



# UNIVERSITY OF WASHINGTON

## CIAC

CENTER FOR INFORMATION ASSURANCE AND CYBERSECURITY

November 28, 2021

To the Honorable Secretaries of State, Elections Directors and Cybersecurity Staff

RE: Beyond Fax and Email: Securing Electronic Ballot Transmission

We are writing to support provision 1081 in H.R. 4350, the National Defense Authorization Act for Fiscal Year 2022. This provision would fund the electronic transmission of voter ballots for UOCAVA voters. The purpose of this letter is to illustrate the need to modernize and secure the electronic transmission of ballots, both to and from the voters, as required by federal and state laws.

Section 1081 of the NDAA improves elections security by funding pilots to replace outdated methods of electronic ballot transmission currently used by a majority of state and local elections jurisdictions. The pilot funding allows for testing of a federally approved cloud, that fully meets NIST cybersecurity framework standards. To be clear, cloud-based ballot transmission is not “online voting.” Unlike online voting systems, cloud-based ballot transmission meets each of the following:

- 100% of the ballots submitted via the cloud generate a paper ballot which election offices must approve for processing before tabulation.
- The voter must verify the ballot before submitting via electronic submission.
- Every voter has the option to print the ballot and return by postal mail if that option exists in their area of the world.
- The process returns a handwritten voter signature, or other voter credential as required by state laws
- Unlike the current methods of fax and email ballots transmission, the electronic ballot enables the voter to independently review and confirm the ballot submitted was the ballot received.
- Cloud based balloting does not tabulate any ballots.

In short, the secure cloud is transmitting a ballot to the voter and to the election office which results in a voter verified paper ballot. The secure cloud acts as the equivalent of the post office. Where most elections jurisdictions are currently using fax and email to comply with ballot transmission laws, Section 1081, provides funding to pilot cloud-based document (ballot) transmission. Consider the current uses of the cloud.

- IRS.gov – cloud-based
- Healthcare.gov – cloud-based
- National Security Agency (NSA) – cloud-based
- Deposit checks with a mobile phone camera and sending it to the bank
- Transmitting real estate documents, signatures, and funds through the cloud

---

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

Each cloud-based transmission technologies, including electronic ballots, has an audit trail. Tracking the chain of custody of ballots may even be easier via the cloud because data transactions are highly auditable and recoverable.

## **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.<sup>i</sup> 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.<sup>ii</sup>

## **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.<sup>iii</sup> 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.<sup>iv</sup> 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.<sup>v</sup> 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.<sup>vi</sup> 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<sup>vii</sup>. 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, as well as legal opinions 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. We are examining cloud-based cybersecurity vulnerabilities and comparing them to email and fax machines<sup>viii</sup>.

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 electronic document (ballot) transmission solutions should provide:

Table 1. Electronic Ballot Transmission Comparison

Cybersecurity Requirements	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

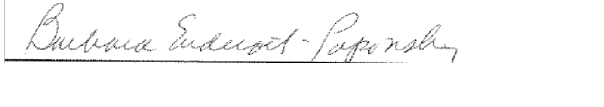

The U.S. Federal Directive issued on May 21st instructs all federal agencies to immediately move toward cloud computing, stating specifically: “(federal agencies) must prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance.”<sup>ix</sup> For the same cybersecurity reasons all U.S. federal agencies must move to the cloud ... and so should electronic ballot transmission.

We believe that the pandemic has changed the urgency of adopting cloud-based technologies in all areas of our public and domestic life, including social equity in voting. Electronic ballot transmission goes beyond UOCAVA voters and extends into populations that are restricted from access to voting. Section 1081 funds pilots to explore more secure methods of delivering and returning electronic ballots to eligible voters in remote locations around the world. Such voters can use public infrastructure such as libraries, home computers and personal mobile devices for transmitting ballots. Given the current use of 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.

Passage of Section 1081 would serve to provide scientific-based evidence on the cybersecurity threats, mitigations and validations required for secure ballot transmission. Section 1081 of the NDAA ensures essential ongoing pilots and research into this critical area of elections security.

We encourage members of Congress to support Section 1081 of the NDAA. Passing the provisions in Section 1081 will allow a reasonable and verifiable way to measure and secure this critical component of elections infrastructure.

Sincerely,

	
Dr. Barbara Endicott Popovskiy Executive Director of the Center for Information Assurance and Cybersecurity at the University of Washington	Mike Hamilton, CEO, Critical Insights Cybersecurity Field Experience in Municipal Settings
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	Former CISO for the City of Seattle.
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 <a href="http://www.uwb.edu/ciac">www.uwb.edu/ciac</a> <a href="mailto:bendicot@hawaii.edu">bendicot@hawaii.edu</a>	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.

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

<sup>1</sup>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](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

---

<sup>ii</sup> 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

<sup>iii</sup> 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

<sup>iv</sup> 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>

<sup>v</sup> 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

<sup>vi</sup> 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

<sup>vii</sup> Verizon. 2021. Verizon Data Breach Investigators Report. 2021. Executive summary. Download from their website

<sup>viii</sup> Endicott-Popovsky, B., McCullough, K., Ayala, A., Liang, S. Hamilton, M. In process. Working title: Electronic Voting Cybersecurity Vulnerabilities, Mitigations and Validations.

<sup>ix</sup> Executive Order on Improving the Nation's Cybersecurity | The White House. May 21, 2021