Voting System Examination of Hart InterCivic Verity Vanguard 1.0

Brian Mechler, Technical Examiner
Exam Dates: September 16-18, 2025
Report Date: October 25, 2025

1.0 Background

An examination of the Hart InterCivic Verity Vanguard 1.0 voting system was conducted at the Texas Secretary of State Elections Division offices on September 16-18, 2025.

Verity Vanguard 1.0 is a comprehensive voting system, and the first to receive certification from the U.S. Election Assistance Commission (EAC) under version 2.0 of the Voluntary Voting System Guidelines (VVSG) [1]. The scope of certification sought in Texas includes the following components [2]:

- Vanguard Define - A software component used to enter election data.
- Vanguard Deploy - A software component for generating election definitions and associated media.
- Vanguard Capture - A central device used by election officials to scan paper ballots, perform contest resolution, and convert voter selections to electronic Cast Vote Records (CVRs).
- Vanguard Results - A software component used by election officials to tabulate results and generate reports.
- Vanguard Settings - An application which “allows authorized users to manage a very limited set of [workstation] operating system functions” [3].
- Vanguard Users - An application to “enable authorized users to create and manage user accounts within the [Verity Vanguard] system” [3].
- Vanguard Manage - An application that “enables authorized users to add, copy, import, export, archive, restore, and manage elections” [3].
- Vanguard Libraries - An optional feature which gives users the ability to save translations and audio data from prior elections for future use.
- Vanguard Test Decks - An optional feature which can generate a pre-marked set of ballots for Logic and Accuracy (L&A) testing.
- Vanguard Boost - A device used by poll workers to issue ballots in the polling place.
- Vanguard Flex - A voter-facing ballot marking device (BMD).
- Vanguard Vault - A polling place ballot scanning device.
- Vanguard Adapt - A voter-facing device which “enables voters to mark, verify, and cast their ballot, all without touching a piece of paper” [3].

The examination consisted of device and workstation installation from the Trusted Build, configuration and verification of the installed images, vendor presentation, vendor Q&A, accessibility tests, a L&A test, and unscripted interactions with the devices and workstations. I did not participate in the accessibility tests, readers can refer to the legal examiners' reports for more details on compliance with accessibility requirements. In addition to the appointed examiners, representatives from the Texas Secretary of State, the Texas Office of the Attorney General, the EAC, and Hart InterCivic were present throughout the exam.

Verity Vanguard is a completely new product line certified under a new major revision of the VVSG. Thus, there are no changes from prior releases to remark upon. However, many Vanguard components share similar functionality to their counterparts in the Verity 2.x systems. Where appropriate, those associations to prior branding will be made for the benefit of readers with familiarity of the prior product line.

This document will cover observations from the exam. Readers should refer to the EAC Certificate of Conformance [2] for a complete list of configuration options, commercial off-the-shelf (COTS) components, and system limits.

2.0 Verity Vanguard Workspace

The Vanguard Workspace is the the set of all software components that run on the jurisdictions's election management workstations. Workspace applications operate in kiosk mode, meaning the workstations boot up directly into Vanguard Workspace environment. User access to the underlying operating system is significantly limited. Access to the Windows desktop is only granted to users with Administrator privileges, and such access has to be granted by Hart Technical Services with a temporary passcode. Vanguard employs strict application allow-listing; only applications on the allow-list are able to be executed on the workstation. No user installation of software on the workstation is allowed. Hart delivers workstations with the Verity applications pre-installed and pre-configured to operate in kiosk mode [3].

2.1 Workstations

There are two workstations certified for use with Verity Vanguard 1.0. The HP Z2 SFF G9 which is required for new customers and the HP Z4 G4 for existing Verity customers. The workstations run Windows 10 Enterprise 2021 LTSC as their operating system (OS). Both variants employ two 1TB hard drives in a RAID1 configuration for data redundancy. The Z4 G4 workstation uses platter drives, while the Z2 SFF G9 uses solid state storage media. Workstations are configured with Secure Boot enabled. BitLocker drive encryption is enabled after installation and

configuration of the Vanguard Workspace software. User logins require a USB security token unique to the user for multi-factor authentication (MFA). FIPS 140 security policies are enabled on the workstations, and validated cryptographic components are used for the encrypting and digital signing of data. In [4], Hart describes physical security measures and best-practices for jurisdictions to protect the integrity of Vanguard Workstations.

Workstations can be configured as standalone or networked together in a client/server configuration. Client/server configurations are typically used to allow multiple users to perform program functions simultaneously. In this configuration, all data from the networked application is stored on the server workstation. In [3], Hart depicts the set of supported standalone and client/server configurations for Vanguard workstations.

In [4], Hart states that

> Vanguard Server Client networks connect only to each other on a local network, and cannot connect to an outside network. All networks arrive at the customer preconfigured. Vanguard certified components and hardware do not contain any wireless hardware, internal chips, or antennas. In addition, all software disables the use of wireless by default.

and

> Vanguard supports isolated networking of workstations to distribute large workloads. The network configuration does not support Internet access. The firewall only allows certificate-based authenticated connections through only the ports and protocols necessary to support specific Vanguard functionality. For stand-alone workstations and polling place devices (which lack networking hardware), the firewall is configured to reject all connections.

2.2 Define

Vanguard Define is used to enter data for elections, including jurisdictions, contests, candidates, propositions, translations, and audio. Define allows for the proofing of data, layout, and performs validation. In Verity Voting 2.x, this set of functions was grouped under a component called “Verity Data”.

COTS USB media may be used to to import and export data. In [4], Hart provides procedures and recommendations for the use of COTS USB media.

Though Define provides the ability to proof all entered election data and audio recordings, it only provides previews of how ballots will look. Ballot layout proofing happens in Deploy.

Define can be run on a standalone workstation with Deploy, a standalone workstation with Deploy and Results, or on multiple Define/Deploy workstations networked on a closed LAN.

2.3 Deploy

Vanguard Deploy is the application that allows election officials to proof ballot data and layout, print ballots, configure polling place device settings (including the management of device users), and create various media that will be used to load the election definition and perform other election related functions. This set of functionality was grouped under a component called “Verity Build” in Verity Voting 2.x.

Deploy can be run on a standalone workstation with Define, a standalone workstation with Define and Results, or on multiple Define/Deploy workstations networked on a closed LAN.

2.3.1 Media

Much of the media required to administer an election is created in Deploy.

vDrives are custom USB storage media that must be obtained by Hart. The hardware allow-listing on Vanguard devices and workstations will only allow the use of vDrives for certain functions. vDrives are used to transfer the election definition created in Deploy to polling place devices and Capture workstations. On devices, they store logs, and where applicable, cast vote records (CVRs), scanned ballot images, and scanned printed vote record (PVR) images. They are also used to create recovery (i.e. backup) drives and to transfer CVRs and other election metadata from Vanguard Vault and/or Capture to Vanguard Results for tabulation.

Verity Keys are security devices that fit into a standard USB port. They are unique to the election. Sensitive operations in the administration of an election require the Verity Key to be inserted and associated passcode entered. Verity Keys are also used to distribute the private signing key used to digitally sign election data like CVRs. In Deploy, application and device passwords specific to the election and Key are written to the Verity Key. Given their sensitivity, Hart recommends users have limited access to Keys and Key passwords and that jurisdictions maintain chain of custody logs for Verity Keys [5].

Device Security Tickets act as a form of MFA for election workers to access “Poll Worker”, “Maintenance”, and “Administrator” role-based functions on Vanguard

Devices. Security Tickets are printed on business card stock. They are election specific and cannot be reused for subsequent elections.

2.3.2 Ballot Printing and Numbering

Only certain printer models are certified for use in ballot printing directly from Deploy. For low-volume printing, Brother HL-L6400DW, Brother HL-EX415DW, and HP 4001dn printers may be used. The OKI C831, OKI C844, OKI 911, and IntoPrint Sp1360 printers can be used for direct printing of ballots from Deploy in higher-volume scenarios [4].

Deploy gives jurisdictions a few different options for ballot numbering:

Pre-printed unique identifiers are non-serialized numbers that can be used during scanning to detect and reject duplicate ballots. These identifiers can be represented on the ballot with a barcode or a barcode and human-readable number. The unique identifier is not tied to or associated with the voter in Vanguard. In general, no personally identifying voter information is stored in the Vanguard system.

A second, separate unique identifier for use in risk limiting audits (RLAs) can be imprinted by scanning devices onto ballots and PVRs.

Yet another separate human-readable number called a “ballot number” can be included in the margins of printed ballots. Deploy can configure this numbering to be started or restarted at any number. The intended use-case of ballot numbers is the inventory of paper ballots. Per [5], “ballot numbers are not used during the ballot scanning process.”

2.4 Capture

Vanguard Capture is an application used by election officials for ballot scanning at the jurisdiction’s central office. Capture also supports voter intent adjudication for damaged ballots and ballots with marginal marks. Capture converts voter selection marks to CVRs. The CVRs are written to vDrive(s) for transfer to Vanguard Results where vote tabulation and reporting of election results take place. Write-in resolution also takes place in the Results application.

In Verity 2.x, this component was branded as “Verity Central”.

Canon DR-G2110 and DR-G2140 are the high-speed scanners certified for use with Capture. These scanners can be configured with an optional imprinter capability which uses an ink cartridge to apply a unique ID to left edge of the face-up side of the ballots relative to their orientation in the feed tray. In [6], Hart states that “if a batch must be rescanned (e.g., due to rejected ballots), the ballots must be rotated to avoid overprinting.”

Capture uses optical character recognition (OCR) to read voter selections on PVRs. While other election data may be encoded in bar codes or QR codes, no voter selections are encoded into non-human readable portions of the ballot.

Capture can be run on a standalone workstation or on multiple Capture workstations networked on a closed LAN where multiple scanning stations can be operated in parallel.

2.5 Results

Vanguard Results is the application used by officials to tabulate election results and generate reports. Results reads CVRs from vDrives received from Vanguard Vault devices or Vanguard Capture workstations. Results is where election officials perform write-in resolution. It is also the application used to collect and store all election logs from the set of Vanguard devices used in the election.

In Verity 2.x, the component performing tabulation and reporting was branded as “Verity Count”.

Results can be run on a standalone workstation, a standalone workstation with Define and Deploy, or on multiple Results workstations networked on a closed LAN.

2.6 Settings

Vanguard Settings is available on all Vanguard workstations. It provides authorized users a way to manage a limited set of operating system functions:

- Setting system date and time
- Exporting software application file hashes for software validation
- Accessing the operating system (requires limited-use passcode from Hart)
- Importing printer configuration files
- Changing the certificate set
- Exporting system logs

Regarding certificate sets, in [4] Hart says:

> This Vanguard feature allows jurisdictions to change workstation and device certificate sets; this can be done at the jurisdiction’s discretion. For example, a state may choose to be assigned a unique certificate set to prevent accidental compatibility with other states’ Vanguard voting systems. A jurisdiction might also choose to update their certificate set in the event the previous set had been compromised.

2.7 Users

Vanguard Users is the application where administrators create and manage user accounts. Vanguard Users is available on all server and standalone workstations. Accounts on client workstations are managed by the server. Administrators use the application to configure software user accounts, roles, and access policies. This is also where user-specific Workstation Security Tokens are created for workstation users. Workstations require users to insert this token into a USB port as a form of MFA.

This functionality was branded as “Verity User Manager” in Verity 2.x.

2.8 Manage

Vanguard Manage is used to add, copy, import, export, archive, restore, and manage elections. Once an election is added or imported in Manage, it can be opened and interacted with using the software features available to the user on the workstation they are logged into. Vanguard Manage is available on all server and standalone workstations.

2.9 Libraries

Vanguard Libraries is an add-on application that can be unlocked on any Vanguard Define/Deploy workstation. Users of Libraries are able to add, import, and save translations and audio for reuse.

2.10 Test Decks

Vanguard Test Decks is an add-on application that can be unlocked on any Vanguard Define/Deploy workstation. Per [3],

> Test Decks allows users to generate a pre-marked set of ballots (a “Test Deck”) that can be used for Logic and Accuracy Testing of the Vanguard voting system. Test Decks allows users to select a marking pattern and generate a test deck which is then available to print and/or export within the Vanguard Deploy software application.

2.11 Observations

Through a secure chain of custody, the Texas Secretary of State Elections Division obtained the hard drive and CFast images used in the EAC certification, i.e. the

Trusted Build. Hart personnel used those same files to perform installation under the supervision of the examiners.

The configurations demonstrated at the exam were a subset of the total available. However, both types of HP workstations were demonstrated as were examples of standalone and client/server configurations. There were no major concerns with the Vanguard workstation hardware or configurations. Installation and configuration is always performed by Hart; thus, there is no added burden or opportunity for misconfiguration by the jurisdictions. The COTS components performed adequately during the observed tasks.

Hash validation is a critical component of acceptance and L&A testing. It is the process that is used to ensure that the software and/or firmware of a voting system matches exactly with what was certified by the EAC. A hash is the output of a cryptographic function run on a file or drive partition that acts like a digital fingerprint. If a file or partition has changed in any way, it will produce a different hash result. Hart provides two methods for hash validation. One method involves the use a System Validation Tool that is part of Vanguard Settings, and the other is a manual process which requires access to the base OS. Both processes result in a hash manifest file which can be checked against a Trusted Hash Manifest using third party tools. Examiners observed the export of hashes using both methods. Instructions for both methods are straightforward in the documentation; however, the manual method requires significantly more effort and the involvement of Hart Technical Services to obtain access to the OS desktop.

The hash manifests for all workstations under examination were exported using Vanguard Settings. Those exported manifests were compared and successfully validated against the Trusted Hash Manifest using the “diff” tool on an Ubuntu 24.04.3 LTS laptop. The manual method produced a hash manifest in a different file format than the Trusted Hash Manifest. Both file formats are human readable, but time did not allow for the manual comparison of the hundreds of exported hash values. Examiners conducted a handful of spot checks which were successful. Since the exam, Hart has submitted ECO-01720 to the EAC for review. This ECO updates the documentation of the manual process with instructions for formatting the exported manifest in a way that allows for automated comparison to the Trusted Hash Manifest using standard third party tools. Texas examiners have not yet had the opportunity to assess the changes in ECO-01720. Approvals of minor modifications in Texas typically take place only after EAC review and approval.

Examiners observed that the passcode used to access the OS desktop is not obfuscated when typed into the user interface. While the risks of non-obfuscation in this case are minor (this is a limited-use passcode), it is a security best practice to obfuscate passwords when typed, and Hart should correct this oversight in future versions of Verity Vanguard. There were no other instances where the non-obfuscation of passcodes were observed.

Use of Vanguard Define was not directly observed as the data, layout, and audio for the L&A Test were created prior to the start of the exam. However, no issues were observed during the export to Vanguard Deploy, during the L&A Test, or during unscripted testing. Examiners observed the import of a signed election export from Define into Deploy as well as the creation of election media. No issues were observed with this process.

According to [7], if pre-printed human-readable unique IDs are configured in Deploy, digits 2-7 of the unique ID are the device serial number. In the case of pre-printed ballots for hand-marking, the documentation is unclear on where the device serial number would come from. However, for PVRs produced by BMDs, this may meet the state's ballot numbering requirements.

There were some small issues with the instructional text and features of Vanguard Devices which would likely be addressed by improvements to the Deploy application. Those issues will be addressed in detail in Section 3.5 which deals with observations from interactions with Vanguard Devices.

During the L&A Test, examiners observed the use of Vanguard Capture to scan batches of ballots and PVRs. No issues were found with respect to accuracy, speed, paper jams, or interpretation of ballot marks. The quality of the scanned images was good and suitable for the adjudication of ballots. Ballots and batches of ballots with issues were appropriately detected and rejected.

During the L&A and unscripted testing, examiners adjudicated ballots, observed the tabulation of votes from vDrives, and observed the generation of reports using the Vanguard Results application. The tabulated results matched the expected outcome of the L&A Test. During unscripted testing, examiners attempted to process vDrives that had already been tabulated, and the Results application appropriately flagged the media as having already been read.

In the Results UI for write-in assignments, contest write-ins can be assigned to candidates in batches. After the assignment has been made, the most recently assigned candidate is still highlighted in the menu of available candidates. After the next batch of write-ins is selected, the previously selected candidate could be absent-mindedly assigned. From a user experience workflow perspective, it is understandable why Hart made this design choice. However, requiring a few extra clicks on the part of the user is worth ensuring the correct assignment of write-ins to candidates. In future versions of Verity Vanguard, Hart should deselect all candidates in the Available Candidates menu after batch assignments have been made.

3.0 Verity Vanguard Devices

Vanguard Devices are the set of equipment used in the polling place. Devices are “purpose-built…contain no networking hardware, including no wireless capabilities” [3]. All Vanguard Devices operate in kiosk mode and share a common hardware platform. They implement a Secure BIOS which verifies a chain of trust prior to the system booting up. CFast drives store device firmware and are encrypted with BitLocker encryption (following the first boot). Application allowlisting is enforced to prevent the execution of unauthorized software.

The CFast compartment has multiple layers of physical security. In [4], Hart describes physical security measures and best-practices for jurisdictions to protect the integrity of Vanguard Devices.

Per [3]:

> The Verity device is required to be shipped from the Hart facility to the customer with all applications installed and the device configured to operate in Kiosk mode; there is no user installation of software on the device allowed. There is no access to the desktop, whatsoever.

Windows 10 Enterprise 2021 LTSC is the operating system for all devices, and all devices use an Intel Atom 6413E embedded processor as the CPU.

All devices are capable of being used with the Vanguard Access Audio Tactile Interface (ATI) peripheral to aid with accessibility.

vDrives are used to load election definitions, store logs, and where applicable, store CVRs and ballot images. Election data is also written to the CFast card for redundancy.

Some functions require the use of a Verity Key. The USB compartments of Vanguard Devices have been designed such that the door cannot be closed with a Verity Key still inserted. Device Security Tickets are used to initiate and authenticate “Poll Worker”, “Maintenance”, and “Administrator” role-based functions.

Hart provides two methods of hash validation of device firmware. The first method requires an Administrator-level user to run the System Validation Tool from the application partition of the device CFast to export a hash manifest to a standard USB drive (i.e. USB storage media other than a vDrive). This exported manifest can be compared against the Trusted Hash Manifest using third-party tools. The second method involves the removal of the CFast card from the device, then performing a read-only mount of the CFast onto an air-gapped Ubuntu 20.04 LTS system. In [8], Hart provides a list of commands to perform the write-protected mounting and

compute a SHA256 hash of the entire drive partition. This output can be compared against a trusted hash provided by the Texas Secretary of State.

Hart employs a unified write filter (UWF) which redirects all write operations to the OS and application partitions to virtual memory. This allows for the repeatable hashing of entire CFast partitions.

3.1 Boost

Vanguard Boost is a poll worker facing device. It can be used to print blank paper ballots for hand marking on-demand from an attached COTS printer. It can also be used to issue VotePasses which are paper tickets used by voters to activate a voting session on the Vanguard Flex BMD. The Brother HL-L6400DW, Brother HL-EX415DW, HP LaserJet Pro 4001dn, and OKI Data C844dn printers are the COTS components certified for ballot printing with Boost [3]. Vote data is not stored on Boost, but Boost can produce Ballot Count, VotePass Count, and Ballots Issued reports.

3.2 Flex

The Vanguard Flex is a BMD with an integrated thermal printer that creates a printed vote record (PVR) that is both human- and machine-readable. Unlike prior Verity systems, all Vanguard BMDs are standalone; there is no equivalent to the Verity Controller in Vanguard.

Voting sessions on Flex are activated directly by the poll worker or by a VotePass ticket issued to the voter by Boost. VotePasses contain a thermally printed activation QR code that is inserted into Flex and scanned and authenticated. Prior to activating the voting session, Flex burns a thermally printed “stamp” over the QR code preventing its reuse.

Voters insert a blank sheet of thermal paper and use the touchscreen or ATI to mark and review their choices. When complete, voters print their PVR and take it to the Vanguard Vault where it is scanned and automatically deposited into a ballot box.

No CVRs are stored on Flex.

3.3 Adapt

Vanguard Adapt is a BMD specifically designed to accommodate voters with dexterity impairments. Voting sessions are activated by a poll worker. Blank paper is automatically fed to an ink printer. Voters use the touchscreen or ATI to mark and review their choices. When complete, the PVR is exposed to the voter behind a glass

window where it can be reviewed without manual handling. If accepted by the voter, the PVR then drops down into the integrated ballot box.

Vanguard Adapt does not scan or tabulate ballots or store CVRs. Ballots automatically deposited into the ballot box would be scanned by Vanguard Capture at the jurisdiction's central office. Spoiled ballots can be retrieved without opening the ballot box doors. However, unlike Vanguard Vault, there is no mechanism to prevent a provisional ballot from dropping into the ballot box. Nor is there a mechanism for provisional ballots to be out-stacked to a separate compartment.

3.4 Vault

Vangaurd Vault is primarily used as a polling place scanner. It can also be used as a low-volume central scanner for small jurisdictions. Vault securely attaches to an integrated ballot box, and ballots are automatically deposited after being scanned and accepted.

Vault can be configured to reject ballots under certain conditions (overvote, undervote, provisional, etc). In most cases the voter can either choose to override the rejection or seek out a poll worker for assistance. Vault can be configured to produce an interactive summary screen of voter choices when a ballot is scanned, but it cannot be configured to produce this summary on demand. The feature is either always on or always off.

The Vault scanner uses optical character recognition (OCR) to read voter selections on PVRs. While other election data may be encoded in barcodes or QR codes, no voter selections are encoded into non-human readable portions of the ballot that would be scanned and tabulated.

3.5 Observations

All of the Vanguard Devices were used as part of the L&A Test and unscripted testing.

Examiners witnessed the installation of CFasts from the Trusted Build into all of the voting devices under examination.

Hashes for each device were pulled using the System Validation Tool and successfully validated against the Trusted Hash Manifests. The manual hash validation method was used on a subset of devices and also successfully validated against Trusted Hashes. Use of the System Validation Tool was straightforward. However, the System Validation Tool application lives on the same CFast partition from which hashes are exported, and thus, is not a fully independent method of validation. In the very unlikely scenario that a bad actor were able to compromise

the system, the only fully independent validation of device firmware is the manual method which hashes the application partition of the CFast itself.

The manual method is more cumbersome for the user and not without risk. These risks are addressed by Hart in [8]:

> [Use of the System Validation Tool] protects the system from human error. During manual retrieval, a deviation from the documented process or a mistake can result in the voting system becoming unusable. This can result from actions such as skipping a step, using a different Operating System while retrieving files from the CFAST, and simple mistakes like moving a file instead of copying it, among other potential mistakes. If a voting system component is altered during manual retrieval, it will be unusable and a new CFAST or Hard Drive set must be deployed by Hart to make the system usable again.
>
> Recent, documented security breaches by insiders in multiple states have resulted in voting system software files being copied and distributed to unauthorized third parties. The manual retrieval and verification process opens a window for an insider to maliciously retrieve and distribute voting system software files without leaving any evidence, because seals and other protections must be removed as part of the manual process. The System Validation Tool protects against this scenario in two ways. First, the exported files are encrypted, which protects them from reverse engineering and other attacks. Second, all physical security features remain in place (locks, seals, etc.). This means that both tamper-prevention and tamper-evidence protections stand between an inside attacker and the voting system software files.

I recommend that jurisdictions use the System Validation Tool in most cases. The manual method should be reserved for spot checks, validation checks that happen on a longer cadence, or cases of suspected tampering or malfeasance. Jurisdictions should establish strict chain of custody and multi-person verification procedures for using the manual hash validation method.

The Boost device was user friendly and no issues were observed with its use.

Flex was similarly user friendly. The integrated thermal PVR printer was resistant to feed issues, and paper jams could be cleared with relative ease in a non-intrusive fashion. There were multiple layers of protection preventing the activation of multiple voting sessions with the same VotePass. Examiners attempted some informal penetration testing of this feature and were thwarted at every turn.

Vault was resistant to paper feed issues and jams. It appropriately rejected ballots that had already been scanned as well as ballots that met the criteria configured in Deploy. The attached ballot box meets state requirements on physical security.

The Vault's touchscreen UI was generally user friendly, but there were a few issues with messaging and voter interactions that could be improved. If a ballot has a marginal mark, the issue is flagged for review with the message, "One or more marks are too small. Marks that are too small may or may not be counted." The voter is allowed to override this issue. Instead, issues of this nature should require poll worker intervention. This is different than an under- or over-vote scenario where the voter knows the consequence of their choice.

When a ballot for another election is inserted into the Vault scanner, the UI displays a message that says, "This ballot is not readable. Either the device could not find a barcode or the inserted sheet is not the correct length." To prevent confusion, this message should instead read, "Either the device could not find a barcode *for this election* or the inserted sheet is not the correct length."

The Vault can be configured to provide the voter a review screen of their choices based on their scanned ballot. This option could be helpful for voters with accessibility impairments (they could review the scanned ballot using an attached ATI), and it provides a somewhat independent check on the voter's PVR. Unfortunately, if this feature is enabled, it is always on for every voter and could slow down polling places. I recommend Hart add a configuration option in Deploy to enable the review screen on demand or if an ATI is attached to Vault.

In a prior voting system report, I expressed some discomfort over imprinters in polling place scanners [9]. However, Section 9.1.5-G of the VVSG 2.0 alleviates this concern [10].

The Adapt device is voter-friendly, and noble in its attempt to provide accessibility to voters with dexterity impairments. Unfortunately, it's design creates a confluence of other issues that make it difficult to recommend as a polling place device. It is the only device in the Vanguard system that prints PVRs on regular paper instead of thermal paper which may make it easier to violate the secrecy of the ballot. Adapt also has no mechanism to prevent provisional ballots from being deposited into the attached ballot box with regular ballots or to out-stack them. In [3], Hart states that "Adapt enables voters to mark, verify, and cast their ballot, all without touching a piece of paper", but the provisional voting procedures in Texas require provisional ballots to be placed in a separate envelope. Provisional voters in Texas with dexterity impairments would already need outside help to place their ballot in the provisional envelope. To say all voters can use any polling place device for voting except the Adapt for provisional voting may be at odds with other parts of Texas' laws governing elections.

4.0 Conclusions

While some minor issues arose during the examination, none were disqualifying. Overall, Verity Vanguard 1.0 is a comprehensive voting system that is secure, accurate, and user-friendly. The system reported L&A results accurately. Hart personnel provided clear and knowledgeable answers to the examiners' questions.

Jurisdictions should carefully consider which hash validation method to use and take extreme care if/when using the manual method. Given Hart's statement that "a state may choose to be assigned a unique certificate set to prevent accidental compatibility with other states' Vanguard voting systems" [4], I recommend that all jurisdictions request unique certificate sets from Hart to prevent such accidental compatibility.

Furthermore, jurisdictions should follow best practices for physically securing Vanguard workstations and devices, and they should train personnel on how to properly apply and check security seals to prevent tampering.

Vanguard does not include any DRE devices. Every voter's choice is represented in human-readable text on a paper ballot or printed vote record. If jurisdictions opt to use BMDs, they should provide bar magnifiers with guidelines in every poll booth and conduct public outreach campaigns to encourage voters to double check their PVRs prior to depositing them in the ballot box. Every voter can do their part to audit the security of an election by reading their own ballot or PVR to ensure their selections match their intent.

In future versions of Verity Vanguard, Hart should:

- Obfuscate all passcodes when entered.
- Make it harder for users to accidentally batch assign write-ins to the wrong candidate.
- Improve Vault messaging and ballot review features.

I recommend certification of Verity Vanguard 1.0 with the caveat that the Secretary of State should consider excluding Vanguard Adapt from the set of components certified for use in Texas. I am not an expert in legal compliance with Texas accessibility requirements for the polling place, nor am I an appropriate voice to speak for the disabled community. However, it is my understanding that the other Vanguard devices when paired with the Vanguard Access ATI meet the State's accessibility requirements.

5.0 References

[1] United States Election Assistance Commission Certificate of Conformance, Hart Verity Vanguard 1.0, EAC Certification Number HRT-VV-1.0, Jul-07 2025, URL: https://www.eac.gov/voting-equipment/verity-vanguard-10

[2] Application for Texas Certification of Voting System – Form 100, Verity Vanguard 1.0

[3] Verity Vanguard 1.0 System Overview, Document Number 1000812, Revision A09

[4] Vanguard System Administrator's Guide, Document Number 6700-001, Revision A05

[5] Vanguard Deploy User Guide, Document Number 6710-002, Revision A05

[6] Vanguard Capture User Guide, Document Number 6710-003, Revision A05

[7] Vanguard Ballot Printing Guide, Document Number 6740-001, Revision A05

[8] Verity Vanguard Manual Application Hash Validation Process Document, Document Number 1000828, Revision A.00

[9] B. Mechler, Voting System Examination of Election Systems & Software EVS 6.3.0.0, Apr-2023, URL: https://www.sos.state.tx.us/elections/forms/sysexam/brian-mechler-ess-exam-report-evs-6300.pdf

[10] Voluntary Voting System Guidelines VVSG 2.0, Feb-2021 URL: https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf