

Subject: Preliminary Report of Subversion in the Antrim County Election Management System, Results Tallying and Reporting Application
Date: 5/9/2021
Analyst: Jeffrey Lenberg

Executive Summary

The Antrim County Dominion Democracy Suite, Election Management System (EMS), Results Tallying and Reporting (RTR) application has been found to be subverted. Numerous error conditions that are identified by the tabulator are ignored by the EMS/RTR. The error conditions are easily reproduced and displayed on the tabulator, yet the EMS/RTR has been subverted in a fashion to purposefully ignore vote manipulation. This technical behavior is consistent with a subversion being deployed in the Antrim County EMS/RTR and is designed to mute such error reporting. This subversion technique is common among malicious actors seeking to proactively handle error conditions that would jeopardize their ability to modify software's performance.

The J Alex Halderman expert report dated March 26, 2021 does not accurately describe the conditions that occurred in the Antrim election. The shifting of votes described by Halderman during the November 3, 2020 election should have resulted in Biden's votes being shifted to the Natural Law Party, Straight Party Vote, which in turn would have resulted in Rocky De La Fuente (the Natural Law Party Candidate) receiving a large number of votes as a result, or an error condition should have occurred on the EMS/RTR for a vote shift outside of the Presidential contest. Neither of these scenarios occurred because the EMS/RTR was subverted in a fashion to handle such an error silently and treat that situation as an undervote (no vote for the Presidential race at all).

Testing of related scenarios has shown the ImageCast Precinct (ICP) tabulator properly reported a critical error and shut down the tabulator when there were votes shifted between contests. However, when the EMS/RTR was presented with the same results file processed on the tabulator, it reported no errors, but instead erroneously reported those vote choices as blanks (undervotes) instead of generating a critical error.

The evidence of a subversion in the EMS/RTR is sufficient that an expert review of the source code for the EMS/RTR is warranted to determine the extent of the subversion and breadth of the configuration options available to the malicious actors that would employ it.

This assessment is based on the review of the Antrim County EMS/RTR and testing with an ICP tabulator. If more forensic information and source code becomes available for review, this assessment will be reevaluated in the light of the new

evidence available. Upon receipt of the source code a specific evaluation of the error handling routines will be conducted along with static and dynamic code analysis to definitively determine the specific behavior of the software.

Details

Discovery of Subversion of the Antrim County EMS/RTR

A specific test was designed to determine how the Antrim County EMS/RTR along with the tabulator would handle the swap of Biden votes with the Natural Law Party (Straight Ticket Vote from the Contest Above on the ballot).

The rationale for making this test was the fact that Halderman indicated that the shift of votes that occurred would have changed the index of the candidate selection to cross the boundary from the Presidential contest to the Straight Party Ticket contest. This shifting across the boundary of a contest should have created a critical error condition during the processing of votes, however, in the case of Antrim County election it did not.

The test scenario is as follows:

Ballot Style: Helena Township, Precinct 1 (1124)

DVD File Name: 1120_8_8_0_DETAIL.DVD

internalMachineID for Biden: 3016

internalMachineID for Natural Law Party: 3015

Votes Cast on Test Ballots (See Appendix A):

Biden: 2

Trump: 4

Jorgenson: 1

Both the EMS/RTR and the ICP tabulator used exactly the same DVD file listed above.

The test scenario implemented a swap between the internalMachineID fields of Biden and the Natural Law Party in the VIF_BALLOT_INSTANCE.DVD file to attempt to cause Biden's votes to be swapped with the Straight Party/Natural Law Party.

The expected outcome was that Biden's votes would be assigned to the Natural Law Party (Straight Party Vote) and the result would be Biden's votes being tallied for the Natural Law Party Presidential Candidate Rocky De La Fuente.

The test revealed the following:

- The ICP reported a critical error and does not finish processing the vote file, does not print a paper tape, writes the error to the log file, and forces a mandatory shutdown of the tabulator
- The EMS/RTR loads the same file with no errors and takes all of the Biden votes and treats them as undervotes

The 1120_8_8_0_DETAIL.DVD file is a result file containing the votes that are cast on the ICP. When the poll is closed, the ICP software processes the file containing the votes and produces a paper tape with the tallies for each candidate. This process works normally as long as the internalMachineID is not modified or the modification stays within the boundaries of the those “expected” for the specific contest, for example the Presidential Contest. In other words, a malicious actor can swap internalMachineIDs within the same Contest for any candidate so long as the index remains in the correct range for that same contest.

However, for the purposes of this test the internalMachineIDs were swapped between different Contests, the software in the ICP reports a critical error (see Figure 1). The ICP does not finish processing the vote file (Figure 1), does not print a paper tape, requires the operator to shut-down the tabulator (see Figure 2), and records details of the error in the slog.txt file (Figure 3) on the compact flash card. The tabulator takes drastic action to inform the operator that a very serious problem has been encountered. Note that the vote result file 1120_8_8_0_DETAIL.DVD is still correctly stored on the compact flash card.

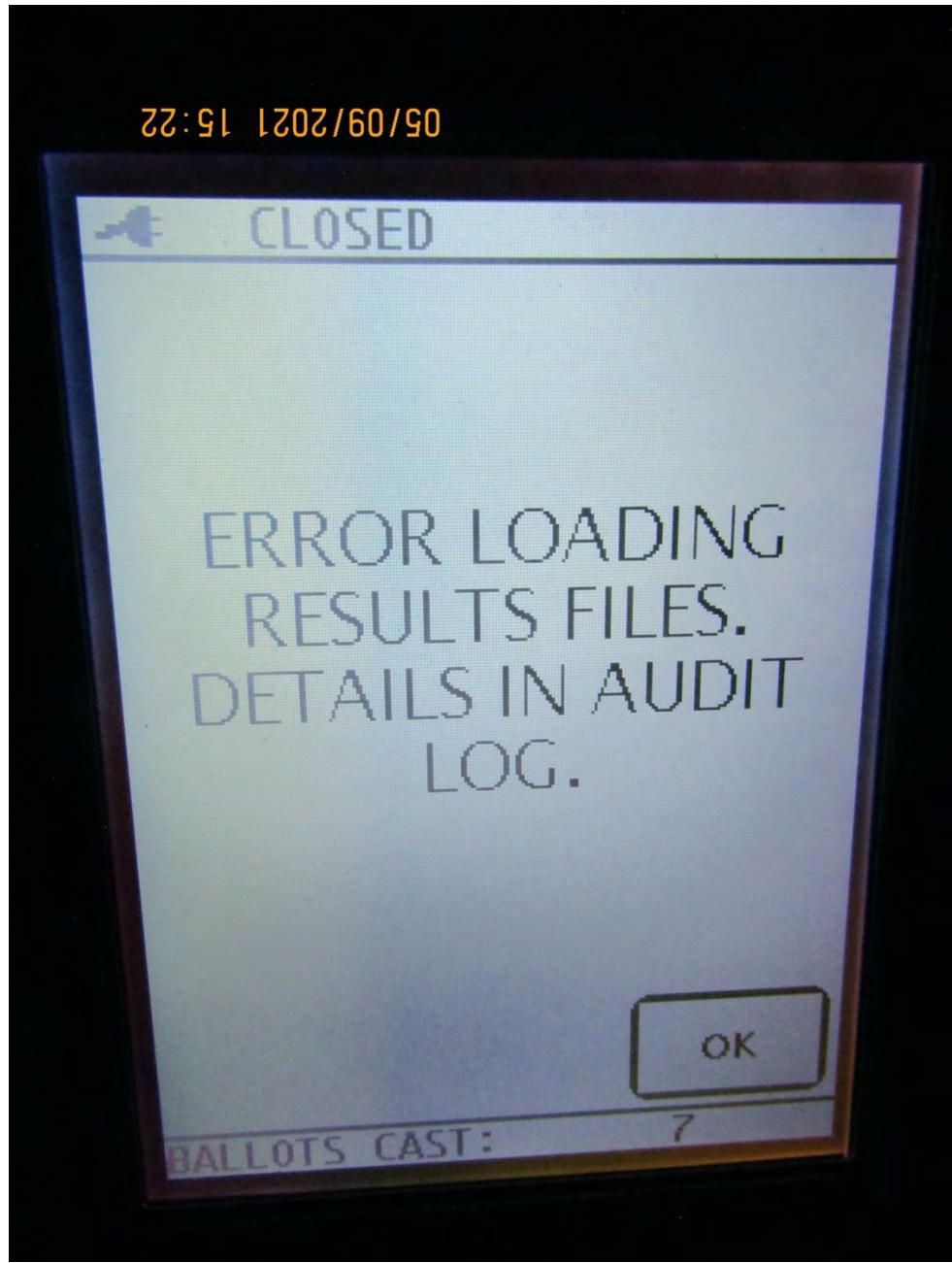


Figure 1 - ICP Error Loading Results File



Figure 2 - ICP Critical Error - Shutdown Required

Nov 03/2020 06:36:48	ScanVote	Total number of ballots = 4.
Nov 03/2020 06:36:58	ScanVote	Ballot 1124 processed successfully.
Nov 03/2020 06:36:58	ScanVote	Total number of ballots = 5.
Nov 03/2020 06:37:09	ScanVote	Ballot 1124 processed successfully.
Nov 03/2020 06:37:09	ScanVote	Total number of ballots = 6.
Nov 03/2020 06:37:20	ScanVote	Ballot 1124 processed successfully.
Nov 03/2020 06:37:20	ScanVote	Total number of ballots = 7.
Nov 03/2020 06:38:13	Security Audit	Administrator key for 'Admin' detected.
Nov 03/2020 06:38:13	Admin Audit	Administrative Key inserted
Nov 03/2020 06:44:23	Admin Audit	Admin chose to Close the Poll
Nov 03/2020 06:44:55	Admin Warning	Error Reading Admin key.
Nov 03/2020 06:44:57	Security Audit	Administrator key for 'Admin' detected.
Nov 03/2020 06:44:57	Admin Audit	Administrative Key inserted
Nov 03/2020 06:45:10	Admin Audit	Admin chose to Close the Poll
Nov 03/2020 06:45:24	Admin	Correct passcode entered for Close.
Nov 03/2020 06:45:24	Admin	Requesting confirmation to close poll.
Nov 03/2020 06:45:35	Admin	Starting election database close poll procedure.
Nov 03/2020 06:45:35	Election	Saving Poll-Close time.
Nov 03/2020 06:45:36	Election	Beginning to create Total Results file.
Nov 03/2020 06:45:36	Election Error	TotalOneContest: Raw Results, cannot find choice instance 3016)
Nov 03/2020 06:45:36	Election Warning	- Problem (30023) creating Total Results file ". Raw Results will be used instead
Nov 03/2020 06:45:37	Election Error	TotalOneContest: Raw Results, cannot find choice instance 3016)
Nov 03/2020 06:45:46	Admin Audit	Advising Administrator of error (30023) printing report RESULTS TAPE.
Nov 03/2020 06:45:46	Admin Critical	HandlePollSelection: Error 30023. Forcing shutdown
Nov 03/2020 06:45:56	Admin Audit	Shutdown system.
Nov 03/2020 06:45:57	Control	>> DvsShutdown(fast:00000000).
Nov 03/2020 06:45:57	Control	>> Shutting down AVS.
Nov 03/2020 06:45:57	Control	>> Module (WavDecoder) shutdown successful.
Nov 03/2020 06:45:59	Control	>> Module (Event) shutdown successful.
Nov 03/2020 06:45:59	Control	>> Module (Election) shutdown successful
Nov 03/2020 06:45:59	Control	>> Module (Admin) shutdown successful
Nov 03/2020 06:45:59	Control	>> Module (Diagnostics) shutdown successful.

05/09/2021 18:44

Figure 3 - *slog.txt* File Contents from Compact Flash Card

The same compact flash card is then loaded on to the Antrim EMS/RTR software. The card reports that it loaded successfully both the vote results and the log file (See Figure 4). Prior to loading this compact flash card the EMS database is directly manipulated in the same way that the file sent to the tabulator was manipulated by swapping 3015 and 3016 internalMachineID in the ChoiceManifestion table of 5744 vote choices spanning all of the contests on all of the 49 ballots types.

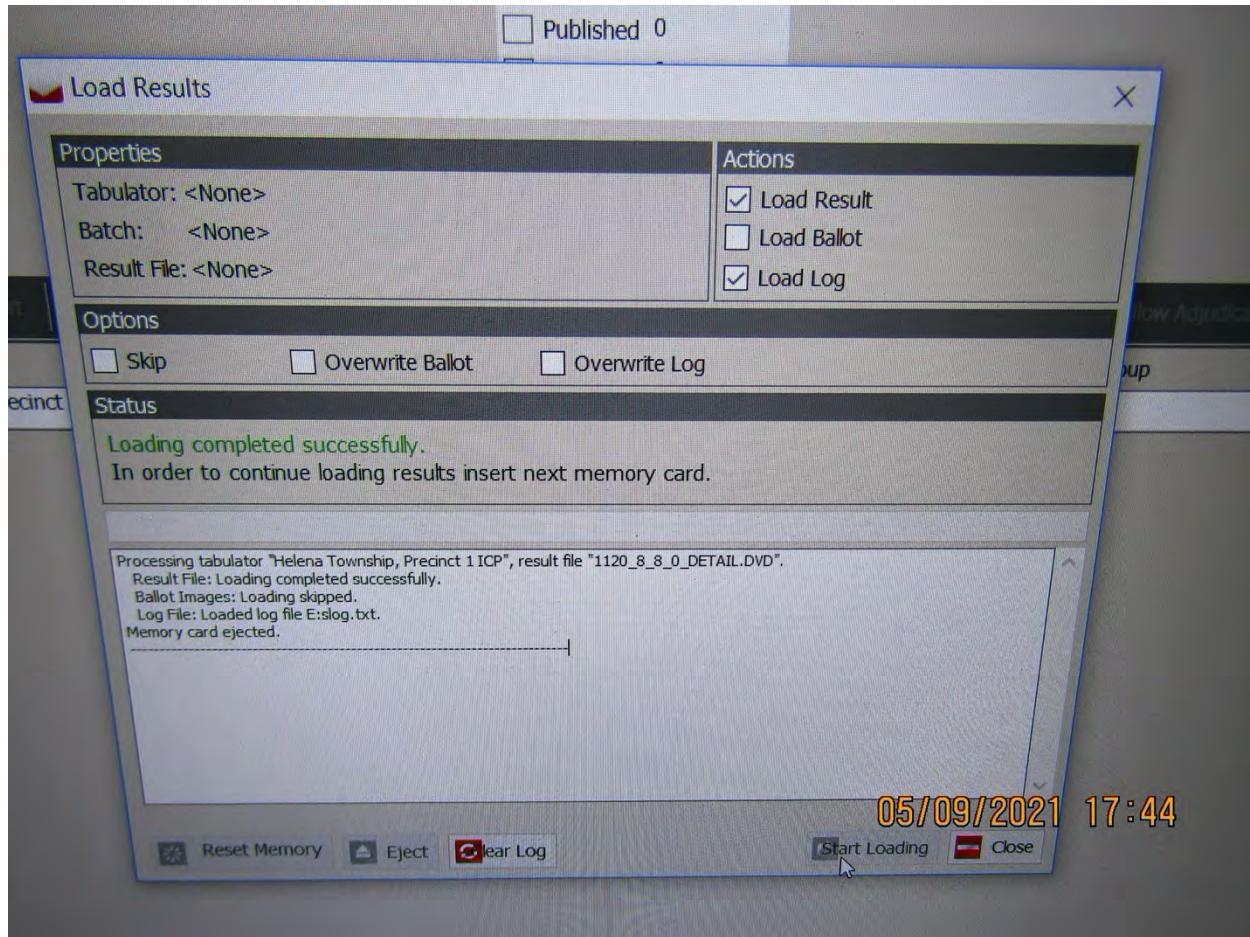


Figure 4 - EMS Successfully Loads Results File

The displayed results indicated that Biden is missing his votes and they are reported as blank ballots and undervotes for that contest (See Figure 5). One of two things should have happened. Either Biden's votes should have been assigned to the Straight Party/Natural Law (internalMachineID = 3015) in which case Bidens vote for President would have been assigned to De La Fuente and note that this did not occur. The other possibility is that the software was able to check the range for internalMachineID range for the contest in which case it would not have found the reference for the Biden vote choice and it should have created an error very similar to what the ICP output. This would be a critical error that should have stopped the application from further processing the compact flash card. Because the Biden vote choice must exist and it did not exist, the application should have stopped loading the results with an error message as to the fact that the results were corrupted. However, no errors were indicated of any kind by the EMS/RTR. The Biden votes just became blank votes (no choice) when there clearly is a choice on the ballot. In summary, either the shifted votes should have gone to De La Fuente (via Straight Party – Natural Law Party) or the application should have created a critical error that would have kept the votes from being tallied and reported.

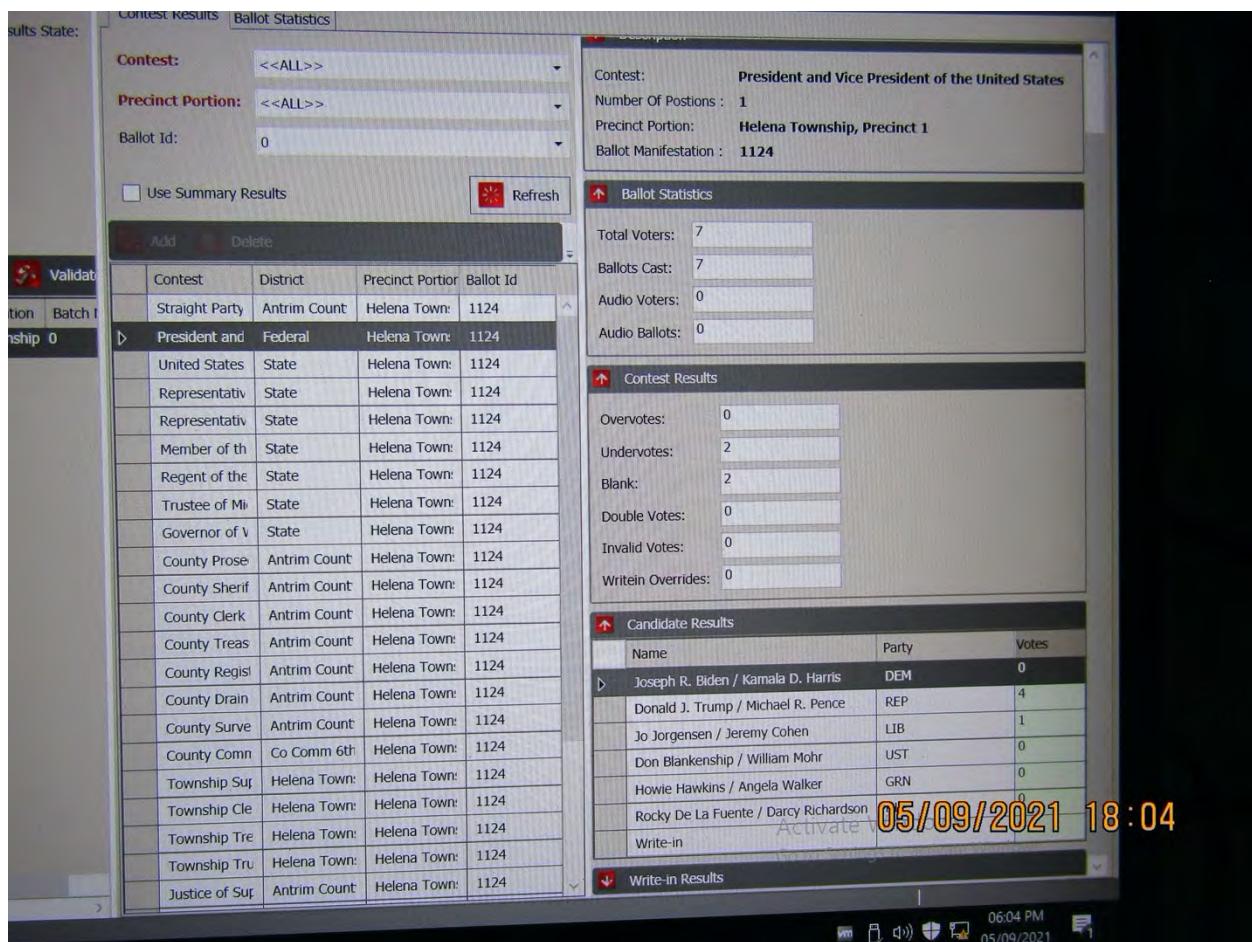


Figure 5 - Biden Undervotes Results

The conclusion of this test indicates EMS/RTR technical behavior consistent with a technical subversion. Further in-depth analysis of source code would be required to gain definitive clarity on the specific nature of the subversion. This would include analysis of the error handling routines, code traces, static and dynamic code analysis.

Under the penalties of perjury, I declare that I have read the foregoing report and that the fact stated in it are true.


 Jeffrey Lenberg
 Date: 5/9/2021

STATE OF MICHIGAN
COUNTY OF OAKLAND

The foregoing instrument was acknowledged before me this 9th of May, 2021 by Jeffrey Lenberg,

Ann M. Howard

Notary Public

Printed Name: Ann M. Howard

My Commission Expires: 2/24/2023

ANN M. HOWARD
Notary Public, State of Michigan
County of Oakland
My Commission Expires 02-24-2023
Acting in the County of Oakland

Appendix A – Ballots Used in Test

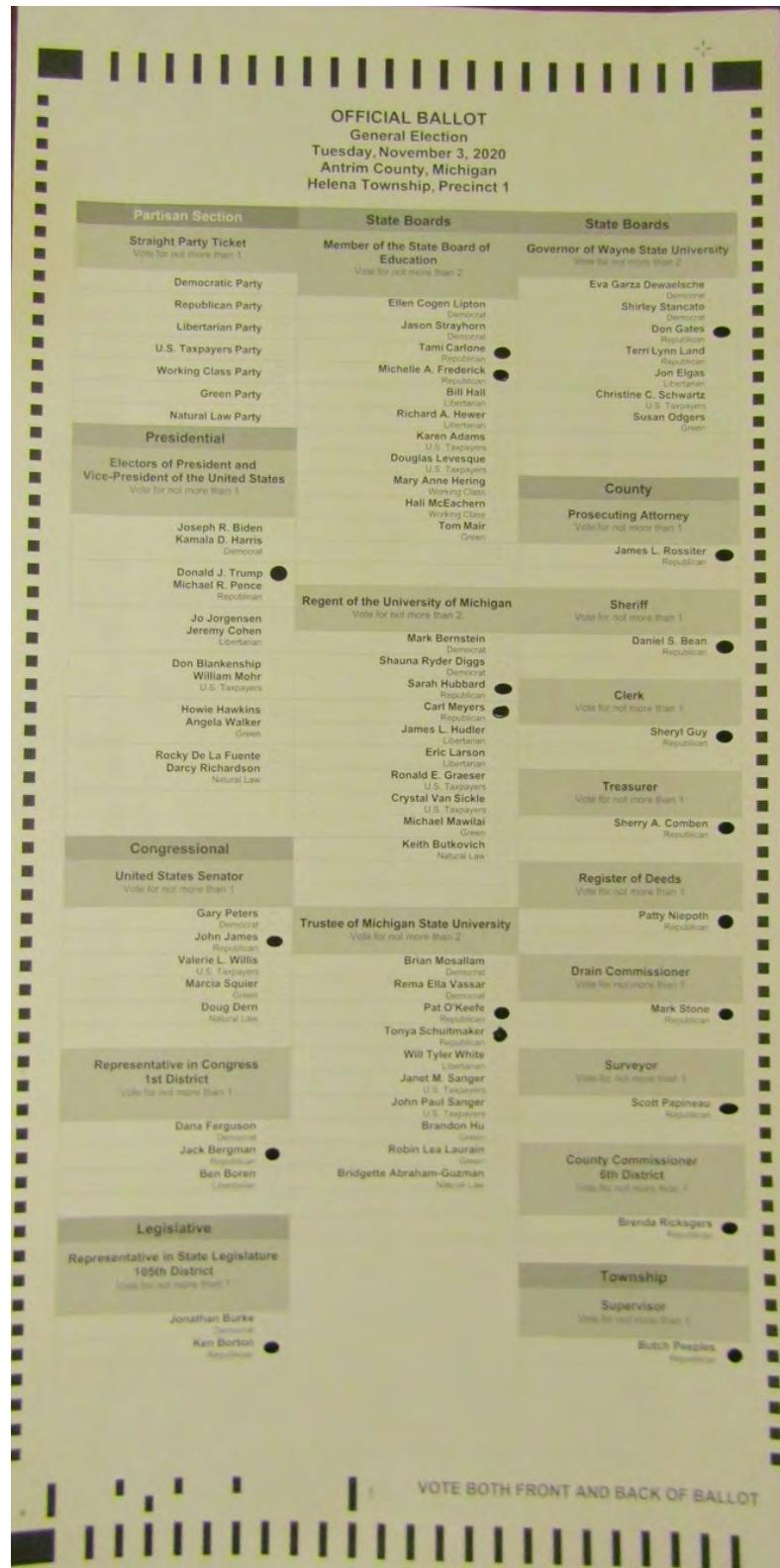


Figure 6 - Trump/James/Bergman

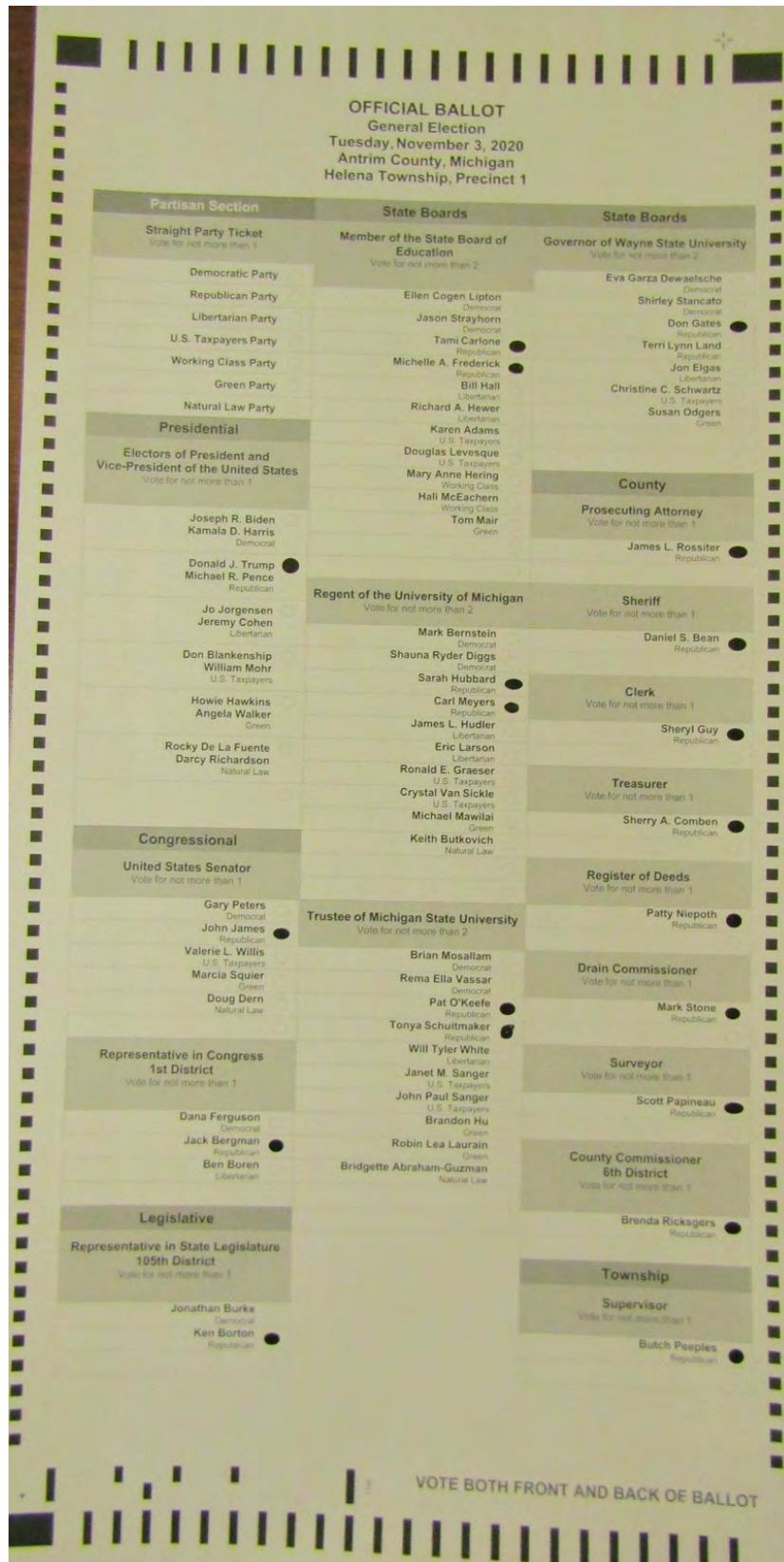


Figure 7 - Trump/James/Bergman

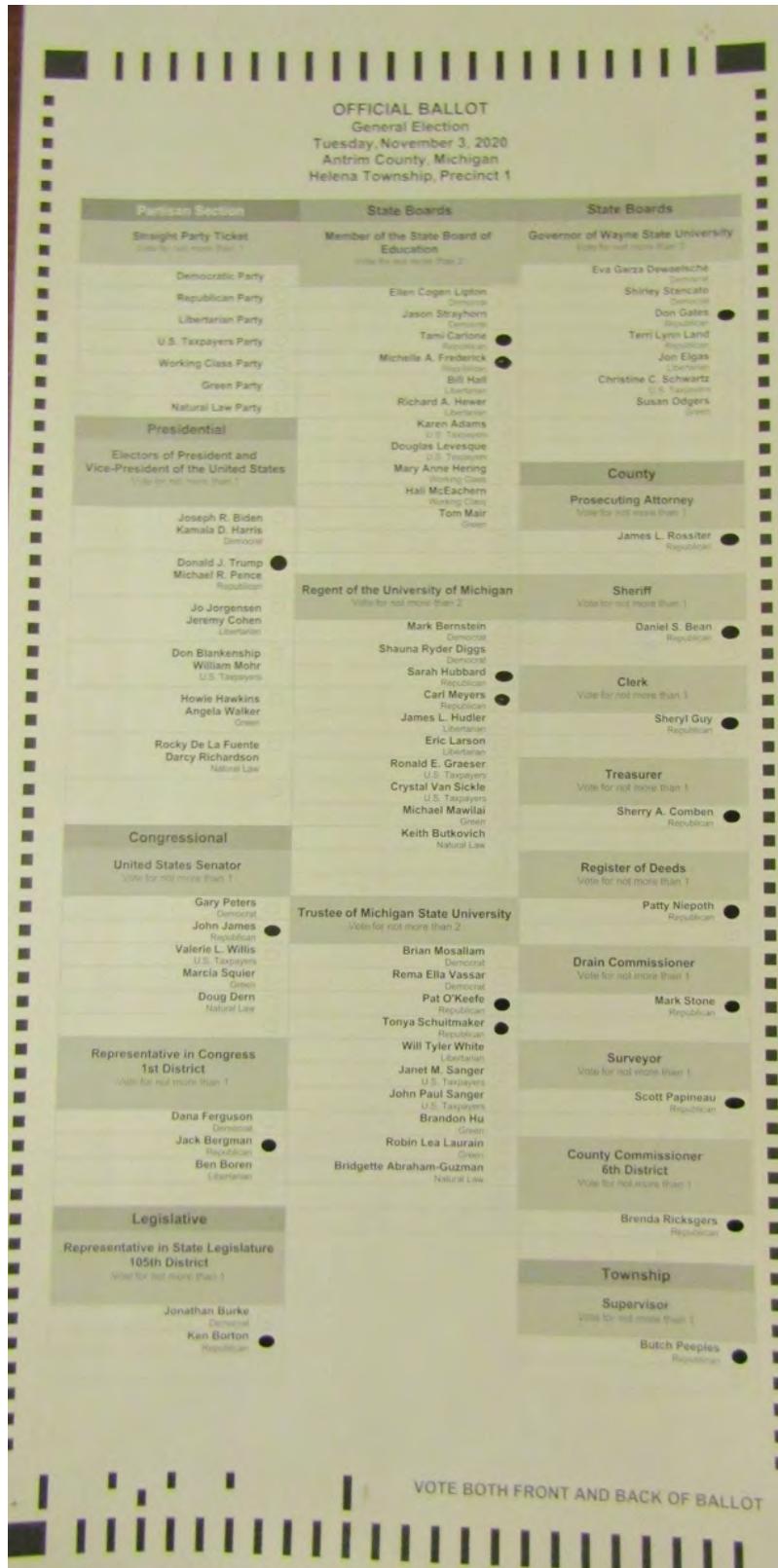


Figure 8 - Trump/James/Bergman

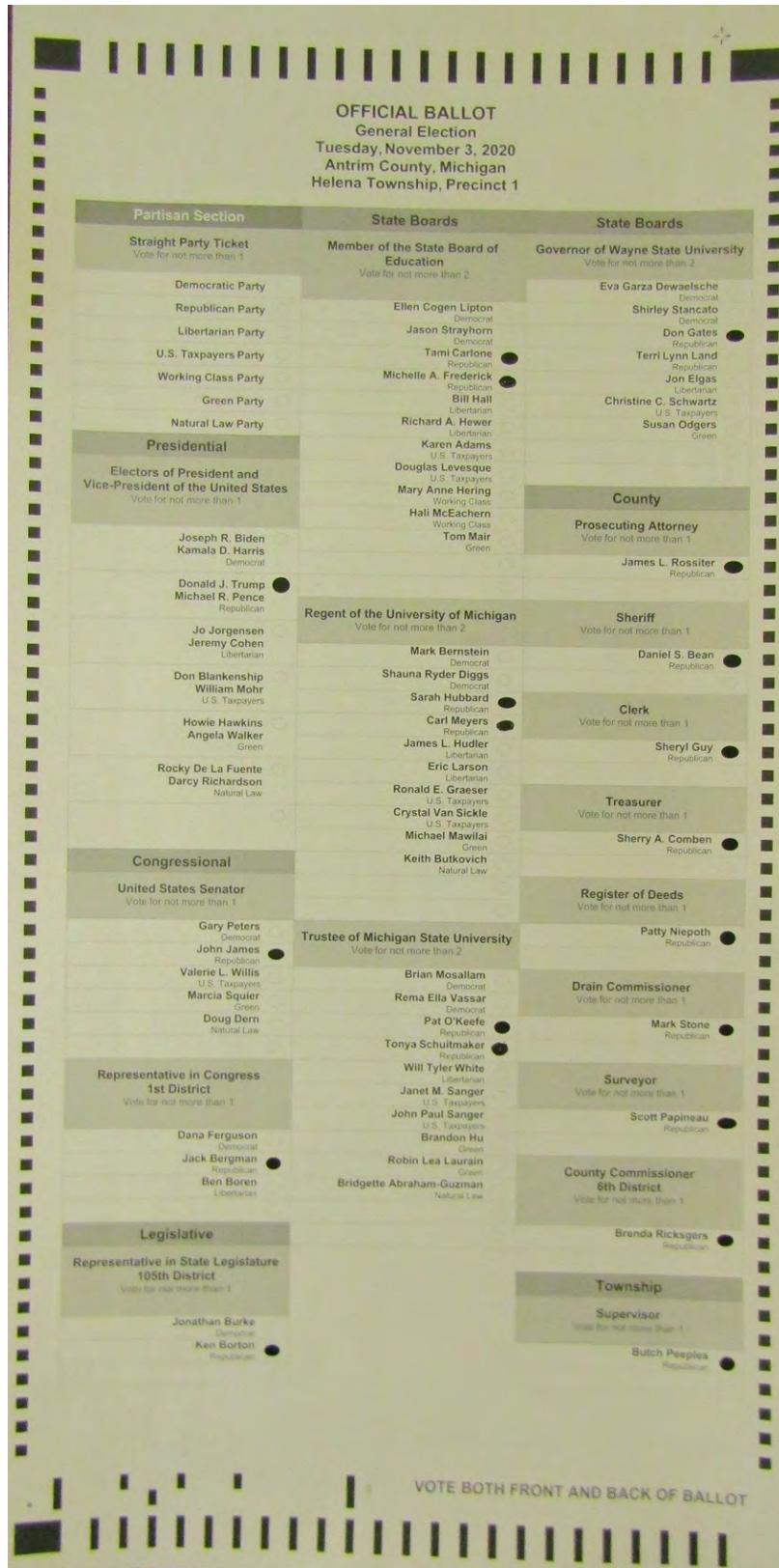


Figure 9 - Trump / James / Bergman

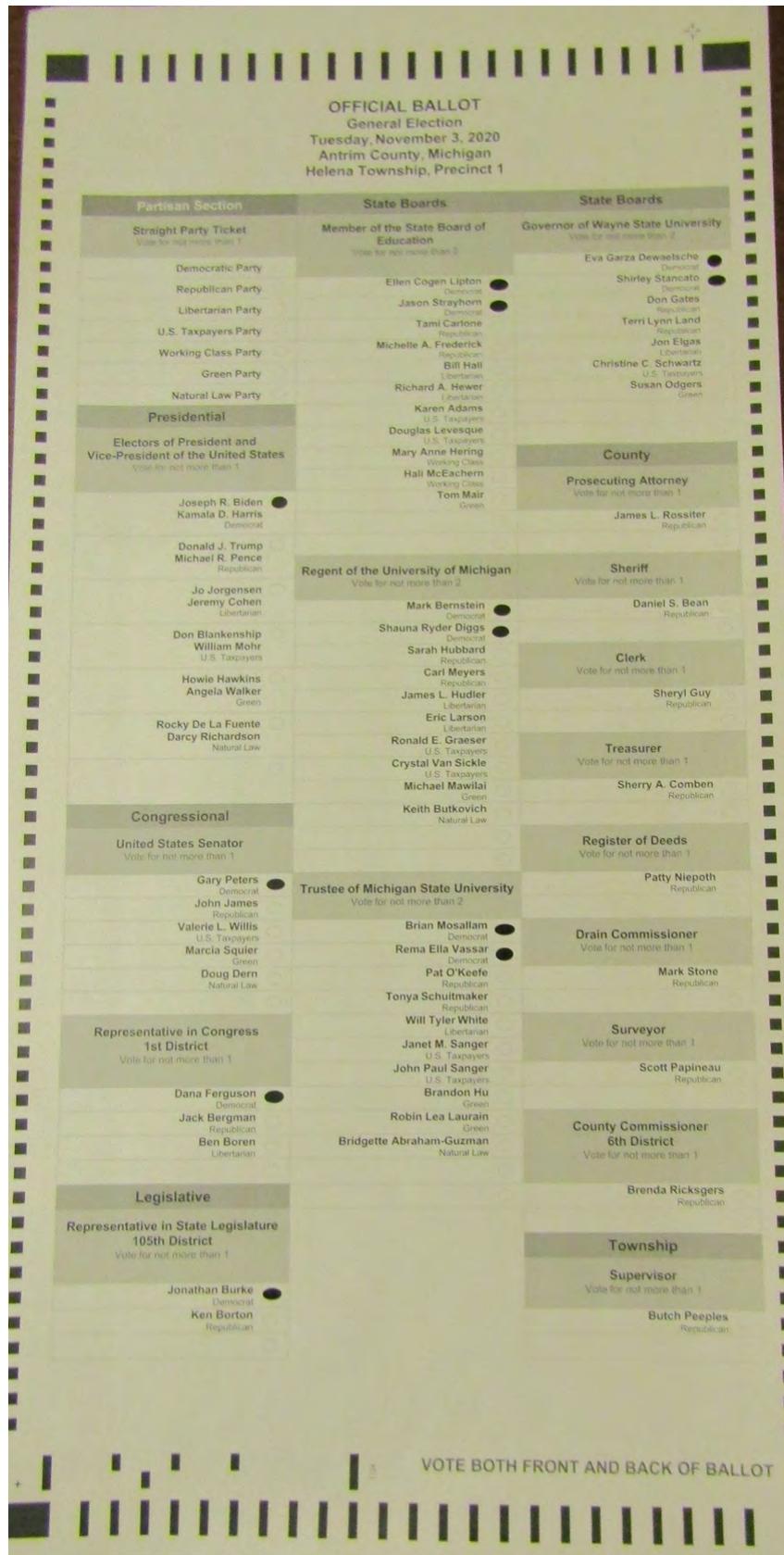


Figure 10 - Biden/Peters/Ferguson

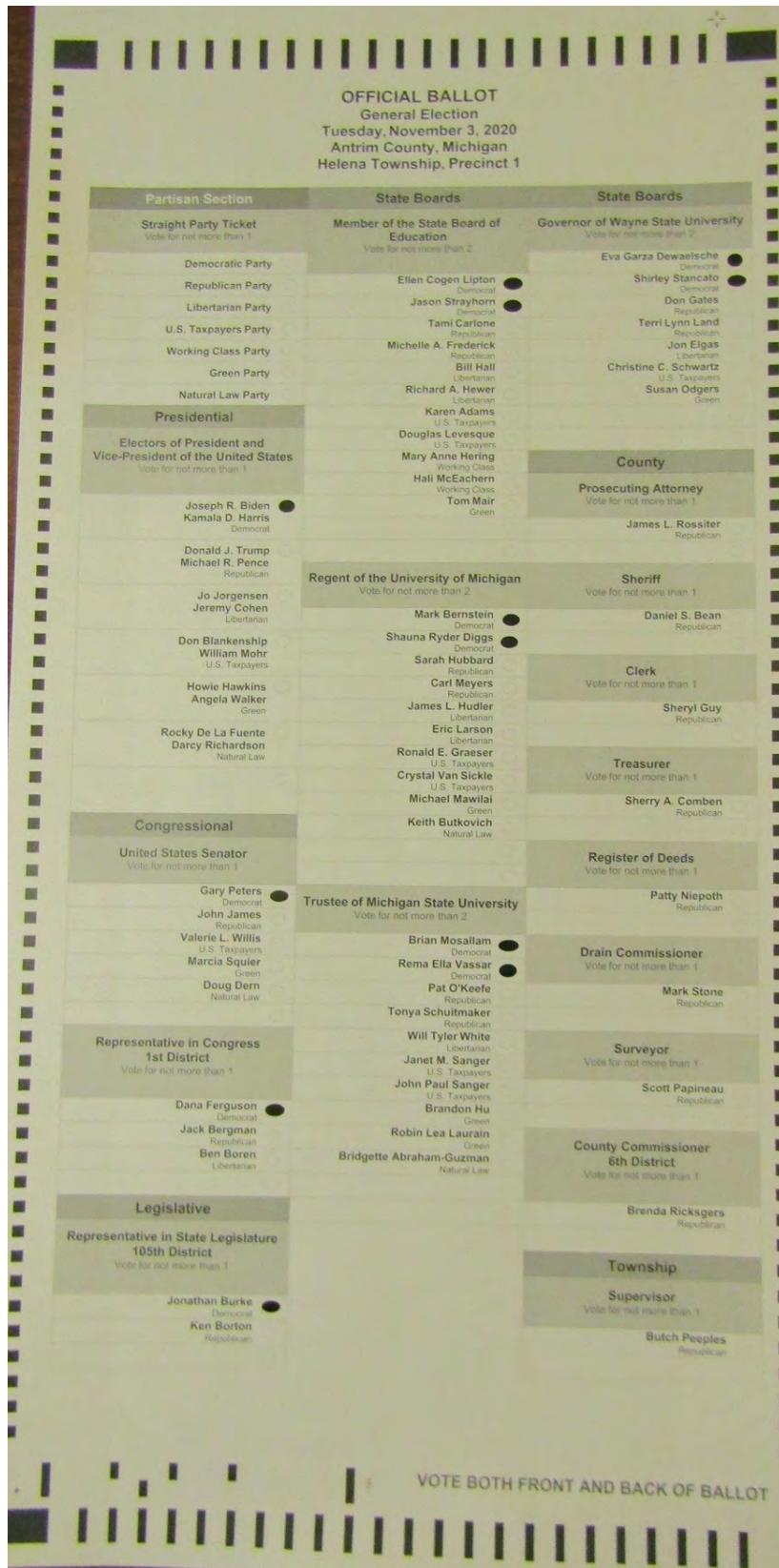


Figure 11 - Biden/Peters/Ferguson

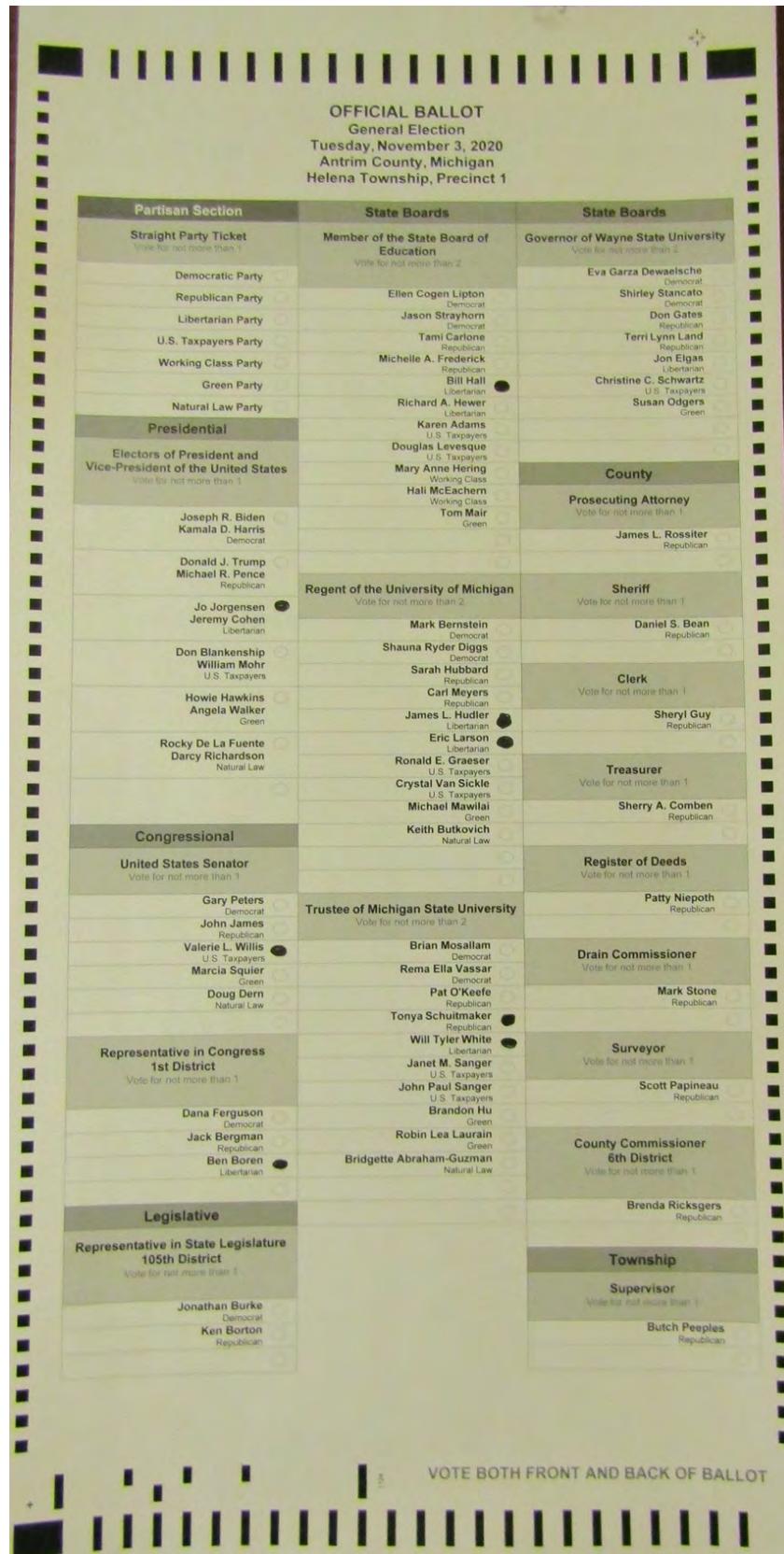


Figure 12 - Jorgenson/Willis/Boren