

Date: 5/16/2021

Subject: Summary of Security Deficiencies in the Antrim County Voting Systems

Analyst: Jeffrey Lenberg

## **Executive Summary**

This summary describes a subset of the critical deficiencies in the security of the electronic voting systems used in Antrim County, Michigan for the November 3, 2020 election.

Election workers/contractors with the technician/supervisor passcode can change the date/time on the Imagecast Precinct (ICP) tabulator tapes by resetting the time on the tabulator after they enter their passcode. The election worker/contractor can then proceed to print a new election tape from the tabulator with whichever data/time stamp they prefer. If a malicious election worker/contractor wished to run additional ballots outside of the election window or after hours, the ability to reset the time to print new tapes makes it extremely difficult to identify fraudulent activities because the paper tapes figure prominently in the canvassing process. See the expert report by Penrose dated May 3, 2021 that shows in the EMS the technician passcode of “123456”.

All of the Antrim County election workers and contractors that perform work on the EMS utilize the same account to work on the system. This account has administrative access and can be used to modify the EMS database to manipulate vote totals. The 6 account first name/last names pairs listed in the system database are as follows: Ben/Smythe, John/Smith, Ryan/Smoth, MRO/M01, Return Office/Admin, MRESuper/Admin. These are the only users that account for log entries regardless of who is actually logged into the system and making changes.

The password enforcement policies on the EMS are substandard, they even allow the users to set purposefully “weak” passwords as a feature.

The absence of best practice security procedures to require individual accounts for users to protect accounts and passwords is inexcusable in a system that is used to conduct elections. In addition, the ability to reset date/time on tabulators, reopen the polls, reprint tapes makes fraud very feasible for even low sophistication actors.

## **Details**

Election workers have the ability to set the time on a tabulator at any time in order to print paper tapes that show the appropriate date/time stamp. The technician/supervisor password enables the workers to have this capability. The

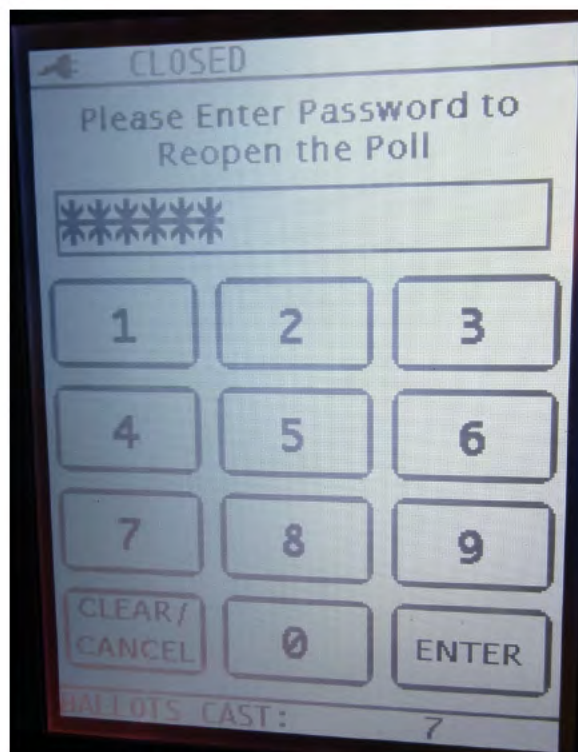
process is straightforward and is performed by traversing the menus on the tabulator itself.

For this demonstration scenario, the following steps were performed to illustrate that the ICP paper tabulator tapes can be custom modified to show a specific time of poll closure for the election, regardless of the actual date and time.

- The ICP is powered on.
- The ICP Poll is opened by scanning the security key fob on the ICP sensor and entering the poll worker security passcode of “11032020”, and a zero tape is printed.
- 7 demonstration ballots (same reference ballots from Lenberg report dated May 3, 2020 Exhibit A) are fed into the tabulator demonstration purposes.
  - The vote breakdown on the original ballots for the Presidential Contest is as follows:
    - 4 votes for Trump
    - 2 votes for Biden
    - 1 vote for Jorgenson
  - The vote breakdown on the original ballots for Senate
    - 4 votes for James
    - 2 votes for Peters
    - 1 vote for Willis
- The ICP Poll is closed by placing the security key fob on the ICP sensor which brings up an administrative menu to close the poll. As soon as the poll is closed a paper tape of the tabulation is automatically printed. The paper tape includes a flip of Trump and Biden votes.
  - The vote breakdown on the paper tape for the Presidential Contest is as follows:
    - 2 votes for Trump (flipped from Biden to Trump)
    - 4 votes for Biden (flipped from Trump to Biden)
    - 1 vote for Jorgenson
  - The vote breakdown on the paper tape for Senate
    - 4 votes for James
    - 2 votes for Peters
    - 1 vote for Willis
- The ICP Poll is reopened by placing the security key fob on the ICP sensor and entering the technician passcode “123456”



*Figure 1 - ICP LCD Closed Poll Menu*



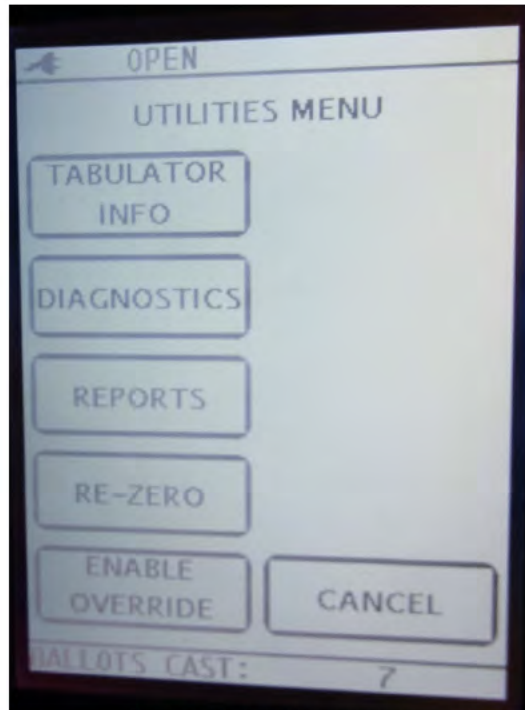
*Figure 2 - ICP LCD Menu to Re-open the Poll*

- 7 ADDITIONAL demonstration ballots are fed into the system with the same original ballot breakdown as the initial group of ballots used in the demonstration.
- The security key fob is placed on the ICP sensor, and a menu appears automatically ICP LCD showing CLOSE THE POLL, UTILITIES, BALLOT REVIEW, POWER DOWN, and CANCEL

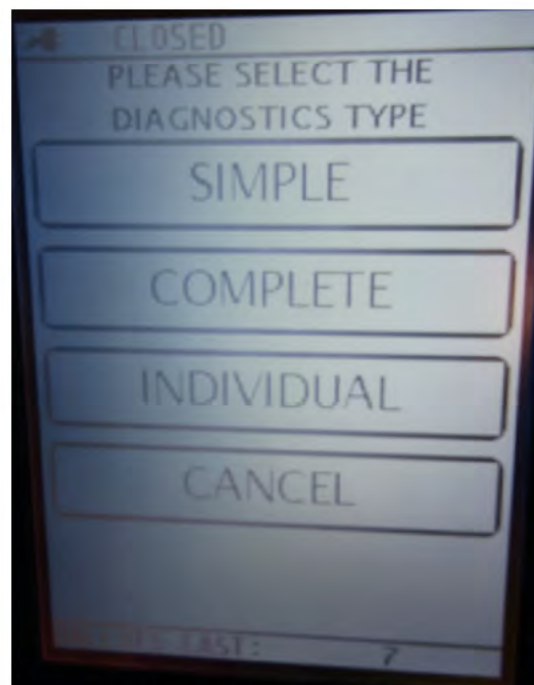


*Figure 3 - ICP LCD Administrative Menu*

- The following menu selection is made on the tabulator LCD
  - UTILITIES -> DIAGNOSTICS -> INDIVIDUAL -> INTERNAL CLOCK -> SET DATE AND TIME
  - See Figures 4-9



*Figure 4 - ICP LCD Utilities Menu*



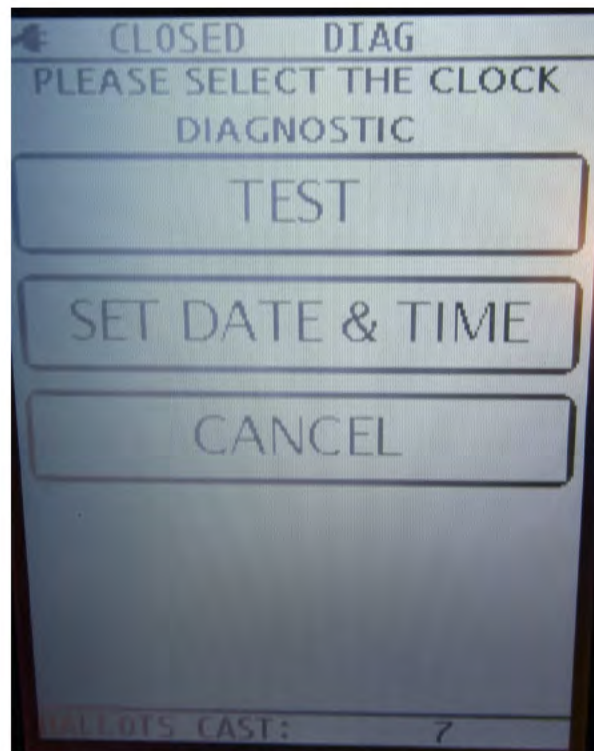
*Figure 5 - ICP LCD Selection Diagnostics Type*



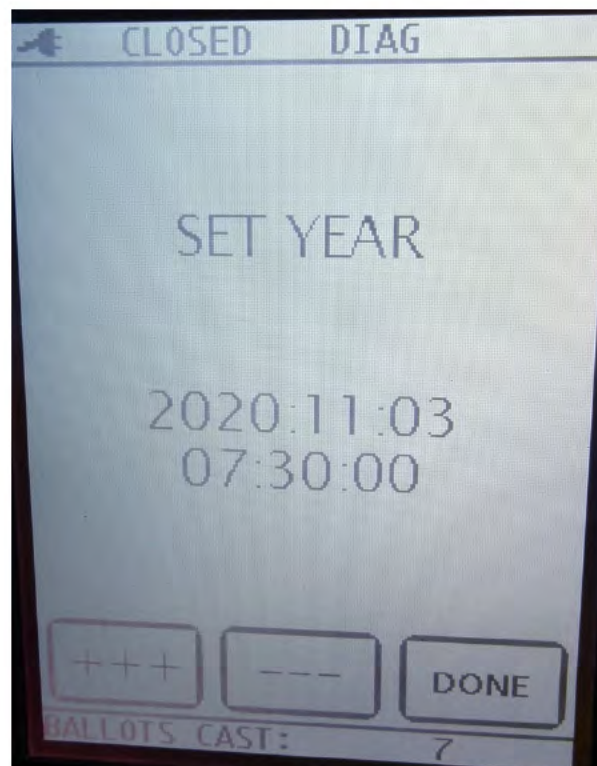
*Figure 6 - ICP LCD Device Selection Menu*



*Figure 7 - ICP LCD Clock Diagnostic*



*Figure 8 - ICP LCD Set Date/Time*



*Figure 9 - ICP LCD Dialogue to Set Time*

- Set the date/time to the election date/time the poll was originally closed
  - This specific action represents the most egregious vector for fraud for local election workers/contractors with administrative access to the tabulators and to any ballot(s)
  - The ballot images are stored on the EMS and additional blank ballots are in the possession of Election Source contractors and any local official with physical access to the media. (see Penrose report dated May 3, 2021)
  - The poll worker/technician passcodes along with access to additional ballots (could be only one) would be sufficient to perpetrate this fraud
- On the ICP LCD select CANCEL on the DIAGNOSTICS sub-menu
- On the ICP LCD select CLOSE POLL and enter the poll worker passcode “110302020”
- The malicious actor initially makes an estimate the number of fraudulent votes needed to win the election and programs for that scenario. However, often they need to add additional votes beyond the pre-planned fraud estimates, requiring the polls to be *re-opened again* to add additional fraudulent votes to achieve their objectives.
- The ICP Poll is reopened by placing the security key fob on the ICP sensor and entering the technician passcode “123456”
  - Once again, 7 ADDITIONAL demonstration ballots are fed into the system with the same original ballot breakdown as the initial group of ballots used in the demonstration.
  - The security key fob is placed on the ICP sensor, and a menu appears automatically ICP LCD showing CLOSE THE POLL, UTILITIES, BALLOT REVIEW, POWER DOWN, and CANCEL
  - The following menu selection is made on the tabulator LCD
    - UTILITIES -> DIAGNOSTICS -> INDIVIDUAL -> INTERNAL CLOCK -> SET DATE AND TIME
  - Set the date/time to the election date/time the poll was originally closed
    - Again, this is done to ensure the paper tapes printed from the tabulator remain consistent and fraud is not detected during the canvassing process.
  - On the ICP LCD select CANCEL on the DIAGNOSTICS sub-menu
  - On the ICP LCD select CLOSE POLL and enter the poll worker passcode “110302020”



- This demonstration continues to follow the same process of injecting fraudulent votes and maintaining the exact same date and time for the poll opening, closing, and printout to the minute.
  - This is done for two more rounds of adding 7 more fraudulent ballots per round
  - The total number of fraudulent ballots added is 21 in this demonstration while maintaining the same date and time to the minute as the original election results on the ICP tabulator paper tape.
- The fraudulent actor may run this attack ad infinitum at their leisure.

Total Votes:		0
President and Vice President of the United States (1)		
Joseph R. Biden / Kamala D. Harris (Democrat):	4	
Donald J. Trump / Michael R. Pence (Republican):	2	
Jo Jorgensen / Jeremy Cohen (Libertarian):	1	
Don Blankenship / William Mohr (U.S. Taxpayers):	0	
Howie Hawkins / Angela Walker (Green):	0	
Rocky De La Fuente / Darcy Richardson (Natural Law):	0	
Write-in:	0	
Total Votes:	7	

Total Votes:		0
President and Vice President of the United States (1)		
Joseph R. Biden / Kamala D. Harris (Democrat):	8	
Donald J. Trump / Michael R. Pence (Republican):	4	
Jo Jorgensen / Jeremy Cohen (Libertarian):	2	
Don Blankenship / William Mohr (U.S. Taxpayers):	0	
Howie Hawkins / Angela Walker (Green):	0	
Rocky De La Fuente / Darcy Richardson (Natural Law):	0	
Write-in:	0	
Total Votes:	14	

Total Votes:		0
President and Vice President of the United States (1)		
Joseph R. Biden / Kamala D. Harris (Democrat):	12	
Donald J. Trump / Michael R. Pence (Republican):	6	
Jo Jorgensen / Jeremy Cohen (Libertarian):	3	
Don Blankenship / William Mohr (U.S. Taxpayers):	0	
Howie Hawkins / Angela Walker (Green):	0	
Rocky De La Fuente / Darcy Richardson (Natural Law):	0	
Write-in:	0	
Total Votes:	21	

Total Votes:		0
President and Vice President of the United States (1)		
Joseph R. Biden / Kamala D. Harris (Democrat):	16	
Donald J. Trump / Michael R. Pence (Republican):	8	
Jo Jorgensen / Jeremy Cohen (Libertarian):	4	
Don Blankenship / William Mohr (U.S. Taxpayers):	0	
Howie Hawkins / Angela Walker (Green):	0	
Rocky De La Fuente / Darcy Richardson (Natural Law):	0	
Write-in:	0	
Total Votes:	28	

Total Votes:		0
United States Senator for State (1)		
Gary Peters (Democrat):	2	
John James (Republican):	4	
Valerie L. Willis (U.S. Taxpayers):	1	
Marcia Squier (Green):	0	
Doug Dern (Natural Law):	0	
Write-in:	0	
Total Votes:	7	

Total Votes:		0
United States Senator for State (1)		
Gary Peters (Democrat):	4	
John James (Republican):	8	
Valerie L. Willis (U.S. Taxpayers):	2	
Marcia Squier (Green):	0	
Doug Dern (Natural Law):	0	
Write-in:	0	
Total Votes:	14	

Total Votes:		0
United States Senator for State (1)		
Gary Peters (Democrat):	6	
John James (Republican):	12	
Valerie L. Willis (U.S. Taxpayers):	3	
Marcia Squier (Green):	0	
Doug Dern (Natural Law):	0	
Write-in:	0	
Total Votes:	21	

Total Votes:		0
United States Senator for State (1)		
Gary Peters (Democrat):	8	
John James (Republican):	16	
Valerie L. Willis (U.S. Taxpayers):	4	
Marcia Squier (Green):	0	
Doug Dern (Natural Law):	0	
Write-in:	0	
Total Votes:	28	

Total Votes:		0
Representative in Congress 1st District (1)		
Dana Ferguson (Democrat):	8	

Figure 10 - Manipulated Vote Totals on Tabulator Tapes



*****	*****	*****	*****
Antrim County Antrim November 2020 Tuesday, November 3, 2020	Antrim County Antrim November 2020 Tuesday, November 3, 2020	Antrim County Antrim November 2020 Tuesday, November 3, 2020	Antrim County Antrim November 2020 Tuesday, November 3, 2020
Tabulator Name Helena Township, Precinct 1 ICP	Tabulator Name Helena Township, Precinct 1 ICP	Tabulator Name Helena Township, Precinct 1 ICP	Tabulator Name Helena Township, Precinct 1 ICP
Tabulator ID 8	Tabulator ID 8	Tabulator ID 8	Tabulator ID 8
Voting Location Helena Township	Voting Location Helena Township	Voting Location Helena Township	Voting Location Helena Township
<u>Precinct:</u>	<u>Precinct:</u>	<u>Precinct:</u>	<u>Precinct:</u>
Helena Township, Precinct 1	Helena Township, Precinct 1	Helena Township, Precinct 1	Helena Township, Precinct 1
-----	-----	-----	-----
Poll Opened Nov 03/2020 08:01:15	Poll Opened Nov 03/2020 08:01:15	Poll Opened Nov 03/2020 08:01:15	Poll Opened Nov 03/2020 08:01:15
Poll Closed Nov 03/2020 08:03:23	Poll Closed Nov 03/2020 08:03:30	Poll Closed Nov 03/2020 08:03:34	Poll Closed Nov 03/2020 08:03:31
Report Printed Nov 03/2020 08:03:26	Report Printed Nov 03/2020 08:03:33	Report Printed Nov 03/2020 08:03:38	Report Printed Nov 03/2020 08:03:34
-----	-----	-----	-----
Unit Model: PCOS-320C (Rev 1072)	Unit Model: PCOS-320C (Rev 1072)	Unit Model: PCOS-320C (Rev 1072)	Unit Model: PCOS-320C (Rev 1072)
Unit Serial: AFAJH20246	Unit Serial: AFAJH20246	Unit Serial: AFAJH20246	Unit Serial: AFAJH20246
Protective Counter: 40623	Protective Counter: 40630	Protective Counter: 40637	Protective Counter: 40644
Software Version: 5.5.3-0002	Software Version: 5.5.3-0002	Software Version: 5.5.3-0002	Software Version: 5.5.3-0002
-----	-----	-----	-----
Total Scanned: 7	Total Scanned: 14	Total Scanned: 21	Total Scanned: 28
Total Voters: 7	Total Voters: 14	Total Voters: 21	Total Voters: 28
=====	=====	=====	=====
Ballot ID: 1124	Ballot ID: 1124	Ballot ID: 1124	Ballot ID: 1124
Ballots Scanned: 7	Ballots Scanned: 14	Ballots Scanned: 21	Ballots Scanned: 28
=====	=====	=====	=====
<u>Precinct:</u>	<u>Precinct:</u>	<u>Precinct:</u>	<u>Precinct:</u>
Helena Township, Precinct 1	Helena Township, Precinct 1	Helena Township, Precinct 1	Helena Township, Precinct 1
-----	-----	-----	-----
Straight Party Ticket (1)	Straight Party Ticket (1)	Straight Party Ticket (1)	Straight Party Ticket (1)
Democratic Party	Democratic Party	Democratic Party	Democratic Party

Figure 11 - Specific Times Manipulated on the Tapes Corresponding to Figure 10

## Administrator Accounts and Passwords

The Dominion Election Management System (EMS) database accounts have the following user names: John Smith, MRO M01, Return Office Admin, Ben Smythe, MRESuper Admin, Ryan Smoth.

FROM [Antrim May 2020-2020-02-24-16-25-17].[dbo].[AppUser]

100 %

Results Messages

	Id	username	password	firstName	lastName	__classid	salt
1	4004A444-6AF5-4A75-B22B-16C7564A05B5	Techadvisor	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	John	Smith	9001	0x
2	6CC70D62-BF0B-4D6E-8E78-3FC66BF81083	MRO01	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	MRO	M01	9001	0x
3	6CC70D62-BF0B-4D6E-8E78-3FC66BF8EF83	ROAdmin	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	Return Office	Admin	9001	0x
4	7AC70D62-BF0B-4D6E-8E78-3FC66BF8EF83	Admin	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	Ben	Smythe	9001	0x
5	9BC70D62-BF0B-4D6E-8E78-3FC66BF8EF83	SAdmin	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	MRESuper	Admin	9001	0x
6	57C10FCF-3412-4EDD-BC81-588F25D72C35	RTRAdmin	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	Ryan	Smoth	9001	0x

Figure 12 – Dominion EMS Database Administrator Accounts

Admin	Election Project has been created with Election Event Designer version 5.5.12.1	2019-01-08 09:27:28.340	UserAction
Admin	Instance with name '4c95f7f1-51bc-4149-95ed-72f4c5f3ffe0' of type 'LanguageProfile' modified: name = 'English'; isDefault=True; purpose = 'Ballot Content';	2019-01-08 09:27:28.340	TraceMessage
Admin	Instance with name '4c95f7f1-51bc-4149-95ed-72f4c5f3ffe0' of type 'LanguageProfile' with id = '4c95f7f1-51bc-4149-95ed-72f4c5f3ffe0' is created.	2019-01-08 09:27:28.340	TraceMessage
Admin	Instance with name '20fe3ee1-22e3-4eb2-839d-cb69d505ef27' of type 'LanguageProfile' modified: name = 'English'; isDefault=True; purpose = 'Audio';	2019-01-08 09:27:28.340	TraceMessage
Admin	Instance with name '7ac70d62-bf0b-4d6e-8e78-3fc66bf8ef83' of type 'AppUser' modified: password changed; firstName changed from 'John' to 'Ben'; lastName changed from 'Smith' to 'Smythe'; position = "; description = "; contactAddress = "; contactPhone1 = "; contactPhone2 = "; contactEmail = ";	2019-01-08 09:27:28.340	TraceMessage
Admin	Instance with name '20fe3ee1-22e3-4eb2-839d-cb69d505ef27' of type 'LanguageProfile' with id = '20fe3ee1-22e3-4eb2-839d-cb69d505ef27' is created.	2019-01-08 09:27:28.340	TraceMessage
Admin	User initiates generation of password.	2019-01-08 09:27:28.343	UserAction
Admin	User initiates generation of password.	2019-01-08 09:27:32.063	UserAction
Admin	User initiates generation of password.	2019-01-08 09:27:32.063	UserAction
Admin	Project security elements created	2019-01-08 09:27:32.063	UserAction
Admin	User initiates generation of password.	2019-01-08 09:27:32.063	UserAction

Figure 13 - UserInfo Log Change from John Smith to Ben Smythe

Any user with access to the EMS using the EMS Admin username and password to log into the Dominion Democracy Suite Election Event Designer (EED) application will appear to be “Ben Smythe” in the log files. This obfuscates identity of the true user on the system and makes it impossible to perform security audits and ongoing monitoring for suspicious activities. The EED application is used to design the entire election, it is used to program the election files on to the compact flash cards, and it is used to program the security key fobs that are required to open, close, reopen, or rezero the polls.

If there were inappropriate or fraudulent activities occurring on the EMS they would be attributed to the shared account and follow-on investigations would be



stymied by the lack of specificity when it comes to the identity of the user active on the system.

Similarly, any user with access to the RTR using the EMS RTRAdmin username and password to log into the Dominion Democracy Suite Result Tallying and Reporting (RTR) application will appear to be “Ryan Smoth” in the log files. This was found in the template for Michigan (Figures 14 and 15). So one can assume that all counties in Michigan that were programmed using this template will all have Ryan Smoth as the RTRAdmin User. This obfuscates identity of the true user on the system and makes it impossible to perform security audits and ongoing monitoring for suspicious activities. The RTRAdmin operator account offers the option of choosing a “weak” password as a feature. (Figure 16) This option to choose a weak password is against all best security practices and leaves the RTR Operator role susceptible to exploitation by malicious cyber attackers. The RTR application is the one used to import, reject, validate, publish, and unpublish results contained on the compact flash cards and/or results transmitted via modem to a county-located Listener computer (proposed for Antrim but apparently not purchased) that then relays them to the EMS computer. Results can also be manually entered at this point overriding results from any other source. Once they are “published” into the reports that then go out to the media there is no external indication that the results were “manually” entered into the system instead of coming from the tabulators.

Admin	Instance with name '7ac70d62-bf0b-4d6e-8e78-3fc86bf8ef83' of type 'AppUser' modified: password changed; firstName changed from 'John' to 'Ben'; lastName changed from 'Smith' to 'Smythe'; position = "; description = "; contactAddress = "; contactPhone1 = "; contactPhone2 = "; contactEmail = ";	2019-01-08 09:27:28.340	TraceMessage
Admin	Instance with name '20fe3ee1-22e3-4eb2-839d-cb69d505ef27' of type 'LanguageProfile' with id = '20fe3ee1-22e3-4eb2-839d-cb69d505ef27' is created.	2019-01-08 09:27:28.340	TraceMessage
Admin	User initiates generation of password.	2019-01-08 09:27:28.343	UserAction
Admin	User initiates generation of password.	2019-01-08 09:27:32.063	UserAction
Admin	User initiates generation of password.	2019-01-08 09:27:32.063	UserAction
Admin	Project security elements created	2019-01-08 09:27:32.063	UserAction
Admin	User initiates generation of password.	2019-01-08 09:27:32.063	UserAction
Admin	Project ElectionSource.Famous Names Right Oval Closed	2019-01-08 09:28:46.907	UserAction
Admin	User initiates generation of password.	2019-01-08 09:28:46.923	UserAction
Admin	Prompt warning: 'Ballot style has not been set. Go to Settings/Election Event Properties menu, Ballot Settings option and select applicable ballot style.'; User answered with: 'OK'	2019-01-08 09:28:52.440	UserAction
Admin	Project Michigan Template opened	2019-01-08 09:28:57.657	UserAction

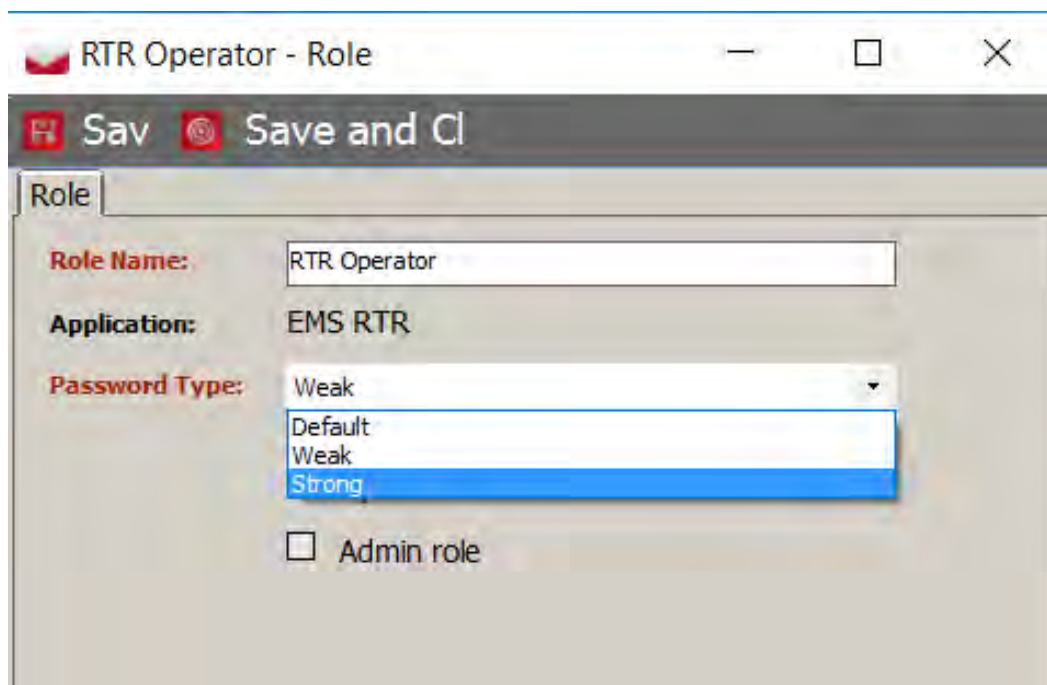
*Figure 14 - Michigan Project Template Opened*

733	Admin	Instance with name 'Transmit to Listener using SSL' of type 'NumberSystemParameter' modified: paramValue changed from '0' to '1';	2019-01-08 16:13:19.740	TraceMessage
734	Admin	Instance with name 'Transmit Results via internal port' of type 'NumberSystemParameter' modified: paramValue changed from '0' to '1';	2019-01-08 16:13:19.740	TraceMessage
735	Admin	Instance with name 'Disable SSL Certificate Verification' of type 'NumberSystemParameter' modified: paramValue changed from '0' to '1';	2019-01-08 16:13:19.740	TraceMessage
736	Admin	Instance with name 'Transmit Totals Results' of type 'NumberSystemParameter' modified: paramValue changed from '0' to '1';	2019-01-08 16:13:19.740	TraceMessage
737	Admin	Instance with name 'Transmit Results via external port' of type 'NumberSystemParameter' modified: paramValue changed from '0' to '1';	2019-01-08 16:13:19.740	TraceMessage
738	Admin	Instance with name 'Cross-voted Ballot' of type 'NumberSystemParameter' modified: paramValue changed from '1' to '0';	2019-01-08 16:13:19.743	TraceMessage
739	Admin	User initiates the Close Project activity	2019-01-08 16:13:19.743	UserAction
740	Admin	Instance with name 'write-in report enabled' of type 'NumberSystemParameter' modified: paramValue changed from '0' to '1';	2019-01-08 16:13:19.743	TraceMessage
741	Admin	Project Michigan Template Closed	2019-01-08 16:13:59.073	UserAction
742	Techadm	Project Michigan Template opened	2019-01-08 16:13:59.073	UserAction

*Figure 15 - Michigan Project Template Closed*

Thus “Ryan Smoth” can enter whatever numbers he would like while ignoring the original values on the encrypted compact flash cards and printed tapes. Mr. Smoth can then go back the next day or any day up until the day the canvass is performed and quietly reopen the polls, add a matching number of votes as he manipulated on election night, change the time to match the original paper tape, and print the results. When the canvass is performed the modified paper tape will match the modified manually entered results. This is obviously an unacceptable combination of features that should not be made available in a secure election system.


### Ability to set “Weak Passwords”



*Figure 16 - RTR Operator Password Strength Dialogue Box*

The password policy enforcement tool for the EMS gives the following error when we attempt to enter the current passwords used on the Antrim County EMS system.

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

A handwritten signature in black ink, reading "Jeffrey Lenberg". The signature is written in a cursive style with a horizontal line underneath it.

Jeffrey Lenberg

**MICHIGAN NOTARY ACKNOWLEDGEMENT**

State of Michigan  
County of Oakland

The foregoing instrument was acknowledged before me on this 16<sup>th</sup> day of May, 2021 by Jeffrey  
Lenberg.

Notary Public Signature: 

Notary Printed Name: Ann M. Howard  
Acting in the County of: Oakland  
My Commission Expires: 2/24/2023