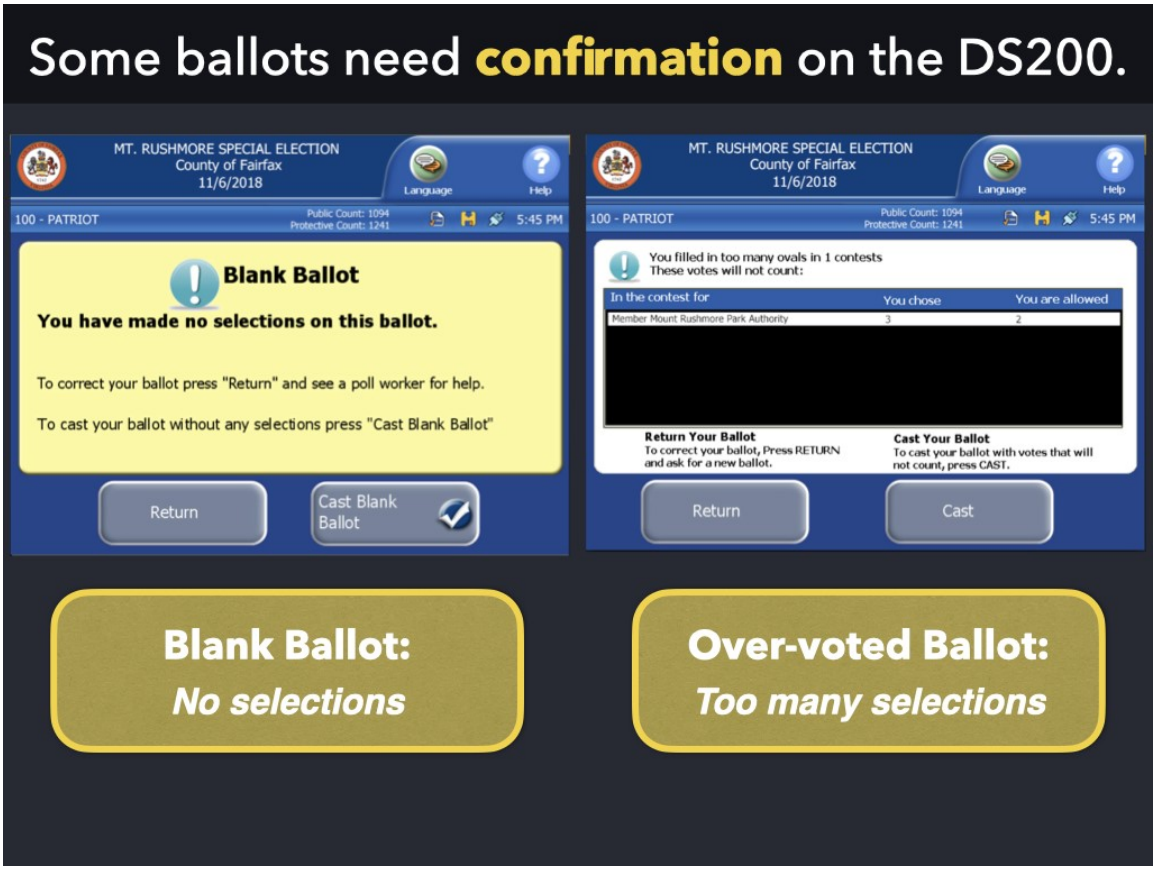
Vulnerabilities of the ES&S DS200 Vote Tabulator

John B. Nevin [https://uncoverdc.com/author/johnbnevin/]



[https://i1.wp.com/uncoverdc.com/wp-content/uploads/2021/08/Ballot-Confirmation.jpg?fit=1024%2C768&ssl=1]

More electronic voting machines in the United States are managed by Election Systems & Software [https://www.essvote.com/] (ES&S) than any other vendor. An in-depth review of the specifications and functions of one of the company's most used voting machines—the DS200 Vote Tabulator [https://www.essvote.com/products/ds200/] —reveals a machine with a difficult-to-detect modem buried in its motherboard, allowing the device mostly undetected access to the internet.

ES&S DS200 Vulnerabilities

Let's Fix Stuff reported [https://letsfixstuff.org/2021/04/modem-chips-embedded-in-voting-system-computer-motherboards/] that the DS200 has a modem embedded in its motherboard, noting that "*Malware can be embedded in hardware as well as software.*" Attorney Matt DePerno [https://uncoverdc.com/2021/05/07/dark-to-light-matt-deperno-election-integrity-in-antrim-mi/] included that finding in Exhibit 6 [https://www.scribd.com/document/513389247/Matt-DePerno-Antrim-Michigan-Lawsuit-Exhibit-6] of his Michigan lawsuit [https://uncoverdc.com/2021/07/15/deperno-persists-forensic-audit-in-michigan-a-must/] . According to Let's Fix Stuff, the chip is "*designed to operate on a virtual private network*" and enables communication with election servers while not having a visible external port:

> "*It is very difficult to detect unless you pry open the machine case to investigate the hardware… Anyone with access to any SIM card could have pre-programmed access to the APN… It demonstrates how electronic voting systems could be connected to the internet with minimal risk of detection.*"

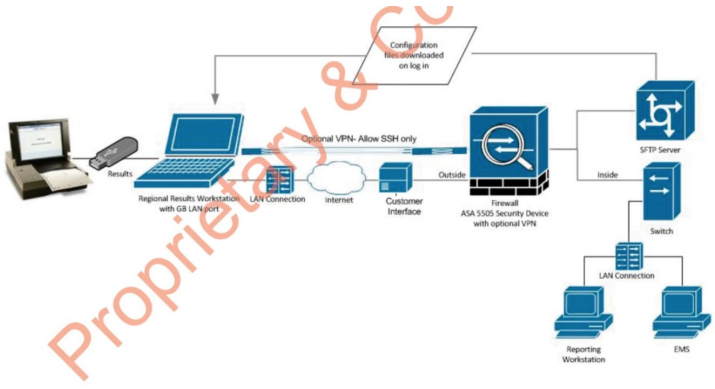
More detail on that vulnerability can be found in an affidavit [https://www.auditelectionsusa.org/2016/12/12/ess-ds200-wireless-vulnerabilities/] from the Executive Director of Americans United for Democracy, Integrity, and Transparency (AUDIT [https://www.auditelectionsusa.org/]), John Brakey. He describes himself as specializing in "evaluating the vulnerability and reliability of election systems" and says the machines are *"vulnerable to insider or sophisticated hacking."*

In 2017, Brakey sent a letter [https://www.scribd.com/document/513390945/AuditAZ-ES-S-DS200-Letter] to the State Election Director serving under the Secretary of State of Alabama [https://www.sos.alabama.gov/] advising that the digital images of cast ballots that are created by the DS200 are part of the chain of custody and therefore must be preserved per federal law—but the DS200 has a vulnerability in which menu options accessible to election officials allow images to be destroyed on election day.

There's a limit to how much we can find out about how the ES&S DS200 counts votes underneath the hood. The code is not open source—the "System & Method for Decoding Marks on a Paper Ballot" is a proprietary "trade secret" and considered intellectual property [https://www.essvote.com/intellectual-property/] owned by the company based on patent law.

"The fact that we have vendors that say 'you cannot look at our code' is the first problem," says Jake Stauffer, a former cyber analyst for the U.S. Air Force. He is one of few who have looked inside the ES&S DS200—his "Red Team" was approved to produce a "Vulnerability & Security Assessment Report [https://www.scribd.com/document/513400991/ESS-RedTeam-Jake-Stauffer-Vulnerability-Security-Assessment-Report] " for the State of California. He is featured in HBO's productions about vulnerabilities in America's voting systems: Hacking Democracy [https://www.imdb.com/title/tt0808532/] (2006) and Kill Chain [https://www.imdb.com/title/tt12041084/] (2020). In Hacking Democracy, he said:

> "*What we found… it's staggering. There were multiple vulnerabilities that could allow an attacker to get the highest level of access to the system. We found multiple operating system patches missing—what that means is that an attacker can inject code into that system, execute that with the possibility of receiving some sort of control.*
>
> *When ES&S discovered that we were not using their testing plans, they were appalled. When we used our own testing plan and found these vulnerabilities, they pretty much told us that they had their own team and that they were not interested.*
>
> *How can a vendor sell a voting system with this many vulnerabilities? I can't find a straight answer*."



ES&S DIAGRAM THE COMPANY SUBMITTED LAST YEAR TO TRAVIS COUNTY, TEXAS, AS PART OF A CONTRACT PROPOSAL SHOWS THE REPORTING SYSTEM AND ELECTION-MANAGEMENT SYSTEM DIRECTLY CONNECTED TO THE SFTP SERVER THROUGH THE SWITCH, AND ALL OF THEM ARE CONNECTED TO THE FIREWALL.

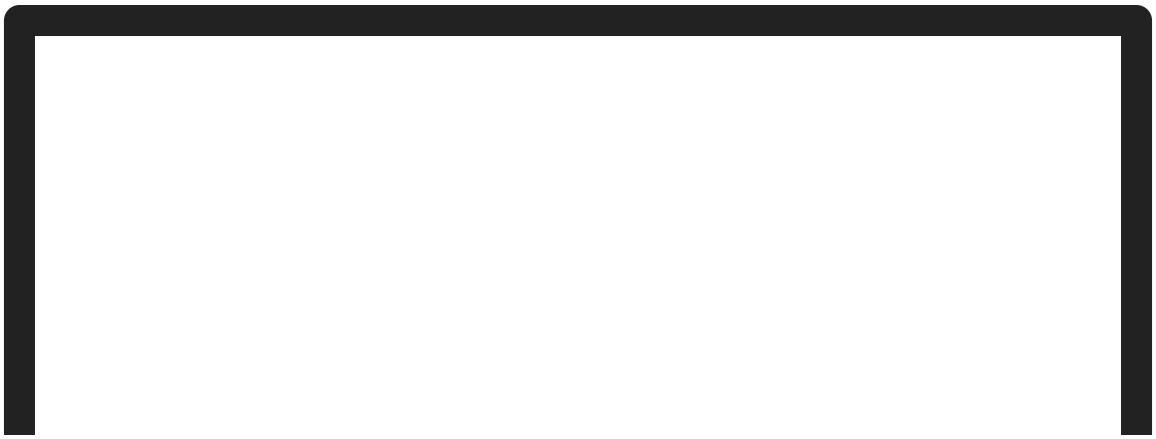
[https://uncoverdc.com/2021/08/03/vulnerabilities-of-the-ess-ds200-vote-tabulator/exclusive-critical-u-s-election-systems-have-been-left-exposed-online-despite-official-denials/] Among other vulnerabilities, the Red Team also found that the file systems on the flashcards used were not encrypted, the system was allowed to boot to a modified version, and that ballot images were unencrypted and alterable. Additionally, the password to access the SSH server *"was cracked within 46 seconds using a common dictionary attack."* The analyst says this process resulted in gaining remote access to an unmodified DS200.

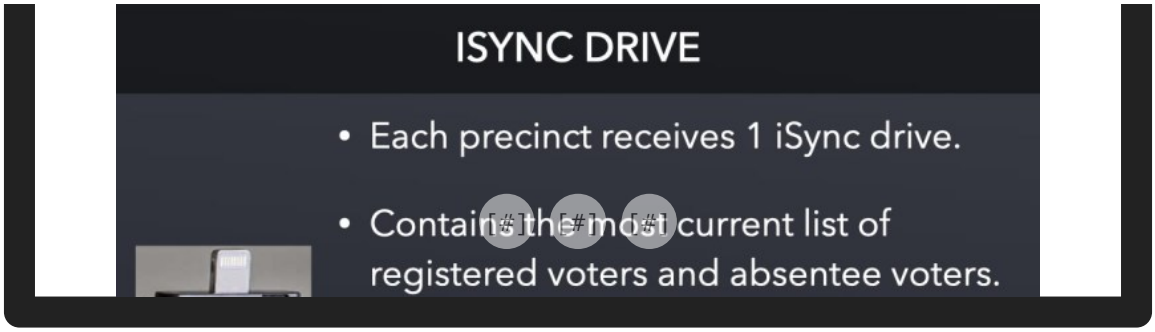
The Red Team report [https://verifiedvoting.org/wp-content/uploads/2020/08/ESS-red-team-CA-2016-1.pdf] states:

> "*Upon further investigation of the DS200, a weak root password hash was discovered, along with an SSH server that allows root logins as well as the ability to trivially image system memory (RAM). This could ultimately lead to a malicious actor obtaining a DS200 compact flash card, modifying the operating system's configuration, and putting a modified operating system into production unbeknownst to election officials or voters.*"

How ES&S DS200 Operates

Anoka County, Minnesota hosts start-of-day Set Up Instructions [https://www.anokacounty.us/DocumentCenter/View/10278/DS200-Ballot-Counter-Set-Up-Instructions-PDF?bidId] to be used by election administrators in precincts that use the DS200; Broward County, Florida created a training & procedures manual [http://assets01.aws.connect.clarityelections.com/Assets/Training/RootPreview/Customers/FL_Broward/Library/Manuals/VST_DS200_and_Ivotronic_Manual.pdf] for poll workers' election day operations, and the following are slides from Fairfax County, VA Office of Elections:





In precincts that operate under an election administration contract that calls for ES&S systems, the DS200 is used alongside optional devices, including the KNOWiNK Pollpad device that is pre-loaded with voter data from an iSYNC drive to check in voters and the ExpressVote Ballot Marking Device (BMD).

Appendix A: Percentage Market Share by Vendor

Vendor	Registrants Reached	% Market Share
Election Systems & Software	83,380,867	43.8%
Dominion Voting Systems	71,006,665	37.3%
Hart InterCivic	20,983,037	11.0%
Unisyn Voting Solutions	3,430,900	1.8%
MicroVote	3,291,260	1.7%
Danaher	2,685,409	1.4%
MTS	2,435,360	1.3%
IVS	1,336,070	0.7%
Five Cedars Group	972,475	0.5%
Clear Ballot	623,083	0.3%

Source: TrustTheVote.org Election Technology Report [https://trustthevote.org/wp-content/uploads/2017/03/2017-whartonoset_industryreport.pdf]

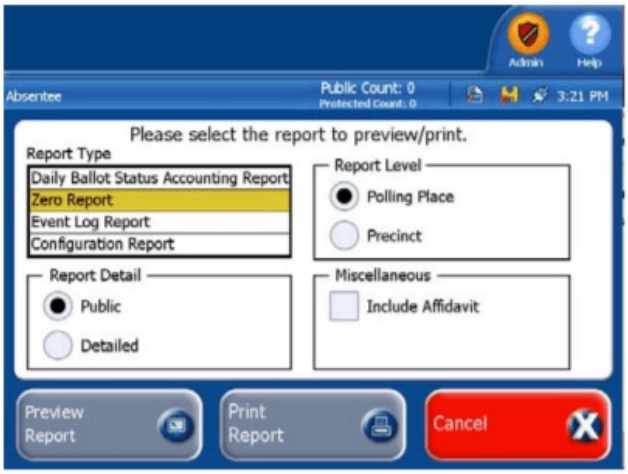
An administrator with password access to the printing options screen on a DS200 can select from several reports. These reports are then printed out on paper similar to a retail cash register or an ATM receipt. These are the “tally tapes” or “ballot tapes” we refer to throughout this article.

Report Options

From the Reports screen, you can print the following reports:

- Press **Ballot Status Accounting Report** to reprint your ballot status accounting report.
- Press **Zero Report** to reprint your zero report.
- Press **Event Log Report** to print an audit log of the activity that has occurred on the scanner. Information such as the date and times when the system is initialized and when it prints reports appears on this report.
- Press **Configuration Report** to print a system configuration report. Information such as election settings, diverter settings and firmware version appears on this report.

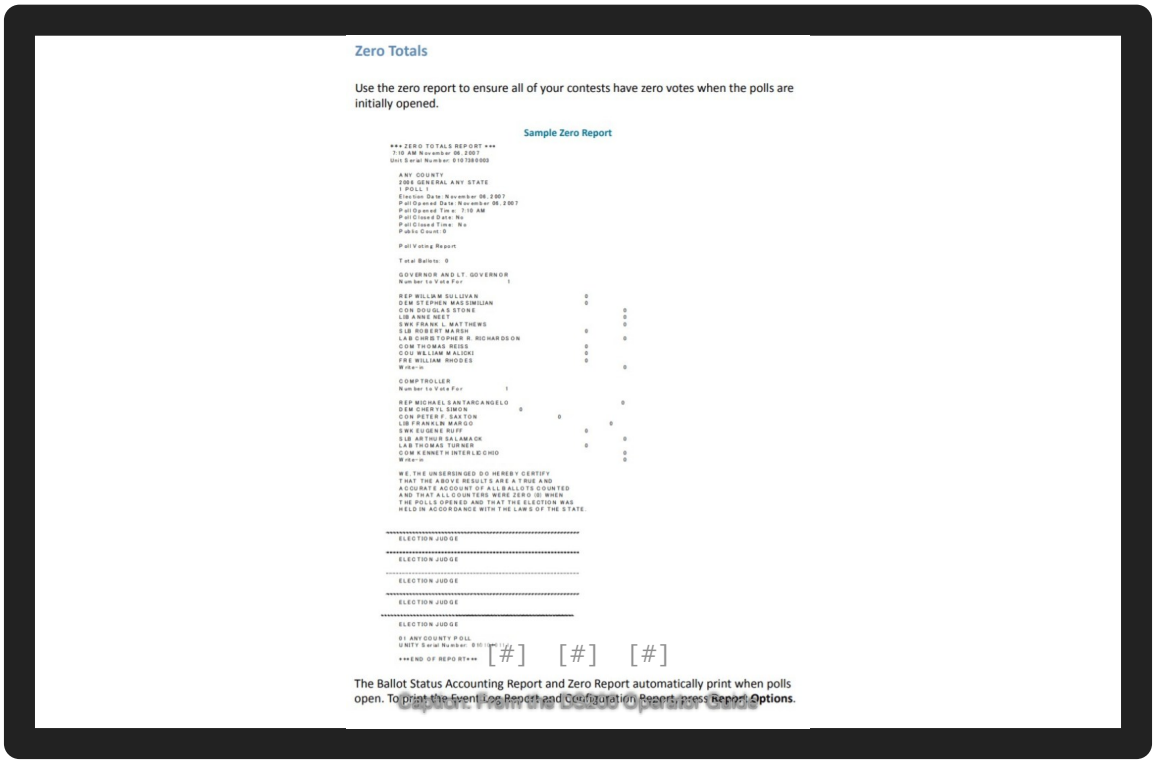
- Press **Preview Report** to view a previewed copy of the report on the screen.
- Press **Print** to print a hard copy of the report.



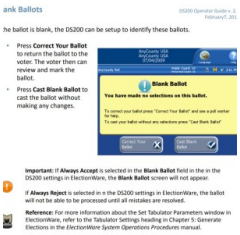
Caption: From the DS200 Operator Guide

Based on the manual, the DS200 instructions give us these definitions of the various printable report types:

- Ballot Status Accounting Report: "[A] descriptive list of system settings that automatically generates when you turn on the scanner. The report includes a list of election configuration settings if the election definition is loaded when you turn on the scanner."
- Zero Totals Report: "[Used to] ensure all of your contests have zero votes when the polls are initially opened."
- Event Log Report: "…lists all of the scanner events that occur from the time you load your election definition USB flash drive into the scanner until you remove the flash drive after the election is complete."
- Configuration Report: "…lists information such as the storage memory availability, firmware information and basic scanner information such as the status of the touch screen and battery charge level."
- Voting Results Report: "…prints the results of your elections."



The "Election Definition" for each jurisdiction is programmed onto a USB flash drive for each tabulator. As stated in the DS200 manual, "An election definition contains all of the candidates, contests and ballot variations that the scanner will process at the polling place. The election definition also contains customizable program options that control how the tabulator operates and reports results." In each jurisdiction, those options — such as whether polls can be re-opened, whether results reports are automatically printed when polls close, and whether the voter can override a rejected ballot — are all decided beforehand and loaded into the "Election Definition."



Caption: From the DS200 Operator Guide

During election day, when a voter tries to cast their paper ballot into the DS200, it could be rejected from the feed mechanism for the reasons explained below. The configuration options above determine the conditions that will trigger the machine to reject a ballot. The machine makes an audible sound, and the voter is shown a message on the screen. Here's a screenshot of an example of what is seen by the voter when their ballot is rejected (in this case because it is blank):

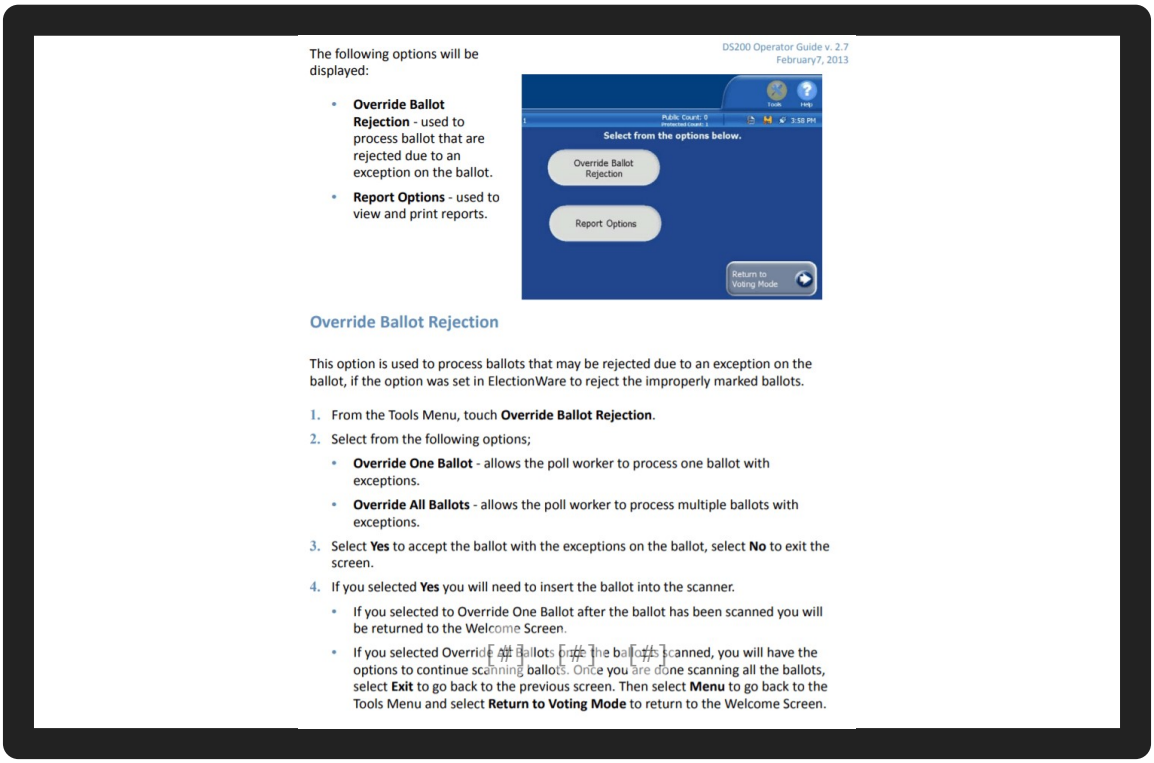
From the ES&S DS200 Operator's Manual:

> "*The DS200 can scan ballots inserted in any direction or orientation. Depending on the options set for your election definition, the DS200 will use one of the following methods for accepting or rejecting blank ballots, overvotes, and undervotes.*
>
> *Unconditional acceptance: The scanner accepts and tabulates results for all ballots. Any contests that are blank, overvoted, or undervoted will be logged as such, and the remaining contests will be tabulated appropriately.*
>
> *Unconditional rejection: The DS200 automatically rejects undervoted, overvoted, or blank ballots. Voters must review and correct ballot selections before the scanner will accept the ballot.*

Query the voter for correction: The DS200 returns a questioned ballot to the voter and displays a screen message that describes the problem and prompts the voter to either review and edit the ballot or cast the ballot as it is."

An election day training manual [https://sos.idaho.gov/elect/Clerk/DS200%20Procedures/U3400_TRN00_DS200_Election.pdf] for the ES&S DS200 explains other conditions in which the machine can be programmed to reject a ballot:

- If the voter has 'undervoted,' it means there are too few markings for the ballot to be considered valid. For example, the voter did not mark any ovals for any candidate.
- If the voter has 'overvoted,' it means there are too many markings for the ballot to be considered valid. For example, the voter marked both Candidate A and Candidate B's ovals.
- If the voter has 'crossover' voted, it means there are markings for more than one party during a closed primary election.
- The ballot may also detect one of these conditions and automatically allow the ballot to pass through into the storage bin.



DS200 Operator Guide v. 2.7
February7, 2013

The following options will be displayed:

- **Override Ballot Rejection** - used to process ballot that are rejected due to an exception on the ballot.
- **Report Options** - used to view and print reports.

Override Ballot Rejection

This option is used to process ballots that may be rejected due to an exception on the ballot, if the option was set in ElectionWare to reject the improperly marked ballots.

1. From the Tools Menu, touch **Override Ballot Rejection**.
2. Select from the following options;
   - **Override One Ballot** - allows the poll worker to process one ballot with exceptions.
   - **Override All Ballots** - allows the poll worker to process multiple ballots with exceptions.
3. Select **Yes** to accept the ballot with the exceptions on the ballot, select **No** to exit the screen.
4. If you selected **Yes** you will need to insert the ballot into the scanner.
   - If you selected to Override One Ballot after the ballot has been scanned you will be returned to the Welcome Screen.
   - If you selected Override All Ballots for the ballots scanned, you will have the options to continue scanning ballots. Once you are done scanning all the ballots, select **Exit** to go back to the previous screen. Then select **Menu** to go back to the Tools Menu and select **Return to Voting Mode** to return to the Welcome Screen.

If you have more information about the DS200 machine, including how to interpret the ballot tapes, please contact us at tips@uncoverdc.com.

[https://uncoverdc.com/author/johnbnevin/]

John B. Nevin [https://uncoverdc.com/author/johnbnevin/]