heighten ballot security, while also expanding accessibility. Consider the current uses of the cloud:

- IRS.gov – cloud-based
- Healthcare.gov – cloud-based
- National Security Agency (NSA) and most federal defense and security agencies now use the cloud
- Bank Deposits – cloud-based
- Real Estate and Financial Services - cloud-based

Cloud-based document transmission technologies, including electronic ballots, offers both a digital and paper audit trail. Tracking the chain of custody of ballots may even be easier via the cloud because data transactions are highly auditable and recoverable. Every byte and every bit of every digital ballot is accounted for.

Background

In 2010, the Federal MOVE Act requires all fifty states and over 8,000 elections offices to electronically transmit ballots to military and overseas voters.ⁱ Additionally, thirty-two states allow military and overseas voters (called UOCAVA voters) to return ballots electronically. Most states and jurisdictions comply with federal and state electronic ballot transmission laws by using fax machines and email attachments.ⁱⁱ

Transmitting ballots electronically: Federally approved cloud, email, or fax machine?

It is well established that the use of a secure, government approved cloud offers more security protections than common email or fax machines in the transmission of critical/classified documents.ⁱⁱⁱ For example, in 2021 the National Security Agency (NSA) recently selected cloud computing to securely protect some of the nation's most critical and classified documents.^{iv} Not a single federal agency has approved fax machines or common email to transmit critical or classified documents.

Three million Eligible Voters – It Takes Only One.

Three million voters in the U.S. are eligible to receive an electronic ballot.^v With little to no security protections, it is only a matter of time before a malicious actor intercepts and compromises an unsecured email, or fax machine. As seen in the post-2020 Presidential election, it takes little (if any) evidence of election manipulation to cause doubt and distrust in the outcome of an election. Of the three million voters that are eligible to receive an electronic ballot, it takes just one compromised fax or emailed ballot promoted in national and social media to sow substantial doubt in an election; however, we cannot give up access to the ballot because we cannot reach perfection.^{vi} We can use cloud-based solutions to reduce the probability of compromised ballots. We can apply the same cybersecurity managed detection and response used by the federally approved cloud-based portals cited above.

Email and Fax – No voter privacy. Manual ballot manipulation required.

In addition to security vulnerabilities, there are no privacy controls around transmitting ballots via email attachments, or fax machines. A prominent number of cybersecurity hacks are pushed through email using a process known as phishing, relying on the user's lack of awareness not to click on certain emails^{vii}. Unlike current cloud-based technologies, every voter submitting their ballot via fax or email must waive their right to a private ballot. Ballots being returned via email, or fax are subject to manual ballot duplication by elections staff.

Leveraging cloud computing to more securely transmit ballots

Given federal and state laws requiring electronic ballot transmission, it is not a question of whether to transmit ballots electronically, it is a question of how to transmit ballots more securely. If federal agencies are transmitting sensitive documents over the cloud, there is a likelihood that we can securely transmit cloud-based ballots as well.

Cloud-based ballot transmission – Security upgrade.

Several states have begun leveraging cloud computing to comply with federal and state laws, or legal rulings that mandate equal access to remote voting (absentee). For this brief, we refer to a study on cloud-based electronic ballot transmission at the University of Washington’s Center for Information Assurance and Cybersecurity. This study used graduated, certified students in Cybersecurity Risk Management, and both research and teaching faculty, to review the most commonly deployed cloud-based electronic ballot transmission technology (OmniBallot from Democracy Live). We examined cloud-based cybersecurity vulnerabilities and compared them to email and fax machines^{viii}.

Electronic Ballot Comparison

Table 1 below shows key security benefits of leveraging a cloud-based electronic ballot transmission solution, versus email and fax machines. Although no solution is free from security risk, based on this review we strongly advise policy makers and elections officials to move toward cloud-based electronic ballot transmission, avoiding email and fax ballot transmission wherever possible.

Amazon Web Services (AWS) hosts the balloting portal we reviewed. AWS possesses FedRamp compliance which authorizes use by the U.S. Department of Defense, FBI, DHS, NSA, CIA, and several other federal agencies. Looking specifically at the use case of electronically transmitting ballots, there are key cybersecurity requirements that any electronic ballot transmission solution should include:

Table 1. Electronic Ballot Transmission Comparison

Cybersecurity Capabilities	Email	Fax	Cloud Solution
Reviewed by independent security lab(s)	N	N	Y
Auditable by third parties	N	N	Y
Verifiable by voters	N	N	Y
Offer voter privacy	N	N	Y
Capable of mitigation in the event of a compromise	N	N	Y

Conclusion

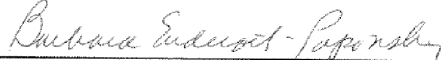
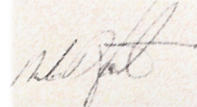
The U.S. Federal Directive issued on May 21, 2021 instructed all federal agencies to immediately move toward cloud computing, stating specifically: “(federal agencies) must prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance.”^{ix} All U.S. federal agencies are moving to the cloud for broader security and protection of classified and critical documents. We conclude ballots are better protected in the cloud than email attachment and fax machines.

Electronic ballot transmission goes beyond UOCAVA voters and extends to voters with disabilities and other populations of voters who cannot vote in-person, or on a paper ballot. Such otherwise disenfranchised voters can use public infrastructure such as libraries, home computers and personal mobile devices for full, secure enfranchisement. Given the current use of outdated email and fax to transmit ballots, elections administrators should instead consider leveraging the same cloud-based systems that secure our national banking systems, financial systems, defense systems, and other trusted systems to ensure all eligible voters have access to voting.

Ongoing pilots and scalable implementations would serve to provide additional scientific-based evidence on the cybersecurity threats, mitigations and validations for secure ballot transmission.

We encourage ongoing funding and research pilots into cloud-based ballot transmission. Support of pilots and implementations of cloud-based ballot transmission will allow a reasonable and verifiable way to measure and secure this critical component of elections infrastructure.

Sincerely,

	
<p>Dr. Barbara Endicott Popovskiy Executive Director of the Center for Information Assurance and Cybersecurity at the University of Washington</p>	<p>Mike Hamilton, CEO, Critical Insights Cybersecurity Field Experience in Municipal Settings</p>
<p>Cybersecurity Professor, University of Washington, University of Hawaii at Manoa Affiliate Professor, Master of Infrastructure Planning and Management Fellow, American Academy of Forensic Scientists Fellow, Aberystwyth University, Wales</p>	<p>Former CISO for the City of Seattle.</p>
<p>Executive Director, Center for Information Assurance and Cybersecurity Center for Information Assurance and Cybersecurity in Education. University of Washington University of Hawaii Manoa Center for Information Assurance and Cybersecurity in Research, Applied Physics Lab Seattle, WA Professor University of Hawaii at Manoa Affiliate Professor at University of Washington Bothell Computer Science and Systems Affiliate Professor, Master of Infrastructure Planning and Management, University of Washington Fellow, American Academy of Forensic Scientists Fellow, Aberystwyth University, Wales www.uwb.edu/ciac bendicot@hawaii.edu</p>	<p>Michael Hamilton; Michael has served as Cybersecurity Policy Advisor for Washington State, Vice-Chair of the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), Chief Information Security Officer for the City of Seattle, and Managing Consultant for VeriSign Global Security Consulting. In a previous life, he developed algorithms for hyperspectral remote sensing as an Ocean Scientist at the NASA Jet Propulsion Laboratory.</p>

In 2021, Governor Inslee’s appointed Dr. Endicott-Popovskiy to a National Governor’s Association Committee. exploring whole-of-state cybersecurity in the state of Washington. Recently, the NSA named her co-PI on a multi-million-dollar NSA Grant, with the purpose of creating a five-state consortium (Washington, Oregon, Idaho, Colorado, Hawaii) focused on elevating the threshold of cybersecurity awareness and preparedness within our national critical infrastructure.

End notes

¹ Uniform Law Commission. 2010. Military and Overseas Voter Empowerment “MOVE” Act. Pub. L. No. 111-84, §§ 577-83(a). https://www.eac.gov/sites/default/files/document_library/files/Military-and-Overseas-Voter-

[Empowerment-%E2%80%9CMOVE%E2%80%9D-Act.pdf](#)

Last Accessed – 11/29/2021

ⁱⁱ National Conference of State Legislatures. Electronic Transmission of Ballots. 2019. Washington DC.

<https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx>

Last accessed 11/29/2021

ⁱⁱⁱ Katz, J. 2020. Electronic Ballot Return Overview. University of Maryland .

<http://www.cs.umd.edu/~jkatz/electronic-ballot-return.pdf>

Last accessed 11/29/2021

^{iv} Konkel, F. NSA Awards Secret \$10 Billion Contract to Amazon. 2021 - Nextgov Website. Last accessed:

<http://www.cs.umd.edu/~jkatz/electronic-ballot-return.pdf>

^v FVAP.gov Federal Voting Assistance Program. 2018. [Overseas Citizens](https://www.fvap.gov/info/interactive-data-center/overseas). <https://www.fvap.gov/info/interactive-data-center/overseas>.

Last accessed 11/29/2021

^{vi} Endicott-Popovsky, Barbara. 2015. A Probability of 1. Cybersecurity and Information Systems Information

Analysis Center. Volume 3, Issue 1. <https://csiac.org/articles/a-probability-of-1/>

Last accessed 11/28/2021

^{vii} Verizon. 2021. Verizon Data Breach Investigators Report. 2021. Executive summary. Download from their website

^{viii} Endicott-Popovsky, B., McCullough, K., Ayala, A., Liang, S. Hamilton, M. In process. Working title: Electronic Voting Cybersecurity Vulnerabilities, Mitigations and Validations.

^{ix} Executive Order on Improving the Nation's Cybersecurity | The White House. May 21, 2021