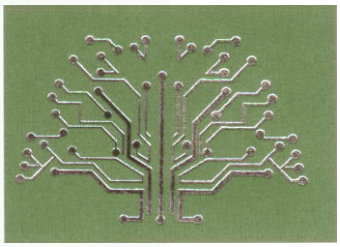


FREEMAN, CRAFT, MCGREGOR GROUP

# California Secretary of State Consultant's Public Report on:

## Security and Telecommunications Testing of the Hart InterCivic Verity 3.0 Voting System

Prepared for the
California Secretary of State

July 23, 2018

## Revision history

| Version | Change date | Author(s) | Changes to previous version |
|---|---|---|---|
| 1.0 | 07-02-2018 | McGregor and Craft | Initial Draft |
| 1.1 | 07-03-2018 | Weingart | Updates |
| 1.2 | 07-05-2018 | McGregor, Craft, Bullock | Updates |
| 1.3 | 07-09-2018 | McGregor, Bullock, Craft and Weingart | Revisions in response to CA SOS comments. |
| 1.4 | 07-13-2018 | Craft | Final |
| 1.5 | 07-23-18 | Craft and McGregor | Revisions in response to CA SOS and Hart InterCivic Comments |

# Table of Contents

## Introduction

The purpose of the Security and Telecommunications Testing is to identify and document vulnerabilities and potential vulnerabilities, if any, to any physical or logical tampering or errors that could cause:

- Incorrect recording,
- Tabulation,
- Tallying or reporting of votes, or
- That might be used to change the outcome of an election, to interfere with voters' ability to cast ballots or have their votes counted during an election or to compromise the secrecy of vote; or
- Could alter critical election data such as election definition or system audit data.

To the extent possible, when a vulnerability is found, the report will indicate whether the vulnerability can be exploited by a:

- Voter: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for less than an hour.
- Poll worker: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for up to one week, but all physical security has been put into place before the machines are received.
- Elections official insider: Wide range of knowledge of the voting machine design and configuration. May have unrestricted access to the machine for long periods of time. Their designated activities include:
    - Set up and pre-election procedures;
    - Election operation;
    - Post-election processing of results; and
    - Archiving and storage operations.
- Vendor insider: With great knowledge of the voting machine design and configuration. They have unlimited access to the machine before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service, and when providing election administration services.

In addition, the report indicates whether exploiting these vulnerabilities will cause any of the following, or other, compromises to the system:

- Unauthorized changes to system capabilities for:
    - Defining ballot formats
    - Casting and recording votes
    - Calculating vote totals consistent with defined ballot formats
    - Reporting vote totals
- Alteration of voting system audit trails
- Changing, or preventing the recording of, a vote
- Introducing data for a vote not cast by a registered voter
- Changing calculated vote totals
- Allowing access to vote data--including individual votes and vote totals--by unauthorized individuals
- Allowing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes

This public report includes descriptions of the findings and vulnerabilities, an evaluation of the risk associated with each vulnerability, recommendations to mitigate these vulnerabilities and our conclusions. Information that cannot be disclosed publically under the Non-Disclosure Agreement between the California Secretary of State (SOS) and Hart InterCivic (Hart), and details of attack methods are not provided in this report in order to make it available to the public.

## Scope of Work and Reporting

This report covers the work completed during the Security and Telecommunications Test of the Hart InterCivic Verity Voting 3.0 System (the system). As previously stated, the purpose of this test is to identify and document vulnerabilities and potential vulnerabilities. The work described in this report does not include an audit of compliance with any standard. While compliance or non-compliance with a specific standard as it relates to a given vulnerability may be included in the discussion of that vulnerability, this report provides no assurance that the system complies with any professional standard, including the California Voting System Standards.

Physical security tests, tamper evidence and detection tests and an evaluation of the use of cryptography were conducted in accordance with FIPS 140-2 “Security Requirements for Cryptographic Modules.” To the extent applicable, penetration tests were conducted to be consistent with NIST Special Publication 800-115 “Technical Guide to Information Security Testing Assessment.” The vulnerability assessments in the work papers are based on “Calculating Attack Potential” as defined in section B4 of

Vulnerability Assessment (AVA) in Common Methodology for Information Technology Security Evaluation (CEM v3.1R2, September 2007)

We are not attorneys and do not offer legal advice. We assisted the SOS by collecting facts and evidence regarding vulnerabilities in the system in order for them to make certification decisions. However, to advise the SOS on the determination of whether the system sufficiently complies with California's certification requirements and whether it should be certified would require an interpretation of law. Accordingly we do not provide recommendations or offer any opinion as to whether the system can be certified.

The work we performed and our findings are strictly limited to the specific serial numbered hardware elements and specific software elements as they were configured and examined during the on-site test. An inventory of those items is included as Attachment A to this report. The results described in this report should be reliable and repeatable for those specific devices. The decision to apply those results to reach conclusions about other devices is solely at the discretion and risk of the SOS and election officials who may purchase the system.

## Manufacturer’s Description of System

The description of the system and the image in this section were provided, and copyrighted, by Hart.

### Brief Description

The system includes software, hardware, device, and peripheral components that allow election professionals to accomplish the following high-level tasks:

Pre-voting tasks:

- Ballot data creation (Verity Data)
- Election definition and ballot production (Verity Build)
- Device configuration

Voting tasks:

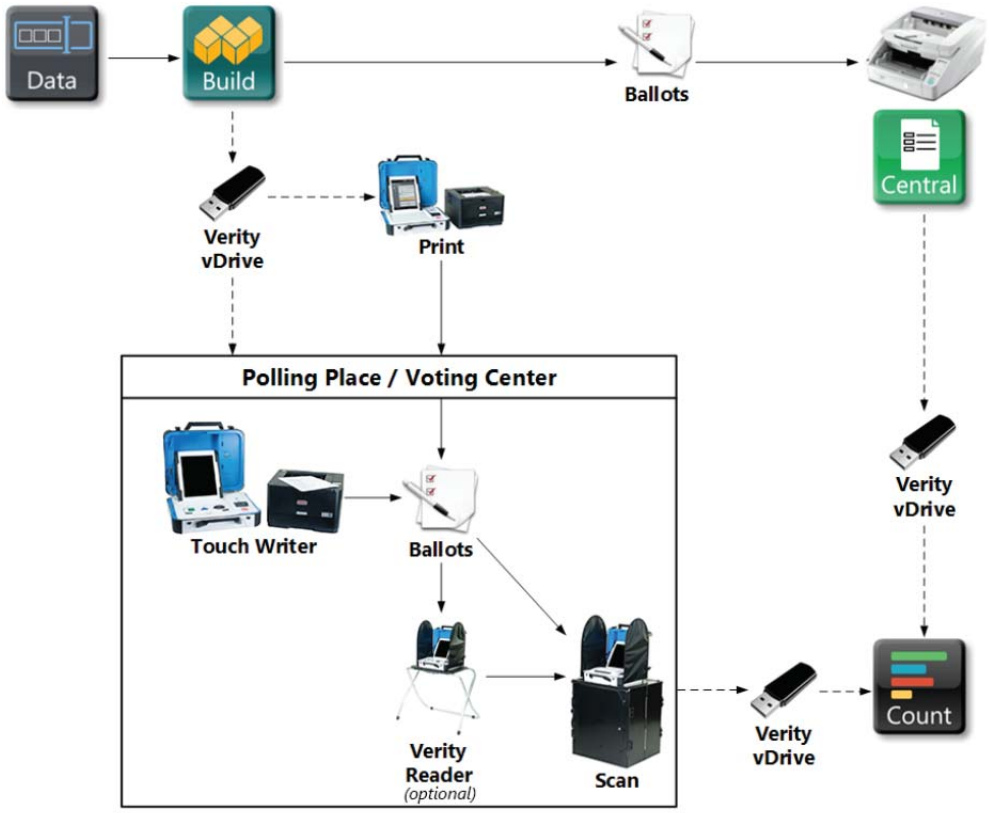
- Polling-place-based ballot printing (Verity Print)
- Polling place Ballot Marking Device (Verity Touch Writer)
- Polling place ballot review (Verity Reader)
- Polling place digital scanning for paper ballots (Verity Scan)
- High-speed, large-volume ballot scanning (Verity Central)

Post-voting tasks:

- Ballot adjudication (Verity Central)
- Counting of votes/Tabulation (Verity Count)
- Consolidation and reporting of results and audit logs (Verity Count)
- Audits and recounts

## System Architecture

Overall system architecture is illustrated in the diagram below.




This diagram illustrates the following components:

Verity Data: Ballot design software

Verity Build: Election definition and media creation/ballot printing software

Verity Central: Central ballot scanning and adjudication software

Verity Print: On-demand ballot printing device

Verity Touch Writer: Accessible ballot marking device

Verity Reader: Optional ballot verification device

Verity Scan: Ballot scanning device

Verity Count: Ballot tabulation and reporting software

Verity vDrive: Specially formatted USB media used to transfer the election ballot styles to voting devices, and to transfer cast vote records to Verity Count for tabulation.

Dotted lines represent the flow of data and air gaps using vDrives.

## Hardware Components

### Verity Scan

Verity Scan is a polling-place-based digital scanner used to cast ballots. It can be used with hand-marked ballots or with those printed using the Touch Writer. Verity Scan provides the voter with the opportunity to check and correct the ballot before casting it. Verity Scan deposits scanned ballots into its ballot box for secure storage.

### Verity Touch Writer

Voters can mark digital ballots using a touch screen using Verity Touch Writer. After the voter has confirmed the selections, the voter prints the marked ballot on the attached printer, retrieves it and casts the ballot.

### Verity Reader

Verity Reader is an accessible ballot verification device; voters can insert their marked paper ballot to visually verify how their ballot will be counted, and/or hear an audio read-back of their ballot selections. Verity Reader is a paper-ballot review device only; Reader does not store or tabulate votes.

### Verity Print

Poll workers can print and issue blank paper ballots to voters using Verity Print. The voter votes their ballot and can cast it using either Verity Scan, or by depositing it into a ballot box to be scanned centrally.

### Verity Access

Verity Touch Writer and Verity Reader devices are equipped with Verity Access, which provides the voter with additional input options: a scrolling wheel and select button, headphones and a connection that may be used with tactile buttons or sip-and-puff devices.

### Verity vDrives

Verity vDrives are used to transfer digital ballot styles from Verity Build to other Verity devices, and to transfer cast vote records from Verity Scan and Verity Central to Verity Count for tabulation. Verity vDrives are inserted into a standard USB port and each Verity Scan, Verity Touch Writer, Verity Reader, and Verity Print device has its own Verity vDrive.

### Verity Key

Verity Key is a small security device that is programmed for each election. Verity Key is also inserted into a USB port.

Verity Key is part of the system's two-factor authentication process. Two-factor authentication requires each user to have a programmed Verity Key and to know the passcode associated with the Verity Key. Both the user passcode and the Verity Key must be authenticated together. Critical operations within the system require the Verity

Key to be inserted and the passcode to be entered. Only when the system authenticates the Verity Key and password will it allow the operation to continue.

### Commercial Off-The-Shelf (COTS) Hardware Components

**Computer Workstations**
Verity software applications (Data, Build, Central, and Count) are installed on specially configured, RAID-equipped computer workstations.

**Ballot Scanners**
Several models of medium- to high-speed scanners have been tested and certified for use with the system in central ballot scanning operations with Verity Central. *

**Ballot and Report Printers**
Several models of printer have been tested for use with the system for the purposes of printing ballots and reports. *

* NOTE – Several models of scanners and printers have been tested and certified for use by other jurisdictions. For the test described in this report, only one scanner was provided. See Attachment A.

## Description of System Tested

The system tested was comprised of three sets of components:

1. The server and client set used for creating, managing and tabulating an election.

   This included the Verity Data/Build standalone and server/client set, the Verity Central standalone and server/client set and the Verity Count standalone and server/client set. A COTS scanner and printer were also used in these configurations. These components are used in the central election office to define, build, deploy, and count ballots.

2. The voting device is used in polls for voting.

   This includes the Verity Scan, Verity Touch Writer and Verity Reader. These components are used in the polls to perform actual voting operations.

3. Verity Keys and Verity vDrives

   These components perform the secure authentication and data transfer operations between the central election office components and the poll components.

## Assumptions

The components that are used in a central election office were installed on standard COTS PCs. No physical security mechanisms, such as locks, seals or tamper-evident labels were applied to these systems, so no physical security tests were performed. Logical security tests were performed on all of these devices.

The poll devices were supplied with physical security locks, seals and tamper-evident labels and they were installed in accordance with the manufacturer's recommendations. As such, a physical security test was performed on all security locks, seals and tamper-evident labels. Logical security tests were performed on all of these devices.

Test procedures assumed that the attacker had an undisturbed place to mount the attacks. It was also assumed that tools and materials, both physical and logical, which are typically used in these attacks were available.

All tools and methods deployed during this security test are commonly available. The physical tools and devices can be purchased at local consumer outlets or online. All of the logical tools can be purchased and/or downloaded online from common locations.

## Approach to Testing

Personnel performing tests included:

Freeman, Craft McGregor Group:

- Kate McGregor
- Jessey Bullock
- Steve Weingart

Personnel witnessing the tests included:

SOS

- NaKesha Robinson
- Todd Ross
- Rodney Rodriguez

The system was set up in the test lab at the SOS office before the test team arrived. After a brief overview of the system, the team contacted the vendor to request election data necessary to conduct the tests as none had been installed on the system prior to the beginning of the test period.

The test began in two phases. Since they were accessible, the software specialist immediately started to work on the servers. The hardware specialist started to try to exploit the locks, seals and tamper-evident labels applied to the poll devices.

Once the physical security was bypassed, the entire team focused their attention on the software resident on the central workstations and servers as well as on the poll devices, Verity vDrives and Verity Keys.

As potential vulnerabilities were discovered, appropriate tools were brought to bear to determine if an exploit was possible. At regular intervals the team discussed the current status and findings to determine if any of the potential vulnerabilities could be used in combination to enable an exploit. This method was repeated and refined as the test continued until the duration of the test period was exhausted.

## Scope Limitation

There was no election data installed on the system that was provided to the test team by the SOS and, once this was discovered, none was provided to the team by the SOS. The necessary data was acquired by contacting the personnel at Hart who were assigned to support the test. Hart sent the election data via overnight delivery and, once it arrived, the test team loaded it on the system following instructions provided by Hart. Ideally, the system should have been populated with data developed by the functional test team during their test and in accordance with the California Use Procedures for the system. Accordingly there is no evidence that the data used in the security test was actually produced on the test system, or that its data structure is the same as that which would be used for California elections.

No intentional physical damage to the devices was permitted. Some elements were disassembled as part of the testing process, but all items were returned to the pretest state at the end of the test. In the case of the client/server systems, some may have had to be reinstalled to be returned to full service.

## Findings and Vulnerabilities

A diagram of the relationship between the attacks described in this section is provided as Attachment B.

### Locks and tamper seals are subject to picking and removal

Lock picking was attempted and was successful using standard widely available lock picks and standard techniques.

Tamper-evident adhesive label seals were removed without damage using a solvent and a razor blade. After removal, the label was allowed to dry and was re-applied to the equipment without leaving evidence of any compromise.

Beaded lock-type seals were opened successfully and reattached with no visible evidence of compromise.

These attacks could be conducted by a poll worker, elections official insider or vendor Insider. They affect Verity Print, Verity Scan, Verity Touch Writer and Verity Reader.

Although these are not complete attacks, they do disable the ability to prevent and detect unauthorized access to the equipment and can be the first step enabling more complex attacks.

The easily defeated locks and seals on the Verity devices resulted in the system failing to meet CVSS 2.1.1.a. which provides that all systems shall “Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability”, and degrades the ability to meet CVSS 7.3.a. which states,” Any unauthorized physical access shall leave physical evidence that an unauthorized event has taken place”

### Unrestricted access to workstation cases.

The cases to the workstations were not secured with tamper-evident labels or locks. The cases were opened in seconds without using any tools. Once access was gained, the BIOS password was removed and the boot order changed. This made it possible to boot the machine from an outside operating system. In addition, there is no disk encryption so the hard disks could be directly accessed and all resident files were accessible and alterable.

This attack could be conducted by an elections official insider or a vendor insider. It affects all system configurations that include a workstation. The workstations are vulnerable to physical attacks that facilitate the software attacks described in findings outlined later in this report.

The configuration of the system workstations presented to the testing team failed to meet CVSS 2.1.1.a. which provides that all systems shall “Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability”. Hart’s failure to secure the workstation cases results in a failure to meet CVSS 7.2.1 which states, “Voting system equipment shall provide access control mechanisms designed to permit authorized access to the voting system and to

prevent unauthorized access to the voting system.", and CVSS 7.3.a., b., and e. which state:

> "a: Any unauthorized physical access shall leave physical evidence that an unauthorized event has taken place.",
>
> "b. Voting systems shall only have physical ports and access points that are essential to voting operations and to voting system testing and auditing.
>
> "e. Access points, such as covers and panels, shall be secured by locks or tamper evident seals or tamper resistant countermeasures shall be implemented so that system owners can monitor access to voting system components through these points.

### Lack of Full Disk Encryption

No component of the system has full disk encryption. Gaining physical access to the machines allowed access to both the operating and application files. Access to the application binaries resulted in recovering and decompiling system source code. While the key material used to protect the integrity of elections was encrypted at rest, the decryption keys were accessible in plaintext. This allowed secrets used to ensure election integrity to be recovered with only physical access to the system's storage device.

The lack of full disk encryption also allowed the whitelisting software to be bypassed on the Verity Count, Verity Build, and Verity Central workstations. The whitelisting bypass was not attempted on the Verity Scan device hardware.

This attack could be conducted by a voter, a poll worker, an elections official insider or a vendor insider. However, it is unlikely that a voter would have sufficient access to the machine to successfully complete the prerequisite defeat of physical security without leaving evidence of the attack.

This vulnerability combined with the unrestricted access to workstation cases resulted in the system failing to meet CVSS 2.1.4.f. which provides that all systems shall "Protect against any attempt at improper data entry or retrieval", and CVSS 7.2.1.b. which states, "Voting system equipment shall provide controls that permit or deny access to the device's software and files."

### Server Spoofing Credential Disclosure

Although the system is configured in a closed Local Area Network (LAN) and utilizes authentication and encryption for incoming connections to the server, authentication and encryption is not enforced on outgoing connections. When a laptop was connected to the network, it was possible to spoof the identity of the server and capture security credentials.

This attack could be conducted by an elections official insider or a vendor insider. It affects all closed LAN configurations on the system.

The lack of authentication on outgoing connections from the server is a failure to meet CVSS 7.2.4.a. which states, “Voting systems shall ensure that only authorized roles, groups, or individuals have access to election data.”

### Shared/Static Secrets

The system has shared static secrets that are used to ensure election integrity. Multiple secrets were shared throughout the system during this test. Recovering these secrets from one component in the system allowed other portions of the system to be attacked. This resulted in gaining administrative access to the operating system desktop, decrypting further secrets and allowing network authentication. In addition, every device configured for an election stores the same key material used to ensure election integrity. As a result, once it is configured for and election, the compromise of any one portion of the system results in a loss of integrity for the entire election.

This attack could be conducted by a poll worker, elections official insider, or vendor insider. It affects all elements and configurations of the system.

Although CVSS has no prohibitions on static or shared secrets, the attacker’s ability to recover these secrets allowed unauthorized administrative access to all system components and results in a failure to meet CVSS 7.2.4.a. which states, “Voting systems shall ensure that only authorized roles, groups, or individuals have access to election data.”

### Unnecessary Applications Available on System

The system has two applications installed that were not strictly required and could be leveraged by an attacker for further exploitation. Hart has subsequently explained that one of these applications was deliberately left on the system for instances of disaster recovery on a damaged system and should not be removed. Gaining access to these applications only requires access to the underlying operating system, which is made possible by penetrating the physical security and exploiting the lack of full disk encryption.

A poll worker, elections official insider, or vendor insider are all capable of conducting this attack. It affects Verity Scan and all configurations of both servers and workstations in the system.

These applications fail to meet the definition of “authorized software” found in CVSS 7.4.6.a. which states, “Setup validation methods shall verify that only authorized software is present on the voting equipment. Authorized software is COTS software components needed to run the voting system and voting software components identified by the manufacturer as authorized.”

### Weak Authentication Encryption for Verity Key allowing unauthorized modification of election results

The system authenticates to the Verity Key via USB over a plaintext protocol. An attacker can recover the password either through code execution on the system or by inserting a USB sniffer into one of the exposed USB ports and triggering the application logic to transmit the authentication material. This is made possible by the lack of authentication of the Verity Key. There is no mechanism on the system to ensure the USB device inserted is a legitimate Verity Key device.

Additional encryption is performed on the key material stored on the Verity Key, however the weak encryption that protects the key material permits a brute force attack to gain access to all of the key material contained on the Verity Key that is needed to modify an election. No further information on this attack will be provided in this public report.

It would be possible for a poll worker, elections official insider or vendor insider to leverage this attack. It affects all of the devices and all configurations of the servers and workstations in the system.

The vulnerabilities described compromise the system’s ability to meet the requirements in CVSS 7.2.4.a. which states, “Voting systems shall ensure that only authorized roles, groups, or individuals have access to election data.”

### Code Execution via Untrusted Deserialization

The system uses an insecure serialization method to transfer data, and this data does not have any integrity checks. An attacker with access to the USB port on the system can provide malicious material that, when deserialized, can result in executing malicious code.

This attack could be conducted by a poll worker, elections official insider, or vendor insider. It affects Verity Scan, Verity Reader, standalone and networked configurations of the system.

The lack of integrity checks results in a failure to meet CVSS 5.2.8.a. which states, “All programmed devices shall check information inputs, whether from manual entry or other external source, for completeness and validity and ensure that incomplete or invalid inputs do not lead to irreversible error.”

## Attachment A – Inventory of Items Tested

| Device Name | Manufacturer and Model | Hart Serial Number | manufacturer Serial Number |
|---|---|---|---|
| Count Server | Hewlett Packard modelZ240 | D1700190106 | 2UA74526W8 |
| Count Client | Hewlett Packard modelZ240 | D1700191006 | 2UA74526WW |
| Count Standalone | Hewlett Packard modelZ240 | D170018906 | 2UA74526WP |
| Central Server | Hewlett Packard modelZ240 | D1700191406 | 2UA74526WR |
| Central Client | Hewlett Packard modelZ240 | D170018906 | 2UA7456WZ |
| Scanner | Canon Imagefourmula DR-G1100 | 001928 | GG307770 |
| Data Build Server | Hewlett Packard modelZ240 | D1700189806 | 2UA74526WV |
| Data Build Client | Hewlett Packard modelZ240 | D1700190206 | 2UA74526WD |
| Data Build Standalone | Hewlett Packard modelZ240 | D1700190706 | 2UA474526WX |
| Verity Scan | Hart InterCivic | X160104801 | |
| Tablet | | | 1701420411 |
| Ballot Box | Hart interCivic | 3005357 | |

## Attachment B – Attack Relationship Diagram