Examination Report on the Hart Verity Vanguard 1.0 Voting System

Andrew W. Appel, October 17, 2025

1 Executive Summary

In my capacity as Examiner of Voting Machines, appointed by the Attorney General of Texas, to advise the Secretary of State on whether to certify the Hart Verity Vanguard 1.0 voting system, I make the following recommendations:

Hart Verity Vanguard 1.0 is a well-designed voting system, suitable for use in the State of Texas for conducting elections, with these restrictions, limitations, and recommendations:

1. The "Adapt" ballot-marking device (an assistive device for persons with disabilities who cannot mark a paper ballot by hand) can be used in Texas only if its procedures for ballot tabulation can be reconciled with Texas law. See section 6.
2. The Secretary of State should provide clear instructions for election-office workers using the "Capture" central-count scanner about how to handle rejected ballots, in case those rejected ballots are legitimate PVR ballots within a batch of hand-marked ballots, or vice versa. See section 8.1.
3. The Hart documentation package accompanying the system should state that the Vault precinct-count optical scanner is a tabulating device, instead of saying (as it does now) that it is not a tabulating device. See section 19.
4. The Secretary of State should provide clear instructions for county election administrators about how to handle the rare (but possible) case where there is a large number of undervotes in a contest that includes qualified write-in candidates. See section 7.1.
5. Since this voting system is designed for use with tamper-evident seals, Texas counties that deploy this voting system should design and deploy a *seal use protocol* specialized to the use of seals on Hart Verity Vanguard equipment. The Director of Elections should consider designing a *model seal use protocol* that counties could adopt. See sections 17 and 18.
6. Texas law requires "hash validation" of voting machines, that is, a procedure for checking whether the voting machine contains the expected, legitimate software. The Hart Verity Vanguard equipment allows different methods of performing hash validation. In light of considerations that I will describe in this report, I suggest that the Director of Elections should recommend to the Secretary of State which of these methods to use, or which combination of methods. See section 13.
7. The Hart Verity Vanguard 1.0 system includes equipment that can be used in polling places for either hand-marked optical-scan paper ballots, or ballots marked via a touchscreen interface (ballot-marking device). Ballot-marking devices are inherently less secure than hand-marked ballots, so jurisdictions adopting the Verity Vanguard system would be wise to use Verity Vanguard with hand-marked paper ballots for all voters except those who cannot mark a paper ballot by hand. For those voters who cannot mark a paper ballot by hand, the "Flex" ballot marking

device, one component of the Verity Vanguard system, is an appropriate voting method. See section 16.

2 Basis for my findings

My conclusions and explanations are based on:

1. My experience studying voting machines, election security, and election procedures since 2004;
2. My reading and understanding of Texas election laws and procedures (though I am not a lawyer);
3. My reading of the Technical Documentation Package provided by Hart to the Election Assistance Commission and to the Secretary of State of Texas, and a report from the EAC-certified Voting System Test Laboratory (VSTL);
4. My observations during the examination meeting, three full working days September 16-18, 2025 at the Office of the Secretary of State in Austin. During this meeting I asked the Hart personnel many dozens of technical questions; the Hart personnel at this meeting had enough technical knowledge about the design, operation, programming, and hardware to be able to answer those questions. Also during this meeting I observed the operation of this equipment by Hart personnel, by staff of the Secretary of State, by other Voting Machine Examiners, and by myself personally.

Many of my analyses and conclusions are, necessarily, based on statements made by Hart personnel, both in writing (in the Technical Documentation Package) and orally (during the 3-day meeting), about how their system works. I will take those statements as made in good faith. But even so, it can happen that the engineering of a system does not always match the intended design: a system may not be as accurate or as secure as its designers believe it to be. In my report I will discuss ways to mitigate these unknowns to achieve trustworthy elections.

3 General principles regarding the use of computers in elections

When we use computers to count votes in our elections, and aggregate vote-counts from different polling places together, we must be aware that computers are general purpose devices whose operation depends entirely on what program is installed. Computer programs may have *bugs*, unintentional programming mistakes that might (in a voting system) lead to miscounting votes. Computer systems may have *security vulnerabilities,* flaws that allow a malicious attacker to make the system miscount votes in favor of the attacker's preferred candidate. To conduct trustworthy elections with computers, we must therefore do *all* of the following:

1. Reduce the number (and severity) of bugs as much as possible by careful design of the hardware and software, and by thorough testing.
2. Reduce the number (and severity) of security vulnerabilities as much as possible by careful design and by using standard, state-of-the-art best-practice designs and methods.
3. Recognize that even with state-of-the-art design and security practices, we can never be 100% sure what software is in a voting system—no voting system can be *perfectly* secure—so we must have means independent of the computerized voting machines to assure that the outcome of the election corresponds to the choices indicated by the voters. This is normally achieved via hand recounts or risk-limiting audits of paper ballots.
4. All of-age resident citizens (unless specifically disqualified) must be able to register and vote, and none but eligible voters. However, voter registration systems and practices, and electronic and paper pollbooks used in polling places, are outside the scope of the current examination, and I will generally not address them.

As of 2025, all three of practices 1-3 are employed in Texas, by statute and by practice.

1. Bugs: It is up to the maker of the equipment to minimize the bugs. However, Texas's certification procedures require examination by EAC-certified Voting System Test Labs (VSTLs) that is a prerequisite to acceptance by Texas. That VSTL examines the source code and hardware of the voting machine, and performs extensive tests of the voting system's operation. The examinations performed in Texas, by examiners appointed by the Secretary of State and Attorney General, have neither the time nor the resources to examine the source code and internal hardware, so we rely on the report from the VSTL.
2. Security: It is up to the maker of the equipment to use a state-of-the-art security design, and it is up to the county that adopts the voting system to use it with security practices adapted to that design. Texas's certification procedures, in the present examination, are reasonably effective in assessing the security of the voting system. Then it is up to the Texas lawmakers and officials to use secure procedures in connection with these machines. These procedures may vary depending on the characteristics of the voting system, so I have made some recommendations about specific procedures for use with the Hart Verity Vanguard 1.0 system.
3. Audits: The only known practical way to ensure that election outcomes reliably reflect the voters' choices—even though we cannot be entirely sure that the computers have no bugs or vulnerabilities—is to have voters mark paper ballots, protect those paper ballots from tampering through good chain-of-custody procedures, and then to either recount the paper ballots by hand or perform a *risk-limiting audit* (RLA) that examines a well-chosen random sample of the ballots, by

hand. Texas, by law, has a pilot RLA program and a goal of achieving full-scale RLAs in the future. In my examination of the Hart equipment, I assess whether it is compatible with efficient RLA procedures.

4 Components of the Verity Vanguard 1.0 voting system

The system presented for examination and certification includes,

- **Election office equipment:** Workstations (desktop computers), high-speed ballot scanners, and printers. On the workstations there are several *application programs:*
  - **Design,** for specifying the contests in an election, the candidates in those contests, the precincts and polling places, and so on.
  - **Deploy**, for turning all this information into ballot layouts in the format that the voter will see.
  - **Capture,** for using *central-count optical scanners* to scan those ballots that are not scanned in the polling places: absentee ballots, accepted provisional ballots, emergency ballots, and ballots from polling places that use ballot boxes instead of precinct-count optical scanners.
  - **Results**, to complete the adjudication process for ballots with ambiguous marks and to count the votes that have been scanned.
  - Several other application programs useful for administration of elections.
- **Polling place equipment,** which Hart refers to as Verity Vanguard *Devices*:
  - **Vault,** Hart's name for its precinct-count optical scanner in the Vanguard system.
  - **Flex,** a touchscreen ballot-marking device (BMD). Those voters who are not marking a paper ballot with a pen, can use this BMD to make selections that then get printed onto an optically scannable paper ballot called a Printed Vote Record (PVR). For voters with vision or motor disabilities who are not able to see or touch a touchscreen, there are ATI (Audio-Tactile Interface) devices. The Flex device does not record or tabulate votes; instead, the PVR ballot is meant to be fed into a Vault optical-scanner (in the polling place) or (more rarely) sent to an election office for central-count optical scan.
  - **Boost,** a pollworker-operated device that serves both as a ballot-on-demand (BOD) system for hand-markable paper ballots and as a means of issuing tickets for voters using Flex BMDs. It is possible for a jurisdiction to run a polling place without using the Boost.
  - **Adapt,** a ballot-marking device with assistive technology that allows voters with disabilities to mark and review a paper ballot without having to handle the ballot.
  - **Imprinter,** an accessory to the Vault optical scanner for numbering ballots.

5 Usability by voters

A voting system must be *usable* by voters, by pollworkers, and by workers in the election office who organize elections, design ballots, and maintain the equipment. An important part of usability is the design of the paper ballots.

Design of hand-marked paper ballots. The system must be designed so that voters can understand their ballots; the ballots must be laid out in ways that do not lead voters to inadvertently mismark their ballots. This is important because badly designed ballots can cause voters to mistakenly overlook some contests on the ballot and miss the opportunity to vote in those contests. The Hart Verity Vanguard *Design* application allows election administrators to design ballots that conform to recognized standards for ballot design. However, the *Design* application also permits election administrators to violate those design standards. This is not illegal, and sometimes it may be useful to violate one design rule to make an overall more usable ballot layout. However, in those cases it would be advisable to alert the election administrator that a design rule is violated, to ensure that is a conscious decision rather than an unintended mistake. Ideally, the *Design* application would have better support for election administrators in producing well-designed ballots. However, as it is I still find the *Design* application suitable for use in Texas. Overall, the hand-markable paper ballots are well designed and easy for voters to understand.

Design of BMD-marked ballots. The design of the Flex touchscreen BMD device, and the presentation of contests, candidates, choices, and review screens, is suitable for use. Other Examiners on the team studied this point in more depth than I did, and may have more to say about this.

Regarding the design of the PVR (printed vote record) ballot produced by the Flex device: this is adequate for use by voters who cannot mark a paper ballot by hand. Unlike a hand-markable paper ballot, the PVR does not list all candidates in each contest and indicate which candidate is chosen. Instead, it lists only those candidates that the voter chose, in block capitals in a small font. (A small font is used to ensure that a ballot with many contests will have a PVR summary that fits on one page.) SMALL TEXT IN ALL CAPS IS NOT AS EASY FOR VOTERS TO READ as mixed-case text in the larger font that is used on hand-markable paper ballots. Several studies have shown that voters who have used BMDs do not carefully check their PVR ballots to make sure the candidates listed there are the same ones they selected on the touchscreen.[1] This has significant consequences for the trustworthiness of elections.[2] Therefore: the Flex device is *sufficient* for use by voters with disabilities who

[1] Those studies were not necessarily on Hart Verity Vanguard PVR ballots, but using BMD-printed ballots with generally similar characteristics.
[2] See: Ballot Marking Devices Cannot Ensure the Will of the Voters, by Andrew W. Appel, Richard A. DeMillo, and Philip B. Stark, *Election Law Journal* Volume 19, Number 3, pages 432-450, 2020.

cannot mark a paper ballot by hand, since the alternative of reading a hand-marked paper ballot is not available to those voters. For use by voters who *can* mark a paper ballot by hand, the Flex device can be regarded as *barely sufficient,* or as *sufficient by Texas law.*

QR Code on Flex ballot *not harmful*. The PVR ballot printed by the Flex and Adapt ballot-marking devices includes both human-readable text listing the voter's selections and a QR code. Voting systems in which votes are represented in barcodes or QR codes, and in which the optical scanners read votes from barcodes (or QR codes) and don't read the human-readable text, pose a grave security concern, because they make it impossible for the voter to verify that the votes on their paper ballot are cast correctly.[3] However, the QR code on the Flex ballot *does not contain any votes that the optical scanner can read.* Verity Vanguard optical scanners (the *Vault* precinct-count optical scanner and the *Capture* central-count optical scanner) read the votes from the human-readable text, by optical-character recognition (OCR). The QR code contains only ballot-style information (i.e., which voting district) and error-correction information to ensure the accuracy of the OCR.[4] Therefore, the Flex PVR ballots should not be considered as "barcode ballots" and they do not present the same security risk as conventional barcode ballots.

6 The Adapt device

Rationale for the Adapt device. The Flex BMD is suitable for use by voters with disabilities who cannot mark a paper ballot by hand. However, after the voter has used the Flex's touch screen or audio-tactile interface (ATI) to mark the ballot, the voter must remove the marked paper ballot from the Flex and carry it to the Vault optical scanner and insert it there. If the voter has a disability that prevents them from performing this task, they must seek the assistance of a pollworker or other assistant. It is my understanding that even so, BMDs with this style of interface are sufficient under Texas law as an assistive technology for voters with disabilities (but I am not a lawyer). Even so, many voters with disabilities would prefer to use a voting machine that does not require them to handle the paper ballot (or to let a pollworker handle their paper ballot).

An optional component of the Verity Vanguard system is the *Adapt* ballot-marking device. This device allows a voter to indicate choices using either a touchscreen or audio-tactile

---

[3] See: Evidence-Based Elections: Create a Meaningful Paper Trail, then Audit, by Andrew W. Appel and Philip B. Stark, *Georgetown Law Technology Review*, volume 4, pages 523-541, 2020.

[4] The Vanguard 1.0 System Administrator's Guide, page 156, says the "Security Hash" (included in the QR code) is "A hash of the voter selections for this sheet. This hash is used to verify the accuracy of the selections returned by optical character recognition. This hash cannot be used to determine the voter's selections." It may not quite be true that "this hash cannot be used to determine the voter's selections", because an exhaustive search of all possible combinations of selections would find one that matches the hash. However, I do not see any way that this compromises the security, privacy, accuracy, or reliability of voting.

interface (ATI). Then, when they have reviewed their choices on the screen (or via audio), the Adapt prints a paper ballot (in the PVR format) and displays it to them under glass. This allows a voter (unless severely visually impaired) to see the actual paper ballot and verify that it contains the correct selections. Blind voters can opt to have the PVR optically scanned and read back to them via audio.[5] The voter can then indicate whether to accept the ballot. If the ballot is accepted, the Adapt conveys the paper ballot into a ballot box, without the voter having to handle it. The Adapt device does not retain an electronic copy of the ballot—it does not tally votes. Therefore, the paper ballots that accumulate during election day(s) on the Adapt must be removed (by pollworkers) from that ballot box and scanned, either by the Vault device in the polling place or by a central-count optical scanner at the election office.

A very important feature of the Adapt is that, after the PVR ballot is printed and displayed to the voter, there is no way that the physical mechanism can convey the PVR back to the printer, *even if all the software on the Adapt were to be replaced by fraudulent software that wanted to print different votes onto the ballot after the last time the voter inspected it.* Several BMDs previously made by various voting-machine companies had mechanical paper paths that *did* allow printing after inspection (if the software were to be hacked). Those other BMDs would not be sufficiently secure to use in elections; and would not comply with requirement 9.1.5-G of the VVSG 2.0, the Federal Voluntary Voting Systems Guidelines version 2.0. But the Adapt's paper path does have this very desirable security measure.

On the basis of its good user interface, and on the basis of its security design, I would be prepared to say that the Adapt is sufficient for use in Texas elections. But there are two deficiencies in its design that lead me to deem the Verity Vanguard 1.0 version of the Adapt *possibly insufficient for Texas elections.* They are: the method of handling provisional ballots, and the method of scanning ballots for later tallying. As I will explain, if Texas procedures could be reconciled with the capabilities of the Adapt, there could be a pathway to certifying the Adapt for use in Texas.

How the Adapt handles provisional ballots. Texas, like most states, handles provisional ballots as follows. If a voter cannot document at the polling place that they satisfy the requirements to cast a regular ballot, that voter marks a ballot and puts it into an envelope. Then the voter or pollworker writes identifying information on the envelope. Then, if within some specified deadline after election day the voter can bring appropriate proof of

[5] Some voters may find comfort in this "read-back" feature, but it does not add any real measure of security or reliability to the voting process. Just before the Adapt prints the paper ballot, the voter is presented with a "review screen" that is accompanied by an audio presentation of the selections voted for. The only plausible way that the printed ballot could differ from this review screen is if the software in the Adapt were hacked by an attacker with the goal of changing votes. Any such attacker would be able to also modify the "read-back" so that it reads back the votes from the previous review screen instead of what's actually on the paper.

eligibility to cast that ballot, the election office moves that envelope into the batch of ballots that will be opened and counted (typically by optical-scan).

But the way the Adapt device handles provisional ballots makes this procedure difficult. For a disabled voter who wants to cast a ballot on the Adapt, the pollworker indicates on the Adapt touchscreen the ballot style number (i.e., voter's voting district or precinct) and whether or not the ballot is provisional. Then, when the Adapt prints the PVR ballot, provisional ballots are marked as PROVISIONAL both in human-readable text and in the QR code. The Adapt then conveys the provisional ballot into the same ballot box as regular ballots. When those ballots are later scanned, the optical scanner can be configured either to count all provisional ballots or reject all provisional ballots found in that batch, but there is no envelope with voter-identifying information—there is no way to "cure" the ballot based on information later provided by the voter, because the connection has been lost between the ballot and the voter's identity.

To use the Adapt with provisional ballots, the following method must be used in the polling place. The election worker brings the provisional voter to the Adapt machine, activates the machine (indicating that it is a provisional ballot), then backs away so the voter can vote with privacy. When the voter is done, and the ballot has been deposited in the voted-ballot compartment, the election worker must immediately open the voted-ballot compartment and remove the topmost ballot. The ballots in that compartment are neatly stacked,[6] so the provisional ballot will be on top. Then that ballot can be put into the provisional-ballot envelope as usual.

I would consider this method *adequate,* but it has some disadvantages. The optics of opening a ballot-box mid-election may be difficult to explain to those witnessing it. Taking the top ballot from the stack, face up, seriously compromises the privacy of the ballot.[7]

However—not just on the Hart Verity Vanguard equipment but using any known technology—I am not sure there is *any* method by which voters with certain disabilities could cast provisional ballots with perfect privacy. So this method may no worse than other methods.

---

[6] The fact that Adapt ballots are neatly stacked in voter order is not necessarily a ballot-privacy problem. The intended use of Adapt is that, upon the close of the polls, those ballots are inserted into a Vault precinct-scanner to be tabulated. The Vault randomizes the order both physically (the Vault's ballot box is large enough so the ballots do not stack exactly in order) and electronically (by randomizing the order of the CVR file).

[7] A simple software modification to the Adapt could make it more suitable for handling provisional ballots. Provisional ballots should be ejected from the top of the machine for the pollworker to put into an envelope. Mechanically, the Adapt hardware is able to do this already. This change would eliminate the need for a pollworker to open the voted-ballot compartment immediately after a provisional ballot is cast. There would still be a ballot-privacy issue, however. The ejected ballot lies face-up on top of the machine, for the pollworker to remove. It is easy for the pollworker to see what's printed on the ballot.

Tabulating Adapt ballots. There is one more aspect of the Adapt that is reasonable in itself but may pose problems in conjunction with Texas law. As I noted above, the Adapt does not count or tally votes, nor retain an electronic record (such as a CVR, cast vote record) of the votes. The paper ballots that accumulate in the ballot box are meant to be scanned, at the polling place, with the Vault optical scanner as part of the process of closing the polls. The reason for doing this is to preserve the secrecy/privacy of the ballot for voters with disabilities by mixing their ballots into the same batch of ballots as the rest of the voters at that polling place.

I am informed that under Texas law, unlike in many other states, it is not permissible for poll workers to feed a batch of ballots into the precinct scanners. In some other states, for example, if an equipment failure causes voters to have to deposit their ballots in the emergency ballot slot for later scanning, and that equipment failure is remedied during election day at the polling place, it is appropriate and permissible for pollworkers to remove those ballots from the emergency ballot box and immediately feed them into the optical scanner.[8] Texas law, in light of the danger of illegitimate ballot-box stuffing, prohibits this procedure.

Instead, if the Adapt were to be used, one interpretation of Texas law is that pollworkers would have to remove the ballots from the Adapt ballot box and put them into a sealed ballot bag to be conveyed to the election office for central-count optical scanning. Central-count scanning of Adapt ballots has several disadvantages:

- First and foremost, unless special measures were taken, it would lead to a small batch of ballots being counted and reported, that contain only the votes of voters with disabilities at that polling place. This would compromise the privacy of the ballot.
- Second, a separate batch of ballots from each polling place destined for the central-count scanners imposes extra administrative effort and extra time and delay in reporting election results.

How to reconcile the Adapt with Texas procedures. Perhaps Texas's prohibition on pollworkers inserting ballots into polling-place scanners is not absolute. For example, suppose a disabled voter uses a conventional polling-place ballot-marking device (such as an ES&S ExpressVote or a Hart Verity Duo, both of which are currently in use in Texas) to prepare and print a ballot. If that voter is physically unable to insert that ballot into a polling-place optical scanner, then presumably a pollworker must assist the voter by *inserting the ballot into the scanner slot.* Now consider the situation where, during an election day, some voters with disabilities have used the Adapt device, and those ballots

[8] *See* "When the optical scanners jam up, what then?" by Andrew Appel, November 2018, https://blog.citp.princeton.edu/2018/11/09/when-the-optical-scanners-jam-up-what-then/

need to be transferred to the Vault optical scanner. Pollworkers performing that procedure are simply *assisting voters with disabilities to insert their ballots into the scanner.*

Therefore I conclude: The Hart Verity Vanguard Adapt can be conditionally certified for use in Texas, as follows. If the Secretary of State and/or Attorney General determine that it is permissible for pollworkers, in the presence of witnesses and with carefully designed procedures, to insert ballots *cast by voters with disabilities* into polling-place optical scanners; or if the Legislature modifies the Texas Election Code to permit this; then the Adapt would be sufficient for use in Texas elections without need for modification or reexamination.

7 Usability by pollworkers in polling places

In observing the operation of the polling place equipment, and reading the user manuals for this equipment, I did not see any usability problems. The equipment is suitable in this regard.

7.1 Write-in candidates with bubble not marked

There is one exception: If a voter fills out a hand-marked paper ballot and writes in a write-in candidate without blackening the "bubble," the Vault polling-place scanner counts this as an undervote. However, I am informed that by Texas law such a ballot should count as a write-in. If undervote alerts are enabled in the election definition, then the voter (after feeding the ballot paper into the Vault device) would get a message that, in this particular contest, they have "undervoted" (not voted for as many candidates as they are eligible to vote for). If the voter were to correctly understand this message to include, "you did vote via write-in but forgot to blacken the bubble", then the voter could take appropriate action (take back the ballot paper that the Vault has spit out, bring it to a marking booth, and fill in the bubble). However, election administrators rarely enable undervote alerts on polling-place scanners, because voters commonly undervote on purpose (there are contests in which they don't care to vote) and undervote alerts would slow down the process.

A better design would be for the Vault precinct scanner and Capture central scanner to detect when there are marks in the write-in area and the bubble is not filled in. On the Vault scanner, this would alert the voter to the need to fill in the bubble. This alert could be distinct from the undervote alert and could be enabled even if the undervote is not enabled. On the Capture scanner, this would flag the ballot for adjudication. However, this design is not what Hart has implemented.

To accommodate the Verity Vanguard 1.0 system to the Texas law that requires the intent of the voter to be respected, I recommend that the Director of Elections advise county election administrators as follows:

> In any contest with a qualified write-in candidate, if the number of undervotes plus the number of write-ins exceeds the number of votes for the (otherwise) winning candidate[9], then all undervoted ballots must be examined to see if there is a write-in candidate with an unmarked bubble. This examination may be done on the paper ballots or on the digital ballot images.[10]

This procedure would achieve the correct *outcome*, in the sense of, "ensure that the candidates with the most votes are the ones that win the election."

8 Usability by election office staff

Election season is a busy and hectic time for election-office staff. A problem that has plagued some computerized voting systems is that mistakes by election workers are not caught by the voting software and its user interfaces. These kinds of mistakes have included:

- Printing a set of optical-scan paper ballots, then adjusting the election definition (perhaps because some candidate must be added or removed from the ballot); which causes the positions of the vote bubbles to shift; which means that the new election definition is incompatible with the printed ballots, and vote-marks will be counted for the wrong candidates.
- Loading a results cartridge (e.g., USB thumbdrive) from a voting machine into the workstation to upload votes; then doing it again, causing one precinct's votes to be double-counted.

The Verity Vanguard workstation applications have good protections against these and other mistakes. For example, if an election worker uploads votes by inserting a vDrive that came from an election-day voting machine, the system checks whether that batch of votes has already been uploaded.

For another example, before ballots can be printed and the Election Definition File created for loading into voting machines, an Election Number must be assigned in the Vanguard Deploy application. If the election definition is then modified in the Define application (it cannot be modified in Deploy), then it must be sent back to Deploy where a *new* election number is assigned. These election numbers are printed (in barcodes) on the paper

[9] Or, in a vote-for-N contest, the winning candidate with the least number of votes among winning candidates

[10] For risk-limiting audits one must use the paper and not the digital images, because one of the purposes of the RLA is to check whether the software is cheating—and if the software is cheating then it can present fraudulent images. But here the purpose is to check whether the voter forgot to fill in a bubble, not to check on mistakes by the software, so the use of the digital image is acceptable. And if an RLA does take place later, it will examine the paper ballots, possibly including this voter's.

ballots[11] and stored as part of the election definition. If the paper ballot is marked by a voter and fed into a voting machine, the machine will reject it as "from the wrong election." If this occurred in the polling place, the voters would still be able to vote by means of emergency ballots; that's inconvenient but it's not as bad as counting their votes for candidates they didn't intend.

8.1 Scanning mixed batches in the Capture application

In observing the operation of the Vanguard Workstation applications and reading the user manuals for these applications, I did not see any usability problems except one:

The Vault polling-place optical scanner can scan a mixed batch of hand-marked ballots and PVR (machine-marked) ballots, as voters present them over the course of election day(s). In contrast, the high-speed central-count scanners attached to the Capture application must be set to scan either a batch of hand-marked ballots or a batch of PVR ballots. If a PVR ballot is found within a batch of hand-marked ballots, or vice versa, the exceptional ballot is treated as unrecognizable and rejected. The high-speed scanner does not stop, and does not physically separate the rejected ballot from the stack, but continues scanning the whole batch, and then generates a warning message and a report regarding the untallied ballots.

In normal circumstances, this is not a problem. The principal use of central-count scanners is to count absentee ballots, which will all be hand-marked. But there are two circumstances in which one might expect a mix of hand-marked and PVR ballots:

- Scanning emergency ballots. If, during election day(s), at some polling places the polling-place optical scanners fail to operate, pollworkers instruct voters to mark their hand-marked ballots as usual, and insert those ballots into the emergency slot of the Vault scanner's ballot box.[12] At the end of an election day, according to Texas procedures, those ballots would be put in a separate sealed ballot bag and conveyed to the election office where they would be scanned and counted by the central-count

[11] This barcode, which includes the election number and the ballot style (i.e., precinct number) is not a risk in the sense of "barcode ballots" because this barcode does not contain any votes. See, Barcodes on paper ballots: the good, the bad, and the stealth, by Andrew Appel, April 2024. https://blog.citp.princeton.edu/2024/04/10/barcodes-on-paper-ballots-the-good-the-bad-and-the-stealth/

[12] Such occurrences do happen. In New York City 2018, heavy rain caused extreme humidity in many polling places, which in turn caused the paper to jam in the optical scanners. https://www.nytimes.com/2018/11/06/nyregion/nyc-voting-machines.html
The emergency-ballot-box-slot procedure was deployed. In Mercer County NJ 2022, a misconfiguration of the ballot-definition barcodes caused every precinct scanner in the county to fail to read the ballots, and the emergency slot procedure was deployed. https://blog.citp.princeton.edu/2022/12/01/why-the-voting-machines-failed-in-mercer-county/
In both of these cases, the ballots in the emergency ballot boxes were later scanned and counted, in a way that did not significantly delay the certification of election results.

optical scanners. But any such batch of ballots would have both hand-marked ballots and PVR ballots from Flex devices in the polling place.

- Polling places without scanners. It would be entirely feasible for a county to operate the Verity Vanguard system without any Vault polling place scanners at all. Voters would be provided with preprinted hand-markable paper ballots; they would mark these ballots and deposit them into old-fashioned ballot boxes. One BMD (such as a Flex device) would be needed in each polling place to accommodate voters with disabilities. Ballots would be conveyed to the election office for central-count optical scanning. The batch of ballots would contain both hand-marked and PVR ballots.

In these circumstances, it is inconvenient that the Capture application on the Verity Vanguard workstation cannot tally a mixed batch of ballots. To count the ballots correctly will require careful handling by the election-office staff. The Director of Elections should clearly document the procedure so that county election administrators can properly train their staff.[13] The procedure should be as follows:

> Use the Capture application to scan the batch of ballots through the high-speed optical scanner, in "hand-marked ballot" mode. At the conclusion of the scan, you may get a dialog box informing you that some sheets could not be scanned and have been "rejected." Click on "view rejected images" and note the ones that look like PVR ballots. Find those PVR ballots in the pile of paper that has run through the scanner and remove them from the pile. Scan these as a separate batch so that their votes can be tallied. Ideally, combine the two batches together for reporting purposes, otherwise the secrecy/privacy of the PVR ballots will be compromised, if there are just a few of them.

9 Security architecture of polling-place devices

In this section I will describe the "security architecture" of Verity Vanguard polling-place devices.[14] In a later section I will evaluate whether this design provides effective security.

---

[13] Page 38-39 of Hart's *Vanguard Capture User Guide* gives an incomplete description of how to handle "rejected images" and does not cover the case that the rejected image is a PVR file. Hart should update its manual. Until Hart updates the manual, I would find the Hart system sufficient for certification in Texas provided that this addendum to the instructions is provided to jurisdictions by the Director of Elections.

[14] I wrote this description of the security architecture based on the Technical Documentation Package provided by Hart and by interviewing Hart engineers during the 3-day examination meeting. During the meeting I read this back to all the Hart engineers, sentence by sentence, to confirm that this is an accurate description of their claim about how the system works. For those portions of the security architecture that are clearly documented in Hart's Technical Documentation Package, the EAC-certified VSTL has had the opportunity to verify that the system complies with the documentation. For those parts of the security architecture that are not as clearly documented in the TDP, I have no independent means of verifying that this how the system works, but I have no reason to doubt that this is the way they believe their system works.

Verity Vanguard devices use a custom motherboard designed for the voting application, with an Intel Atom CPU from Intel's year-2021 generation of processors. The same basic motherboard circuit design is used on all devices (Vault, Flex, Boost, Adapt) but the form factor varies as necessary to fit it into the device's cabinet. The motherboard does not contain a radio of any kind (WiFi, cellular, Bluetooth, or other)[15] and does not have any network ports, nor a NIC (network interface controller). There are three USB ports, accessible through the vDrive compartment, and one CFAST removable media port, accessible through the CFAST compartment.

The BIOS firmware is a custom BIOS (as would be needed for a custom motherboard).

Before starting the BIOS, the Intel BootGuard validates the BIOS—that is, checks that the BIOS is digitally signed by Hart.

One cannot boot directly into a BIOS menu by pressing a button (as one can on some desktop PCs).

[redacted]

In normal operation, [redacted] there are five partitions on the CFAST card: bootloader partition, EFI partition, operating-system (OS) partition, application partition, and data partition. The first four of those partitions are static, that is, never written to during operation and expected to be unchanged from one boot to the next. The data partition stores election-specific data such as election definitions and CVR files, and does change from one boot to the next.

In normal operation, the Windows operating system does write to the operating system partition and the EFI partition. To ensure that the four static partitions on the CFAST card are never written to, the "Unified Write Filter" (UWF) of Microsoft Windows is used. UWF uses virtual memory to intercept and redirect writes to a UWF-protected partition.[18]

[15] The Examiners were not able to open up the machines to inspect the motherboards, but the VSTL report clearly states, "*The system was examined to verify that no wireless capability is available.*" (Voting System Test Report HIN-23003-TR-04, Hart InterCivic Verity Vanguard 1.0 Voting System, by SLI Compliance, June 17, 2025, page 37)

[redacted]

[17] This is another important and necessary security feature.

[18] https://learn.microsoft.com/en-us/windows/configuration/unified-write-filter/

When the BIOS starts, it checks that the BIOS version is the same as the last boot, by checking a cryptographic hash stored in BIOS memory. That is, although the BootGuard (which has already performed its check) is willing to accept *any* Hart-signed BIOS, this check ensures that the BIOS is the *current* Hart-signed BIOS version.

The BIOS checks before booting, by means of digital signatures, that the CFAST card's bootloader partition, OS partitions, and EFI partition are unchanged since last boot. Then it starts a conventional Secure Boot process (for Intel/Microsoft systems, using UEFI) using the bootloader, OS, and EFI partitions. The OS is Windows 10 LTSC (long-term servicing channel), a version of Windows 10 meant for embedded devices, which Microsoft guarantees to support for 10 years.[19]

Once the OS starts running, a "Trellix application control" driver[20] within the OS validates all executables on the OS partition and the application partition, to make sure (by means of digital signatures) that they have not changed since last boot.

All partitions on the CFAST card *except* the application partition are encrypted by BitLocker.[21] In the system install process, performed by Hart upon delivery of the equipment to a jurisdiction, or upon system upgrade, the system images (of OS partition, application partition, etc.) are on the CFAST card as unencrypted FFU (Full Flash Update) files. The hashes of these FFU files can be checked against reference hashes provided by the U.S. Election Assistance Commission (EAC). As part of system install, the system enables BitLocker for all but the application partition; that is, the TPM encrypts the entire partition. BitLocker generates a 48-digit custom recovery key; this is the same image and the same key for all devices; this key is kept in a safe at Hart.

The application partition is not BitLocker-encrypted, because that would interfere with the ability to do external hash-validation of the application software. Instead, the application partition is encrypted by EFS (Encrypted File System, a standard feature of Windows) running in the Windows 10 OS. The application partition is encrypted by the same key on every Vanguard device (such as Vault, Boost, etc.), and by this means the partition has the same hash value on each device, which facilitates hash validation.

After the OS boots, it runs the application software in kiosk mode. One cannot boot the OS into the standard Windows desktop, and in fact the Windows desktop is not even present in the OS partition (or any partition).

---

[19] https://techcommunity.microsoft.com/blog/windows-itpro-blog/ltsc-what-is-it-and-when-should-it-be-used/293181

[20] https://www.trellix.com/products/trellix-application-control/

[21] https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/BitLocker/

Two methods are provided to do external hash validation. The System Validation Tool is application software that resides in the application partition of the CFAST card. It can be run from a menu on the screen of the device. This tool creates a cryptographic hash of the application partition, and writes it to a USB drive. The “Manual method” does not use the System Validation Tool; in this method, one removes the CFAST card from its port and inserts it into a CFAST reader attached to a Linux computer. From there, one can read and hash all of the partitions—in particular, the application partition.

Two sets of digital certificates are used.

1. The "Certificate Set" or "System Certificates" are semipermanently installed on the device by Hart. At the request of the jurisdiction, Hart will install a fresh set of system certificates. A primary use of these certificates is to check the authenticity of ballot definitions and other data conveyed from workstations to voting machines on vDrives, and election-specific certificates conveyed on Verity Key devices, to make sure they have been signed by the Verity Vanguard Workstations. All devices and workstations within a jurisdiction have the same Certificate Set.

2. For each election, a set of “election certificates” (that is, cryptographic keys) is generated. These are generated on the workstations and conveyed to the devices via the Verity Key USB devices, usually at the same time the election definitions are conveyed to the devices by the vDrive USB devices. The key material in the election certificates is used by the voting machines to digitally sign election results such as CVR files.

If "election certificate" keys were to leak, that would pose the risk that an attacker could create fraudulent CVR files signed by the election certificates. In a large county there might be hundreds of voting machines (Vault optical scanners, Flex ballot marking devices, etc.) geographically distributed during an election. During the entire election period, vDrives stay installed in the USB slots of these devices, one per device. If the election certificates were conveyed to the devices via the vDrives, there would be a risk that the election certificates could leak into unauthorized hands by "borrowing" a vDrive from one of the machines.[22]

To significantly reduce the risk that an election certificate might leak via vDrives, they are not conveyed via the vDrives at all. Instead, a separate USB device is used, the Verity Key. The workstation writes election certificates to the Verity Key, which is not simply a USB memory stick but also has password protection and other active security measures. Election certificates on the Verity Key are encrypted and authenticated using the System Certificates.

[22] It's not quite that simple; there are seals, locks and alarms to be defeated, but even so there would be a risk.

Furthermore, the Verity Key is not left in the voting machines during the election, but is removed from the devices as soon as the key material has been transferred to them. The device cannot be closed and prepared for shipment to polling places until the Verity Key has been removed, in part because the Verity Key is longer than a normal USB stick and the lockable door covering the device's USB slots cannot be closed if the Verity Key is left in one of the slots.

Consequently, even a large jurisdiction's voting machine warehouse would need only a few Verity Keys for use by employees transferring election certificates to voting machines, and the Verity Keys never need to leave that warehouse.

Election definitions are conveyed from the Verity Vanguard Workstations to the Verity Devices (Vault, Boost, Flex, etc.) via the vDrive. The vDrive is a standard USB memory stick, but of a high standard of durability and reliability. Every device gets a vDrive, containing an identical copy of the election definition, inserted into a USB slot in the device's vDrive compartment, where it stays until the polls are closed. The device makes use of the part of the election definition corresponding to its proper polling place; the device is informed of its polling-place number during the setup, after the vDrive is inserted, by the election worker in the warehouse, before shipment to the polling place. The election definition is cryptographically authenticated using the System Certificate key; the polling place device checks the authentication before continuing with election functions. There is no need to encrypt the contents of the vDrive because material such as the election definition contains no secrets. That is, the names of contests and candidates in the election are already public information. This means that a vDrive can be read on any standard computer with a USB port.

When the Vault polling-place scanner writes election results (such as CVR files) to the vDrive, it digitally signs them with the Election Certificate key.

9.1 Use of a memory-safe programming language

The Verity Vanguard applications, on the Devices (Vault, Flex, Boost, etc.) and on the Workstations (Define, Deploy, Capture, Results, etc.) are programmed in the C# programming language in the Microsoft .net framework. C#, and .net generally, is a memory-safe language. This design decision significantly reduces the risk of a major class of security vulnerabilities, compared to other widely used programming languages such as C or C++.[23] This choice of programming language is in line with security recommendations

[23] A 2025 report from the National Security Agency and the Cybersecurity and Infrastructure Security Agency entitled "Memory Safe Languages: Reducing Vulnerabilities in Modern Software Development" https://media.defense.gov/2025/Jun/23/2003742198/-1/-1/0/CSI_MEMORY_SAFE_LANGUAGES_REDUCING_VULNERABILITIES_IN_MODERN_SOFTWARE_DEVELOPMENT.PDF
starts out with this paragraph:

from the National Security Agency (NSA), from DoD's Defense Information Security Agency (DISA), and from the DHS's Cybersecurity and Infrastructure Security Agency (CISA). Memory-safe programming is not a panacea—a voting machine made by another vendor using a memory-safe language still had significant security vulnerabilities—but it is a "best practice."

10 Security architecture of Verity Vanguard Workstations

Each Verity Vanguard Workstation is a commercial off-the-shelf (COTS) desktop server computer, configured for the Verity Vanguard setup. There are two versions of this server: a "legacy" server with a slightly slower CPU and a significantly slower hard drive (rotating disk), and a "new" server with a faster CPU and a much faster hard drive (solid-state disk). The "legacy" server is not offered for sale, but jurisdictions that already own a previous Hart voting system can upgrade without having to purchase new Workstation hardware.

The hardware configuration includes one or more Ethernet ports. If more than one Ethernet port, all ports but one are physically blocked by a cover that cannot be removed without opening the cabinet, *and* the operating system is configured to ignore that port.[24]

The hardware configuration contains no radios (such as WiFi, cellular, or Bluetooth).

The CPU is an Intel processor running Windows 10 LTSC[25]. The system normally boots into kiosk mode, i.e., running the Verity Vanguard application rather than the Windows Desktop. One can instead boot into the Windows Desktop, but almost all applications have been removed from the Desktop (and the operating system) so there is not much one can do there.

> "Memory safe languages (MSLs) are gaining momentum. In 2022, the National Security Agency (NSA) released a cybersecurity information sheet (CSI), "Software Memory Safety." [1] In 2023, the Cybersecurity and Infrastructure Security Agency (CISA) published the joint guide, "The Case for Memory Safe Roadmaps," [2] and in 2024, the White House issued "Back to the Building Blocks: A Path Toward Secure and Measurable Software." [3] Though these each address the problem of memory-unsafe code from a different perspective, they all agree that adopting MSLs is a key part to decreasing vulnerabilities and reducing the risk of security incidents."

and it concludes,

> "Memory vulnerabilities pose serious risks to national security and critical infrastructure. MSLs offer the most comprehensive mitigation against this pervasive and dangerous class of vulnerability. Adopting MSLs can accelerate modern software development and enhance security by eliminating these vulnerabilities at their root. Strategic MSL adoption is an investment in a secure software future. By defining memory safety roadmaps and leading the adoption of best practices, organizations can significantly improve software resilience and help ensure a safer digital landscape."

[24] Ideally there should be only one port, but it is difficult to find commercial network interface cards that have only one port.

[25] https://techcommunity.microsoft.com/blog/windows-itpro-blog/ltsc-what-is-it-and-when-should-it-be-used/293181

Hart configures Windows 10 in a "hardened" configuration in which all unnecessary applications and drivers are removed, all unused ports are closed, all Windows Firewall rules are removed (thus permitting no access) except the client-server connection described below, and so on. This hardening follows the Department of Defense's "Microsoft Windows 10 Security Technical Implementation Guide [STIG]."

Intel AMT, "Active Management Technology", is disabled on the Verity Vanguard Workstations.[26] Intel ME, "Management Engine", is also disabled.

The Verity Vanguard Workstation can be configured in single-workstation mode or in client-server mode. In client-server mode, one workstation is the server, containing the election database, and the other workstations are clients, running the user interface. Depending on the configuration, the user interface may also run on the server machine. The clients are connected to the server by a local Ethernet. That is, there is a single "dumb" Ethernet switch; there is an Ethernet cable from each workstation (including the server) to the switch. In client-server mode, the workstations use the System Certificates to authenticate each other.

Other than the Ethernet port(s), the only other ports on the server cabinet are USB. The only USB devices to which the operating system will respond are those on an "allow list." The "allow list" will generally include Hart vDrives as well as any USB devices (such as backup thumbdrives) that a System Administrator specifically adds to the allow list via a Verity Vanguard application.

The hard drive is BitLocker-encrypted, managed by the TPM. The standard procedures (on Intel/Windows computers) of Secure Boot and UEFI are used.

These measures are intended to (among other things):

1. Prevent the Election Management System (EMS) from being connected to the Internet (or any network other than the EMS's internal Ethernet);
2. Prevent anyone from directly accessing the underlying election database except through the Verity Vanguard applications.

A System Administrator can use the "Vanguard Users" application to add and manage users of the software (that is, election office staff) and give them specific privileges using role-based access control (RBAC) or in a fine-grained manner. Each user must have a hardware security token (that plugs into USB) as well as a password.

[26] "Platforms equipped with Intel AMT can be managed remotely, regardless of its power state or if it has a functioning OS or not." (https://www.intel.com/content/www/us/en/developer/articles/guide/getting-started-with-active-management-technology.html).

[redacted]

11 Assessment of the security architecture

Overall (with minor exceptions) I would say that the Verity Vanguard system has a "state-of-the-art" security architecture for consumer-grade devices. That does not mean it is perfectly secure, but it is as secure as it is practical to make such a system. By "state of the art" I mean that Hart is generally following standard best practices. Because they are (generally) standard, that means it is easier to assess the level of security they provide, both for VSTLs and for independent examiners.

Furthermore, the "state of the art" has advanced since the early 2000s when previous generations of voting machines were designed and deployed. Voting machines of that generation (two generations ago) were notoriously insecure: it was trivial to install fraudulent vote-stealing software on them even without physical access. Election management systems (EMSs) of that generation were also insecure: it was trivial to access and modify the underlying database without going through the official application program. Hacking the Hart Verity Vanguard system should be much more difficult.

But "much more difficult" does not mean "impossible." As required by the VVSG 2.0, Hart has provided in its Technical Documentation Package (TDP) a "Risk and Threat Assessment" listing all the ways they can think of that something could go wrong, and for each of those, a severity "Impact" and a "Rarity". Overall the risk assessment has been done well and (I believe) in good faith, but it is incomplete in some important ways.

Example 1: [redacted]

On the other hand, a different line of the risk assessment table reads, "A programming error in the operating system, system executables, or third-party applications causes data at rest

[27] *See* Vanguard 1.0 System Administrator's Guide, page 46.

[28] Such attacks would still (likely) require [redacted] This underscores the importance of following the instructions in the Vanguard 1.0 System Administrator's Guide, page 102: "Vanguard workstations should be secured in a locked area with appropriate physical security controls in place. Access to Vanguard workstation components must be restricted to authorized personnel at all times. In addition, the following physical security controls may be followed for all workstations . . ."

[redacted]

Let me give a concrete example of such a scenario. An important (and useful) protection mechanism in the Verity Vanguard security architecture is the [redacted] From time to time, "white hat" researchers find security vulnerabilities in [redacted] as described in the National Vulnerability Database (NVD) of the National Institute of Standards and Technology (NIST):

- [redacted]: CVE-[redacted]
- [redacted]: CVE-[redacted]
- [redacted]: CVE-[redacted]
- [redacted]: CVE-[redacted]
- . . . and others from earlier years.

Every year, several security vulnerabilities are discovered [redacted] gives the attacker the ability to forge fraudulent CVR files not only for this machine's polling place but for all polling places in the entire county.

Either the attacker can replace the seal without visible evidence of tampering, or not. Perhaps it is noticed that one voting machine's seal is broken. That is unlikely to cause the county to suspend the use of voting machines in this election and count all the ballots by hand. (And if that were the response to a missing seal, then an extremely low-tech attacker could just snip the seals on some voting machines to cause panic.)

This [redacted] vulnerability *by itself* does not necessarily enable election theft, because there are other protections built into the Verity Vanguard system. However, in recent years

we frequently see exploits that string together a chain of vulnerabilities. Thus, I do not consider it far-fetched or extreme to say that it could be feasible for a sophisticated actor to hack a Verity Vanguard voting system, even without insider access, and thereby commit large-scale election fraud.

Example 2. A person with physical access to the Workstation, even if they don't have a password or security token, could [redacted] This attack does not rely on any specific new [redacted] vulnerability being discovered.

Example 3. With extreme insider access, such as key positions within Hart Intercivic, it would be much easier to commit catastrophic fraud. Hart straightforwardly admits this in their "Risk and Threat Assessment." It is good that they acknowledge this. Hart is a reputable company and there is no reason to suspect them of malicious activity. But one way or another, whether from outsiders or insiders, it could be possible that Verity Vanguard could be severely hacked.

11.1 One aspect of the security architecture that is not state-of-the-art

The way that cryptographic keys (System Certificates and Election Certificates) are managed, distributed, and stored does not comport with well-known best security practices. Instead of having a single set of Election Certificates for all devices, "best practice" for public-key digital-signatures would be to generate the signing key (for signing CVR-file election results) within the TPM of the device, such that the private key never leaves the TPM. If that were done, then even if the attacker could defeat BitLocker and read the entire CFAST card, they still couldn't fake a digital signature on a CVR file. That best practice would require every polling-place device to have its own separate signing key, and it would require a secure method to communicate the *public key* of the device back to the Verity Vanguard Workstation. Likely this could be done using the Verity Key hardware. Similar considerations apply to the System Certificates.

11.2 Conclusion of Security Architecture Assessment

The security architecture of the Verity Vanguard system is adequate. It is near state-of-the-art even if it is not 100% state-of-the-art in every respect. It is not possible to make a voting machine that is perfectly secure, even with state-of-the-art best practices. Therefore, we must conduct elections with sufficient auditing of paper ballots to guarantee correct outcomes even in case the voting machines might be hacked.

12 Recommendations in light of imperfect cybersecurity

The cybersecurity architecture of Verity Vanguard Workstations and Verity Vanguard Devices is good but not perfect. It is not likely that perfect cybersecurity can be achieved.

Therefore I recommend that jurisdictions using Verity Vanguard (or any other Election Management System and voting machines) employ the following audit practices:

1. Canvass election results from printed poll tapes! Each Vault optical scanner prints out a "cash-register tape" with the number of votes each candidate received in each precinct covered by that polling location. To defend against the possibility that the EMS (that is, Vanguard Results application on the Workstation) is incorrectly recording or aggregating votes uploaded from vDrive, election officials should compare these uploaded results, precinct by precinct, with the physical printed poll tapes. This can be done after announcement of preliminary (election-night) results and before certification of results.
2. To defend against the possibility that the Vanguard Results app is incorrectly adding up all the precincts, after checking each individual precinct total against the printed polltapes, add them all up independently of Vanguard Results, such as in a spreadsheet on another computer. Ideally, that separate spreadsheet is the one against which printed poll tapes are compared.
3. Before the election, review each ballot style of preprinted hand-markable paper ballots *(on the paper, not just on the screen)* to ensure it has the right contests and candidates. If this is done, then no matter what cybersecurity breaches might occur, a hand recount of the hand-marked paper ballots can get an accurate result. (On the other hand, if voters are given ballots with the wrong candidates or contests on them, a recount cannot correct the problem.)
4. During the election, review (or at least spot-check) Ballot-on-Demand ballots as they are handed to the voters to be marked. This protects against the possibility that the BoD system gives voters the wrong ballot styles, or the supposedly right ballot styles but with incorrect lists of candidates or contests. To perform this review or spot-check, the pollworker needs one good copy (it may be marked "VOID") of each ballot style as a reference, and a printed pollbook mapping voter addresses to ballot styles.
5. Limit the use of BMDs (such as Flex or Adapt) to those voters who cannot mark a paper ballot by hand. The ballot-style spot-checks described above cannot be performed on ballots (PVRs) printed by BMDs, as those ballots already have votes printed on them and it would compromise voter privacy.
6. Canvassing from printed poll tapes can help defend against errors or cyberfraud in the EMS, but cannot defend against errors or cyberfraud in the optical scanner itself. The first line of defense is, of course, the cybersecurity architecture of the Verity Vanguard system. However, the ultimate defense must be Risk-Limiting Audits (RLAs), which can check what votes are on the paper ballots without relying on the say-so of the computer software in the Devices or Workstations.
7. Each jurisdiction using Verity Vanguard should *absolutely* install its own "Workstation Certificate Sets", using the procedure described on page 107 of the

Vanguard 1.0 System Administrator's guide. The reason for this is that if some *other* jurisdiction fails to adequately protect the physical security of its workstations,[29] and in that *other* jurisdiction some attacker steals a copy of the Certificate Set, surely *your* jurisdiction shouldn't be using the same Certificate Set!

8. Needless to say (since it already says so in the System Administrator's Guide), the instructions on page 102 regarding physical security of the Workstations should be taken seriously.

13 Which method to use for hash validation?

Hash Validation is a means of answering the question, "is the legitimate, certified software currently installed in the voting system?"

Hart provides two methods of doing hash validation:

- "Using the System Validation Tool to generate hashes of the encrypted system files."
- "Retrieving copies of the unencrypted software files manually and then hashing those files manually." [30]

Which of these methods should a jurisdiction use? The Hart manual says "it is important for our users to understand that there are tradeoffs" but presents only a one-sided view of the tradeoff. Here I will explain both sides.

Summary: In my opinion, the "System Validation Tool" method is adequate to detect *inadvertent, nonmalicious* installation of a wrong application software version, but does nothing to detect changes to the OS, and in general does not provide much more protection against malicious (i.e., vote-stealing) hacking than the other defenses already built in to the voting machines. The "Manual" method provides stronger assurance against fraudulent modification of the application partition or the OS partition.

Longer explanation: The purpose of "hash validation", of a voting machine, is to provide some assurance that the expected software program is loaded into the computer. If an attacker has installed a fraudulent vote-counting program (on an optical scanner) or vote-marking program (on a ballot-marking device), then he could shift any desired fraction of the votes from one candidate to another, in ways that LAT (logic and accuracy testing) could not detect. Or, an inadvertent (nonmalicious) misconfiguration could have the wrong version of software installed, leading to (inadvertent) inaccuracy of vote-counting or vote-marking.

[29] Vanguard 1.0 System Administrator's Guide, page 102.
[30] Hart Document Number 1000828, Vanguard Manual Application Hash Validation, 2024; page 4.

Almost all of the software[31] on a Vanguard device (e.g., Vault optical scanner) is kept on the CFAST card, a removable media. This card has several partitions.

- One partition contains the bootstrap loader, whose job is to load and start the operating system (OS).
- One partition contains the OS.
- One partition contains the application software, which performs functions such as optical scanning and vote counting.
- There is also an EFI partition, which I will not describe further.
- The data partition contains information that is expected to change, such as election definition and cast-vote records, and is outside the scope of hash validation.

In addition to software on the CFAST card, there is a flash memory on the motherboard containing the BIOS, whose job is to load and start the bootloader.

A sophisticated software attack could corrupt the voting machine (to steal votes) by modifying the application software. Such attacks can be detected by the Manual method but cannot be reliably detected by the System Validation Tool method, because such an attack could modify the System Validation Tool itself to report fraudulent hash codes.

Thus, there is a trade-off. The Hart manual provides one side of this trade-off: that is, the manual method exposes the CFAST card to unintentional or intentional corruption,[32] it requires removing, logging, and replacing the security seal; overall this method is more labor-intensive than using the System Validation Tool. The other side of the trade-off is that manual method achieves more protection against certain kinds of attacks.

Hash Validation of the Operating System. A *more* sophisticated attack could leave the application software unchanged, but modify the OS so that, while the application software is running, its operation is altered to steal votes. Neither the System Validation Tool nor the Manual method can detect this attack, but a simple extension of the Manual method can do so. That is: hash all the static partitions (OS, bootloader, EFI) of the CFAST card as well as the application partition. One complication with this method is that, since those three partitions are encrypted by BitLocker, their expected hash will be different on each device

[31] Other than the BIOS and firmware built into system-on-chip devices such as USB.

[32] The Hart manual also points out that it exposes the CFAST card to unauthorized copying. With a copy of the vote-counting software, an attacker could reverse-engineer it as part of a scheme to devise fraudulent vote-stealing software to install on any Hart Verity Vanguard voting machine. In my opinion, neither Hart nor a jurisdiction should rely on the secrecy of this software. Any software that is installed on tens of thousands of voting machines across many jurisdictions, accessible on any of those machines by clipping a security seal, cannot be assumed secret. If secure elections are achieved using voting machines, it can and must be for other reasons than the assumption that no copy of the software has ever leaked.

(since each device will have a different BitLocker encryption key). I have explained this "Extended Manual method" to Secretary of State staff.

No hash validation of the BIOS. An *extremely* sophisticated attack could modify the BIOS so that, as it loads the bootloader, it modifies the bootloader to modify the operating system, as loaded. No hash validation methods can detect such attacks. This attack would be difficult for an attacker to devise. The best defense against this kind of attack would be a good program of risk-limiting audits (RLAs).

Built-in automatic hash validation. Verity Vanguard devices do internal hash validation every time they are booted up. That is, the BIOS firmware compares the hashes of certain CFAST partitions (bootloader, EFI, OS) to their hash value at the last boot. This BIOS firmware is better-protected (by Intel's UEFI architecture) than the CFAST partitions, so it really is meaningful to have the BIOS do this hash-check. Then, the OS does hash validation of the CFAST application partition.

Therefore, it would be reasonable to use a combination of methods for hash validation:

1. For all voting machines on every boot-up, perform automatic hash-validation of all static partitions. The Verity Vanguard system does this anyway. This provides meaningful detection if the BIOS has not been maliciously hacked. If somehow the BIOS were maliciously hacked (which would be quite difficult but not theoretically impossible for an outsider, but not so difficult for a Hart insider), or if there were a bug in Hart's implementation of this method, this test might be meaningless.
2. For some fraction of voting machines in every election, use the System Validation Tool. This provides protection against inadvertent installation of the wrong version of the application software. It cannot reliably detect installation of the wrong OS software, or against malicious hacking of the application software, OS, or BIOS.
3. For some fraction of the voting machines on a regular basis (either in every election or every two years), use the Manual hash validation method to check the application partition. This can reliably detect installation of the wrong application software. However, if the BIOS and OS are not hacked, the Manual method does not necessarily provide additional protection beyond what Verity Vanguard system does on every boot-up. And if the BIOS and OS are both hacked, then the voting machine could commit election fraud even if the application partition is not modified. Therefore, *if the automatic hash-validation on boot-up works as advertised,* it is not clear that the Manual method adds any value.
4. For some fraction of the voting machines, use the Extended Manual hash validation method to check the OS partition has not been modified since it was first installed. If the BIOS has not been hacked, this check would be redundant. If the BIOS has been hacked, then this extra hash validation check can provide meaningful detection.

I make no specific recommendation about which of these hash methods the State and its subjurisdictions should use, and/or on which fraction of the voting machines. I do recommend that if a validation method is performed on some fraction of the machines, care should be taken to ensure that those machines are chosen *randomly.*

14 Risk-limiting audits and the Verity Vanguard Imprinter

Summary of this section: The Verity Vanguard "Vault" polling-place optical scanner can be equipped with an Imprinter, a device that can aid in doing efficient risk-limiting audits (RLAs) of election outcomes. I have examined this imprinter and found that it works well, it prints legibly, it cannot cause harm by reducing the capacity of the ballot box, and it cannot cause harm by printing illegitimate votes onto the ballot. Because the imprinter is a modular, optional add-on to the Vault scanner, a jurisdiction that chooses not to purchase the Imprinter now can decide in the future to purchase it to make RLAs more efficient. This is a useful feature of the Verity Vanguard voting system.

Although the Verity Vanguard voting system has good cybersecurity protections, those protections are not perfect. It should not be considered impossible that an attacker could replace the software with fraudulent software that deliberately miscounts the votes in favor of one set of candidates. Therefore a jurisdiction must be able to recount *by human inspection* the paper ballots that the voters marked themselves. Because Verity Vanguard is a paper ballot voting system, it satisfies this requirement.

But most jurisdictions don't recount every election. What if a hacked computer shifted 5% of the votes from Smith to Jones, turning a 52-48% victory for Smith into a 47-53% defeat? A six-percent margin of victory would not normally cause a recount.

Therefore many states for a long time have legislated *random audits*. However, the random audits legislated in the 1980s (and still used in some states today) are not very effective. For example, if you randomly select 3% of the polling places and recount the votes just from those polling places, that can sometimes catch fraud (if it's occurring) but it can still miss many polling places where fraud might have occurred. That is, statistically it is not a very effective method.

Since about 2010, much more efficient and effective statistical methods of ballot auditing have been designed:

Risk Limiting Audit (RLA) is any post-election procedure that offers the following statistical guarantee: If the reported electoral outcome is wrong, there is a known, pre-determined minimum chance that the procedure will correct the reported outcome.

For instance, an RLA with a risk limit of 5% has at least a 95% chance of correcting the reported outcome if the reported outcome is wrong (and no chance of altering a correct

reported outcome). This is a much stronger guarantee than the old "3% of the ballot boxes" method could achieve.

An RLA is "any method" that offers that guarantee, and there are several methods of doing an RLA: batch-comparison audits, ballot-polling audits, ballot-comparison audits. A full hand recount is one form of RLA. Some of these methods are more efficient than others, in how much labor it requires by the auditing staff.

Texas Election Code, Section 127.302 requires Risk-Limiting Audits, but the legislature delegated to the Secretary of State the selection of which method to use.

"Ballot polling audits" are reasonably efficient: in a race that's not too close, just sampling a few hundred ballots can confirm that the outcome claimed by the voting machines is correct, even if millions of votes were cast. But in a very close election, with a tiny margin of victory, a ballot-polling audit could require examining (by hand, on paper) many thousands of ballots. In very close elections, or in elections where the total number of votes is small, ballot polling audits may be less efficient than full recounts.

"Ballot comparison audits" are much more efficient, that is, they achieve the same level of assurance (risk limit) by examining vastly fewer ballots. A ballot comparison audit requires that the record of each ballot in the CVR (cast-vote record) file must have a serial number, and the corresponding paper ballot must have the same serial number on it. The voter (and pollworkers) must not be able to see that serial number on the paper, otherwise ballot secrecy/privacy will be lost.[33] The way to get a serial number that the voter cannot see is for the optical scanner to imprint a number onto each ballot as it is being scanned.

Most central-count optical scanners from the major voting-machine vendors have this imprinting component, or can be equipped with it. Some polling-place scanners from some vendors have imprinters.

To be suitable for use in elections, an imprinter must satisfy these criteria:

1. It must print *after* the last time the voter has seen the ballot.
2. It must not be physically capable of printing a vote onto the ballot, *even if the software in the voting machine were to (fraudulently) try to make it do so.* This is normally achieved by making the imprinter a small device that can only print in the margin of the ballot paper.
3. It must not interfere with other functions of the voting machine, such as by causing paper jams or substantially reducing the capacity of the ballot box.

[33] Texas paper ballots have a serial number printed on them that the voter and pollworker can see. This preprinted serial number should not be included in the CVR file or ballot images, otherwise the privacy of the ballot can be severely compromised. For this reason, the Verity Vanguard system does not include the preprinted ballot number in the CVR file. This is an appropriate design decision.

4. It must be durable and reliable.
5. The serial number it imprints must be readable.
6. Imprinters on polling-place scanners must randomize the order of the numbers they imprint, so that ballots cannot be tracked back to the voter.

I examined the imprinter mechanisms of the Verity Vanguard system, both the Capture central-count scanner and the Vault polling-place scanner. These imprinters satisfy all these criteria, so they are suitable for use in Texas.

The Vault Imprinter is an extra-cost option for the Vault polling-place scanner. A county purchasing the Verity Vanguard system might choose to purchase Vault scanners without imprinters. In a future year, that county might determine that the savings to be obtained by making RLAs more efficient[34] justifies the cost of purchasing the Imprinters, and they can be added on at that time.

If at least one county purchases the system with Imprinters, that will give the Secretary of State's RLA team the opportunity to test the ballot-comparison audit method in pilot RLAs.

15 "Boost" device

One component Verity Vanguard system is called "Boost." This device, operated by the pollworker in the presence of the voter, can serve two functions:

- It can print a hand-markable paper ballot in the correct ballot style for the voter's precinct or voting district; that is, it is a ballot-on-demand (BOD) system.
- It can print a ticket for the voter to insert in a Flex BMD, that will call up the right ballot style for that voter to mark on the touchscreen (or via ATI). The Flex will cancel that ticket before starting the vote-marking session, so it cannot be inadvertently or fraudulently reused to make more than one ballot.

Boost is an optional component, meaning that a county can run elections with it or without it. Without Boost, a polling place can be provisioned with preprinted hand-markable paper ballots in all the required ballot styles. Without Boost, when a voter uses the Flex BMD a pollworker can first enable the Flex by entering on the touchscreen the correct ballot-style number.

The Boost device appears to work well for its intended purposes and is adequately secure. It is sufficient for use in Texas elections. The Verity Vanguard system without Boost is also sufficient, in some election configurations.

[34] Providing, of course, that the Secretary of State selects Ballot-Comparison Audits as a permissible method.

The Boost is not an e-pollbook. It does not have a register of voters, it does not record which voters it has issued tickets or ballots for, and it does not know the name of the voters for whom it is issuing tickets or ballots. Boost can be used with or without e-pollbooks, and e-pollbooks can be used with or without Boost.

16 Advisability of limiting the use of ballot-marking devices

Verity Vanguard allows for different kinds of paper ballots in the polling place:

- Hand-marked paper ballots, marked by the voter with a pen.
- BMD-marked paper ballots, printed by a "Flex" or "Adapt" computer ballot-marking device after the voter interacts via a touch-screen or audio-tactile interface (ATI). Hart calls these ballots PVRs, "printed vote records".

Both kinds of ballots are scanned by the same optical scanners (Vault scanners in the polling place or Capture scanners in the election office).

When voters mark paper ballots by means of a computerized touchscreen or audio interface (a *ballot-marking device, BMD)*, there is a risk that the computer, if it had been fraudulently programmed by an attacker, could mark different votes onto the paper than the voter chose (and reviewed) on the touchscreen.

One might think that voters have the opportunity to see what's on their paper ballot before it is scanned, so it is a *voter-verifiable paper ballot.* That is true. But study after study has shown, unfortunately, that the vast majority of voters who use BMDs *do not* inspect their ballots carefully (or at all) before it goes into the scanner. Therefore, if the BMD were hacked (or malfunctions) in some way that the votes it prints onto the paper are different than the votes they chose (and reviewed) on the touchscreen, most voters wouldn't notice. Those erroneous or fraudulent votes would be counted, and in a recount they would be recounted erroneously or fraudulently because they are printed on the paper ballot.

This is a severe disadvantage of ballot-marking devices, and for that reason, it is the consensus of election cybersecurity experts[35] that the use of BMDs should be limited to those voters with disabilities who cannot mark a paper ballot by hand.[36]

Therefore I recommend that counties that purchase the Verity Vanguard system do so in a configuration with hand-marked paper ballots in the polling place for those voters who can

[35] See also: Ballot Marking Devices Cannot Ensure the Will of the Voters, by Andrew W. Appel, Richard A. DeMillo, and Philip B. Stark, *Election Law Journal* Volume 19, Number 3, pages 432-450, 2020.
[36] BMDs are an imperfect solution even for voters with disabilities, but it must be provided as an option.

mark a paper ballot by hand, and a Flex BMD in each polling place for voters who need an assistive technology.

17 Tamper-evident seals on Hart Verity Vanguard devices

As part of an effective seal-use protocol for Hart Verity Vanguard voting devices, election workers must check that seals haven't been tampered with. To do that, they should remove the clear plastic cover over the CFAST card seal, physically pull on the seal, and inspect both sides of the seal. If you leave the clear cover on over the seal and just look at the number, you cannot fully check that the seal hasn't been tampered with. A similar consideration applies to the seal on the Verity Vanguard Workstation.

Now, the long explanation: An important purpose of tamper-evident seals on these voting machines is to help assure that the vote-counting software or the election-definition file has not been replaced with fraudulent files. There are at least two seals on Verity Vanguard devices such as the Vault (precinct-count optical scan) and Flex (ballot-marking device). If these seals are used and checked properly, they can provide real security benefits—providing improved assurance to election officials and to the public that the legitimate vote-counting (or vote-marking) software is working as intended. On the other hand, ill-informed or sloppy procedures will render the seals useless as a safeguard.

The procedures that a jurisdiction uses, governing the installation, logging, checking, and reporting of seals, form a *seal use protocol.*[37] Those protocols are described, for example, in my paper "Security Seals on Voting Machines: A Case Study"[38]. Here I will point out some issues specific to the Hart Verity Vanguard equipment.

The seal covering the CFAST card guards the "crown jewels" of the equipment. That is, the CFAST card has the software that counts votes—that interprets the marks on the paper (in the Vault precinct-count optical scanner) or interprets the voter's touch-screen input and makes marks on the ballot paper (in the Flex or Adapt ballot-marking device). If an

[37] "Seal use protocols are the formal and informal procedures for choosing, procuring, transporting, storing, securing, assigning, installing, inspecting, removing, and destroying seals. Other components of a seal use protocol include procedures for securely keeping track of seal serial numbers, and the training provided to seal installers and inspectors. The procedures for how to inspect the object or container onto which seals are applied is another aspect of a seal use protocol. Seals and a tamper-detection program are no better than the seal use protocols that are in place." From section 24 of "Insecurity of New Jersey's seal protocols for voting machines", by Roger G. Johnston, 2010.
http://www.cs.princeton.edu/~appel/voting/Johnston-AnalysisOfNJSeals.pdf

[38] A. W. Appel, Security Seals on Voting Machines: A Case Study, *ACM Transactions on Information and System Security,* volume 14, no. 2, article 18, 2012. http://doi.acm.org/10.1145/2019599.2019603

attacker were to replace the CFAST card with one containing fraudulent software, that fraudulent software (on Vault) could deliberately misinterpret (that is, lie about the contents of) some fraction of the ballots, shifting an arbitrary percentage of votes from one candidate to another. (Or, on Flex or Adapt, mark the paper ballot with votes different from the ones the voter indicated on the touch-screen or other input device.)

There are several cybersecurity safeguards built into Verity Vanguard devices, but in case those were somehow defeated, the seal would be an additional layer of defense, *if the seal-use protocol is effective.*

The basics of a seal use protocol would include:

1. At a time when there is reason to believe that the CFAST card contains the expected legitimate software, install the CFAST card in its slot. This "reason to believe" could be obtained by hash-code testing, for example.
2. After installing the CFAST card in its slot, replace the cover and screw it down. Then apply a tamper-evident seal.
3. The seal should be tamper-resistant, in the sense that it's difficult to remove it and replace it without evidence of tampering. This seems obvious and self-evident, but it is surprising how many seals on the market fail this criterion! The seal shown in the Hart manual appears to be ULINE model #S-13699R. From my limited examination, I believe this is a good seal,[39] providing reasonable tamper-evidence *if used properly.*
4. The design of the voting machine should be such that it's impractical for an attacker to bypass the seal (to tamper with the CFAST card or vDrive, or with the CPU) without touching the seal. This might seem obvious, but I have personal experience assessing a previous generation voting machine that fails in this regard. To determine whether the Vanguard devices (Vault, Flex, etc.) are resistant to bypassing, a thorough examination would require disassembling machines in a way that was not practical to do during my on-site exam. In my limited examination, I did not see any bypassing vulnerabilities.
5. The seal should be difficult for an attacker to fake. The U-line seal, with its simple cast metal body and numeric engraving, would not be extremely difficult for an extremely sophisticated attacker to counterfeit; but it might be difficult *enough*, and we cannot and should not expect to rely entirely on the seal for the security of

[39] I have not done a thorough expert examination of this seal. However, the State of California has carefully examined the security and effectiveness of several seals for use on voting machines, in its process for certification of voting machines. The Director of Elections should consider looking up the California reports, to see if this exact model of seal (or some other seal) has been found effective and secure for use on voting machines.

elections. From my experience with similar seals made by other vendors, the U-line seal may be *good enough, if used properly.*

6. If the attacker could obtain a duplicate seal with the same serial number, then he could simply cut the seal and (after compromising the CFAST card) replace it with the duplicate. Therefore, the manufacturer should not allow purchasers of their seals to specify the particular range of serial numbers engraved on the purchased batch. This seems obvious, but in the past there have been seal manufacturers who are too accommodating of custom-numbering requests. Very likely, U-line does things the right way, ensuring that no two seals ever have the same number, but election officials might want to seek assurances on that point directly from U-line.
7. I have personal experience devising attacks on a cable-lock seal similar to this one, as described in my "Security Seals on Voting Machines" paper referenced above. In addition to the attacks described in that paper, I can think of other ways to remove the U-line seal and (after tampering with the CFAST card) replace it. These attacks can be detected by a *sufficiently thorough* inspection of the seal: that is, remove the clear plastic cover over the seal, physically pull on the seal to make sure the cable is not loose, inspect for scratches, glue, and other signs of tampering, and flip the seal over to make sure the other side does not have markings on it. **Therefore, best-practices in seal inspection require removing the plastic cover.**
8. There are many other important components of a seal-use protocol. I have described them elsewhere, as noted above, but I'll mention the key point: The protocol should specify whose responsibility it is to check the seal and at what times the seal should be checked. That person should receive training in seal inspection, to understand some of the ways that seals can be tampered with so they know what to look for.
9. Most critical of all, the protocol should require that if something is wrong with the seal, the seal inspector must report this immediately to the appropriate officials.

Similar considerations apply to the seal that protects the vDrive (the USB thumbdrive that contains the ballot definition file the cast-vote-record results). However, on that seal there is no clear plastic cover, enabling easier access for a physical examination of the seal.

Similar considerations apply to the seal that protects the Workstation from having the computer cabinet case opened.

Without following these basic steps, the tamper-evident seals are mere "security theater", decorations that do not provide significant assurance.

Even with the best practices for seals, there can be ways to fraudulently insert vote-stealing software on these (or any) voting machines. That means that a jurisdiction

using computerized voting machines should rely not only on seals, but use other protections such as recounting or Risk-Limiting Audits of paper ballots.

Conclusion: The design of the Hart Verity Vanguard equipment is such that tamper-evident seals can provide some meaningful assurance, if used and inspected in the right way.

18 Tamper-evident seals on Verity Vanguard Workstations

The Verity Vanguard Workstation is a desktop server computer in a tower-format desktop computer cabinet. Like most desktop computer cabinets, it opens by sliding the side panel (in tower format). Like most desktop computer cabinets, it has a hasp (a steel tab with a hole in it) through which the user can put a padlock or seal to prevent sliding open the side panel.

It would be unwise to allow unauthorized people to tinker with the components inside the cabinet. Therefore Hart applies two tamper-evident seals to the cabinet. A cable seal (the same ULINE seal that is shown in the illustration of the CFAST compartment) is threaded through the hasp. A tape seal, a 1-inch by 5-inch (approximately) [redacted] if this tape is removed, the word "VOID" (or similar) appears in the adhesive visible through the clear tape.

For these seals to provide any protection, they must be logged and periodically inspected as part of a seal use protocol. Most of the same considerations as I described above apply. In inspecting the cable seal through the hasp, the integrity of the hasp must be examined as well as the integrity of the seal itself.

19 The Vault is a tabulating device

Hart's Technical Documentation Package (TDP) states that the Vault polling-place optical scanner is not a tabulating device. It is a tabulating device, and the documentation should say so.

> tab·u·late 'ta-byə-ˌlāt
> *transitive verb*
> 1 : to count, record, or list systematically
> 2 : to put into tabular form *(Merriam-Webster)*

The Vault records ballot images as ballots are scanned in. It stores those ballots as individual CVRs (cast vote records) recording which candidates are voted for. This is tabulation, in the sense of "systematically record."

When the pollworker gives the command to close the polls at the end of election day (or at the end of the last election day in the case of an early in-person voting period), the Vault adds up all the votes for each candidate in the CVRs, and prints those totals on the "results tape" (a roll of thermal cash-register-style paper on the side of the Vault). Adding up these results is tabulation in the sense of "count."

20 Other issues

Verity Vanguard Workstations and polling-place devices have a logging system to keep track of all pollworker interactions and other events. This can be useful in case, for example, a forensic examination needs to be performed. I did not study the logging system or inspect examples of log files. I believe another of the Examiners studied the logging system in detail, and I look forward to reading his report.