Secretary of State

Kim Wyman

Clearinghouse Elections Notice

Title: Processing Ballots Returned Electronically

Clearinghouse Elections Notice
Issue #18-05
September 20, 2018

This Clearinghouse is reissued to reflect changes in WAC and replaces Clearinghouse #12-08, Processing Electronic Ballots.

The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) includes any voter that is in the military, reserves, certain military dependents, and overseas voters. WAC 434-235-010 includes definitions for both the state "Service Voter" and the federal definition for "uniformed service voter." Civilians must reside outside the territorial limits of the United States to be considered an overseas UOCAVA voter. The territorial limits include the 50 states, Commonwealth of Puerto Rico, Guam, the Virgin Islands, and American Samoa.

Voters may indicate their status as a service or overseas voter on their voter registration, on a ballot request, in correspondence with the state or county elections office, or simply by listing a military or overseas mailing address.

Only UOCAVA voters may return a voted ballot electronically by fax or email. These voters do not need to return a hard copy of the ballot in order for an electronic ballot to be counted, however, the fax or email ballot must be received by 8:00 p.m. PST. (RCW 29A.40.110, 29A.60.190; WAC 434-208-060, 434-235-040, 434-250-120) Non-UOCAVA voters cannot return a voted ballot electronically.

With the exception of special absentees and federal write-in absentees, the first **valid** ballot returned by a voter must be counted.

A voter issued a special absentee or federal write-in absentee ballot (FWAB) may also vote a regular ballot. The County Auditor only counts a special absentee ballot or FWAB if a regular ballot is not received by the day before certification. If a voter returns a regular ballot, that ballot is counted and the special absentee or FWAB is voided. (RCW 29A.40.050; WAC 434-230-015, 434-250-080, 434-262-032)

Service and overseas voters must be provided with instructions and a secrecy cover sheet for returning the ballot and signed declaration electronically. A voted ballot and signed declaration returned electronically must be received by 8:00 p.m. on the day of the election or primary. (RCW 29A.40.091 (4))

Mismatched signatures and unsigned ballot declarations are processed the same for UOCAVA voters according to RCW 29A.60.165 and WAC 434-261-050.

For fax or email ballots received from **non-**UOCAVA voters, follow these steps:

1) Contact the voter immediately. Inform the voter that a physical ballot must be returned by 8pm on Election Day to have a ballot count in the election.
2) Void the electronic ballot.
3) Count the physical ballot if it is postmarked and signed correctly.

County Auditors must use best practices provided by the Secretary of State for securely handling documents received by email (attached).

For further information, please contact the Certification and Training Program at ctsupport@sos.wa.gov or (360) 902-4165.

An information publication of the Certification and Training Program, Elections Division, Office of the Secretary of State
P.O. Box 40229, Olympia WA 98504-0229, (360) 902-4180

Best Practices for Opening Electronic E-mail Ballots and Other Attachments

- **Strongly Suggested Method**: If you have the technical support staff to help implement, create a Virtual Machine. Make sure it has the software you need and is fully patched and has all of the recommended security lock-down restrictions. Take a Snap Shot of the "perfect virtual machine". Then open e-mails with attached ballots, submit attachments to Virus Total, and then print ballots. At end of session, or if you feel unsure about the state of the virtual machine operating system (because of opening a potential shady malicious attachment) you can easily "roll back" to your perfect pristine virtual machine you started with.

- **Optional method**: Use an isolated standalone computer (a non-domain "work group" mode)
    - Computer setup/Software
        - Make sure the computer has a fresh OS install and is fully patched.
        - Do not install any unnecessary software (If Word Document files or Excel files need to be opened, install the free Microsoft Word and Excel Viewers. Do not install full blown Microsoft Office)
        - If you must install a PDF reader, make sure it is the latest most secure version.
        - Use Windows local group policies to "white lists" the applications that are only permitted to run on the computer. (For example: Chrome, Explorer, Word Viewer, PDF viewer, etc.)
        - Configure the Windows host firewall to block all incoming ports. Configure it to only permit outbound ports to your Counties Outlook mail server and a DNS server (such as Quad Nine: 9.9.9.9).
        - Make sure an up-to-date virus scanner is installed. Virus scanners help but may not detect all threats.
        - Have staff login to the computer as a local box "limited user" account.
        - Make sure the computer is connected to an isolated network (such as a DSL line – not connected to any staff or production networks)
        - Have elections users log into the county e-mail system using a web browser client (such as Outlook Web Access).
    - Accessing Attached Files
        - Plug in a USB printer and print the electronic ballots. Use the printed out ballots for counting and audits.

        - If you need to maintain the original e-mail and attached files, save them to a USB thumb drive and label the thumb drive with "Warning: Potentially infected files! Electronic voting records! Do NOT plug into computer plugged into the network! If any doubts, check with your IT staff".
        - If the file has an attachment, submit it to the following URL to have it checked out for malware. https://www.virustotal.com/#/home/upload (This site is free and will do an in-depth scan of the attached file to see if it has new zero day malware imbedded in the file. There is also a software installable client that makes it easier to scan files. See reference listed below)
        - If the attached file is password protected, be extremely cautious – this is a common method to have the file by-pass antimalware scanning. Be sure to open the file and have it scanned by https://www.virustotal.com/#/home/upload
        - Do not click on URLs in the e-mails!
        - Tip: If ballots have been sent to numerous elections staff inbox folders, do not have them open the files on their workstations! Have them forward the electronic ballots to a special e-mail account reserved for electronic election ballots.
    - Even with all the precautions you have taken, it is still possible for the computer to become infected.
    - Be sure the laptop/computer is fully wiped and re-imaged before using it again.

- **Resources:**
    - How to Whitelist programs in Windows 10: https://www.thewindowsclub.com/whitelist-program-windows-10
    - Quad 9 – Free and Secure Domain Name Resolution: https://www.quad9.net/about/
    - How to setup a Virtual Machine with Windows 10 Hyper-V: https://www.groovypost.com/howto/create-virtual-machine-windows-10-hyper-v/
    - Virus Total Windows Uploader: https://www.virustotal.com/en/documentation/desktop-applications/windows-uploader
    - Read PDF Files Safely - Here is How: https://securitywatch.pcmag.com/apps-and-websites/308409-read-pdf-files-safely-here-is-how
    - Download Word and Excel Viewer: https://www.microsoft.com/en-us/download/search.aspx (Do a search on Word Viewer and Excel Viewer)