GRP Consulting Group, LLC

ALLEGHENY COUNTY PRE NOVEMBER 3, 2015 MUNICIPAL PRIMARY ELECTION

ES&S IVOTRONICS FIRMWARE VERIFICATION STUDY

FINAL REPORT

Developed for:

ALLEGHENY COUNTY

DIVISION OF ELECTIONS

STATE OF PENNSYLVANIA

Document Number GCG-AC-iVo-FRPT-000225

GRP Consulting Group, LLC

TABLE OF CONTENTS

1. INTRODUCTION: ALLEGHENY COUNTY ES&S IVOTRONICS FIRMWARE VERIFICATION STUDY

The Allegheny County, Pennsylvania Division of Elections requested GRP Consulting Group to audit and verify the firmware source code on twenty (20) ES&S iVotronic DRE voting machines before conducting the November 3, 2015 Municipal Primary Election. The devices to be audited were randomly selected from the counties 4700 devices. The purpose was to verify that the samples have in residence on the U1 designated Electronic Erasable Programmable Read Only Memory (EEPROM) chip the firmware version 9.1.4.1 and that all applied firmware versions are accurate and true to the State of Pennsylvania's Trusted Build as held in escrow by the Secretary of State's Office in Harrisburg. The study was accomplished by applying the *'Allegheny County iVotronic Firmware Verification Protocol'* process and was performed on location at the Allegheny County Division of Elections warehouse; located at 901 Pennsylvania Ave., Pittsburgh, Pennsylvania. GRP Consulting Group and Allegheny County staff performed this firmware audit on September 14, 2015.

It is the finding of GRP Consulting Group that the firmware verification audit applied to the resident code on the sample population was found to be unaltered versions of the 9.1.4.1 firmware.

1.1 Approach

1.1.1 Study's Focus

The focus of the exercise was:

1. Implementation of a fair and random selection process.

2. Deploy the verification protocol, known as the *'Allegheny County iVotronic Firmware Verification Protocol'*, to verify on twenty (20) randomly chosen ES&S iVotronics DRE voting devices that they hold in residence on the U1 designated EEPROM chip the exact, true and unaltered version of the 9.1.4.1 certified firmware source code as held in escrow at the Secretary of State's office.

1.1.2 Study's Concentration

The GRP Consulting Group has been tasked to independently apply a repeatable and validated verification protocol to verify that the ES&S firmware version 9.1.4.1 that resides

in escrow by the Secretary of State's office and is resident on the Allegheny County iVotronic Direct-Recording Entry (DRE) - touch screen voting devices – are exact, true and unaltered versions of the certified firmware source code.

1.1.3 Study's Phases

GRP Consulting Group organized the project primary phases, each incorporating the flexibility to accommodate additional requirements, as they may have become known. The general strategy employed was comprised of the following aspects:

1. Setup and configure the verification environment and the parameters associated with each verification cycle;

2. Apply the protocol to verify that before the November 3, 2015 Municipal Primary Election that the 9.1.4.1 firmware on the iVotronic DREs is the true and certified version of the firmware and has not been altered;

3. Execute twenty (20) verification cycles comprised of verification on performed one (1) ADA (American Disabilities Act) compliant iVotronic and nineteen (19) non-compliant DRE units;

4. Conduct reviews and analyses of all verification results and anomalies obtained during the twenty (20) verification execution cycles;

5. Advise the County on possible root cause(s) of any and all anomalies; and

6. Prepare and deliver reports of the verification activities, the results of all verification executions, and conclusions and recommendations in Executive Summary and Final Report formats.

1.2 Purpose

This document is the Allegheny County pre-November 3, 2015 Municipal Primary Election ES&S iVotronic Firmware Verification Study Final Report. This report was developed as a review of the specific technical details, the project's results, and findings.

1.3 Statement of Independence

As an election validation and verification business practice, GRP Consulting Group is technically, managerially, and financially independent from all electronic voting systems vendors as specified in *IEEE 1012-2004* Annex C.

The consultants of GRP Consulting Group shall maintain an independent decisional relationship between its clients, affiliates, or other organizations so that GRP Consulting Group's capacity to perform services objectively and without bias is not adversely affected.

GRP Consulting Group shall maintain independence in fact and in appearance. The validation and verification environment, whether on-site at GRP Consulting Group facilities or partner organizations or at a client's site, shall be organized so that staff members are not subjected to undue pressure or inducement that might influence their judgment or the results of their work.

1.4   References

1.   iVotronic Software Verification Protocols: Allegheny County Proposals; Collin Lynch, President, VoteAllegheny; 9/28/2008

2.   Firmware vs. Uploaded Firmware Chip Data Comparison Procedure; Election Systems and Software, Inc.; 1/18/2008

3.   Allegheny County iVotronic Firmware Verification Protocol; Geoffrey R. Pollich, SysTest Labs, 10/14/08

1.5   Systems Information

Items identified in Table 1 reflect firmware deployed at the Allegheny County Division of Elections warehouse on September 14, 2015:

Table 1 - Matrix of Firmware

Vendor	System	Description	Software/ Firmware Version
ES&S	iVotronic	Direct Record Entry	9.1.4.1
ES&S	iVotronic	ADA Compliant DRE	9.1.4.1

Equipment identified in Table 2 reflects iVotronic hardware selected at the Allegheny Division of Elections warehouse on September 14, 2015:

Table 2 - Matrix of Hardware

iVotronic Serial Number	Microchip Manufacturer	Microchip Part Number
-> V5184218	Spansion	0612FBE-G
-> V5186925	Spansion	0603FRD-G
-> V5184681	Spansion	0612FBE-G
-> V5180028	Spansion	0603FRC-G
-> V5176054	Spansion	0603FRC-G
-> V5182063	Spansion	0603FRC-G
-> V5182201	Spansion	0612EBA-G
-> V5182999	Spansion	0603FRC-G
-> V5186495	Spansion	0612FBE-G

iVotronic Serial Number	Microchip Manufacturer	Microchip Part Number
-> V5181572	Spansion	0603FBC-G
-> V5183170	Spansion	0612FBC-G
-> V5177048	Spansion	0603FRC-G
-> V5177589	Spansion	0603FRC-G
-> V5183860	Spansion	0612GBA-G
-> V5187171	Spansion	0609ERB-G
-> V5184183	Spansion	0612FBE-G
-> V5181316	Spansion	0612EBA-G
-> V5182346	Spansion	0603FRC-G
-> V5182562	Spansion	0612GBA-G
-> V5172691	Spansion	0446FBC-G

Table 3 - Matrix of Testing Hardware

Description	Manufacturer	Model
EEPROM Device Programmer	Logical Devices, Inc.	ChipMaster 6000XPu
Flash Module Programmer Adapter	Logical Devices, Inc.	Version 1
ESD Static Mat with wrist strap	N/A	N/A
#10 Tamper Proof Torx screwdriver	N/A	N/A
Small flathead screwdriver	N/A	N/A

Table 4 - Matrix of Testing Software

Description	Manufacturer	Software Version
Software- CHIPMASTER 6000 XPU for USB	Logical Devices, Inc	ChipMaster 6000Xpu for USB
WinLink2	Logical Devices, Inc	v. 01.51.00
Hex Editor	Xvi32	v. 2.5
Microsoft Visual C++, Binary Editor	Microsoft Corporation	Version 6.0
SHA_V Sha-1 and other SHA segments Hash Code Identification	Microsoft File Checksum Integrity Verifier (FCIV) **http://support.microsoft.com/kb/841290**	Version 2.05

2. ALLEGHENY COUNTY PRE NOVEMBER 3, 2015 MUNICIPAL PRIMARY iVOTRONIC FIRMWARE VERIFICATION PROCESS; PREFORMED SEPTEMBER 14, 2015

To establish a best practice protocol and verification procedure, Geoffrey Pollich, consultant with GRP Consulting Group, reviewed and analyzed the *VoteAllegheny: iVotronic Software Verification Protocols: Allegheny County Proposals,* the ES&S *Firmware vs. Uploaded Firmware Chip Data Comparison Procedure*, and NIST Standard Lab Procedures best practices. It was from these primary sources that the 'Allegheny County iVotronic Firmware Verification Protocol' was established.

2.1 Present during the September 14, 2015 Verification Process:

GRP Consulting Group:

Geoffrey Pollich – GRP Consulting Group, Principle Consultant

Allegheny County Division of Elections:

Mark Wolosik – Elections Division Manager
John O'Brien – Manager of Voting Machines
Elizabeth Dell – Business Analyst, Division of Computer Services

Election Advocacy Observers:

Ron Bandes – VoteAllegheny

2.2 Sample Size Randomization Procedure

The sample size must be carefully selected due the need to open the warranty seal over the lower left chassis screw in order to conduct the firmware verification. When this seal is broken, the DRE must be inspected and tested by ES&S. If a larger sample of machines were inspected per election, the availability of certified election machines may not satisfy the needs of individual precincts for federal, state, county, municipal and special issue elections held over the calendar year. It is also unclear if a larger sample sizes would yield a more valid result than the present sample size appropriately randomized.

Ron Brandes of VoteAllegheny along with Division of Election employees initiated the machine-selection effort to establish 20 randomly chosen iVotronic units for testing. Mark Wolosik, Elections Division Manager, John O'Brien, Manager of Voting Machines, Elizabeth Dell, Business Analyst, Division of Computer Services, and Geoffrey Pollich of the GRP Consulting Group believed the selection was consistent with a valid random selection process and was free of any and all mathematical bias.

3. Allegheny County Pre November 3, 2015 Municipal Primary Election ES&S iVotronic Firmware Verification Study Results

3.1 September 14, 2015 Results

08:30 – 9:30 am GRP Consulting Group and observers arrive at the Allegheny County warehouse facility to set up the verification work area; the Observer launches their randomization process

1. GRP Consulting Group unboxed the CHIPMASTER 6000 XPU EEPROM Programmer; the analyst setup the device to a GRP Consulting Group laptop; County Employees, and the Observer brought 20 randomly picked iVotronics into the verification work area to begin the firmware verification procedure.

09:31 Verify firmware procedure for iVotronic DRE #1

1. Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5184218 was selected.

2. Perform iVotronic Firmware Verify Procedure.

3. Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4. The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code:
   `(F6A8D4570988E2D159398503144E64D48F0CC69F).`

5. The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

09:34 Verify firmware procedure for iVotronic DRE #2

1. Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5186925 was selected.

2. Perform iVotronic Firmware Verify Procedure.

3. Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4. The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code:
   `(F6A8D4570988E2D159398503144E64D48F0CC69F).`

5. The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display

09:37   Verify firmware procedure for iVotronic DRE #3

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5184681 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

09:41   Verify firmware procedure for iVotronic DRE #4

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5180028 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

09:44   Verify firmware procedure for iVotronic DRE #5

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5176954 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display

09:49   Verify firmware procedure for iVotronic DRE #6

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5182063 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code:
     `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

09:52 Verify firmware procedure for iVotronic DRE #7

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5182201 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code:
     `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

09:55   Verify firmware procedure for iVotronic DRE #8

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5182999 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code:
     `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

09:59   Verify firmware procedure for iVotronic DRE #9

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5186495 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:03   Verify firmware procedure for iVotronic DRE #10

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5181572 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:05   Verify firmware procedure for iVotronic DRE #11

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5183170 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:08   Verify firmware procedure for iVotronic DRE #12

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n V5177048 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:12   Verify firmware procedure for iVotronic DRE #13

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5177589 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was an Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The AMD firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:16   Verify firmware procedure for iVotronic DRE #14

1.   Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5183860 was selected.

2.   Perform iVotronic Firmware Verify Procedure.

3.   Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4.   The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5.   The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:19 Verify firmware procedure for iVotronic DRE #15

1. Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5187171 was selected.

2. Perform iVotronic Firmware Verify Procedure.

3. Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4. The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5. The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:22 Verify firmware procedure for iVotronic DRE #16

1. Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->5184183 was selected.

2. Perform iVotronic Firmware Verify Procedure.

3. Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4. The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5. The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:25 Verify firmware procedure for iVotronic DRE #17

1. Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5181316 was selected.

2. Perform iVotronic Firmware Verify Procedure.

3. Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4. The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5. The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

GRP Consulting Group, LLC

10:27 Verify firmware procedure for iVotronic DRE #18

1. Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5182346 was selected.

2. Perform iVotronic Firmware Verify Procedure.

3. Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4. The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5. The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:33 Verify firmware procedure for iVotronic DRE #19

1. Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n ->V5182562 was selected. Perform iVotronic Firmware Verify Procedure.

2. Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

3. The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

4. The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.

10:36 Verify firmware procedure for iVotronic DRE #20

1. Randomly select an iVotronic DRE from the warehouse for the firmware verification procedure; s/n V51772691 was selected. (*ADA Device*)

2. Perform iVotronic Firmware Verify Procedure.

3. Upon opening of iVotronic DRE, the removable CMOS was a Spansion CMOS part S29AL016D90TF101, and the CHIPMASTER 6000 XPU EEPROM programmer was used to read and save the binary firmware code.

4. The Spansion firmware chip was successfully read into the PC and the hash code generated did match the trusted build hash code: `(F6A8D4570988E2D159398503144E64D48F0CC69F)`.

5. The iVotronic DRE was closed and powered by County employees to verify that the DRE was working properly with the correct firmware date, time, and version number showing on the initial display.
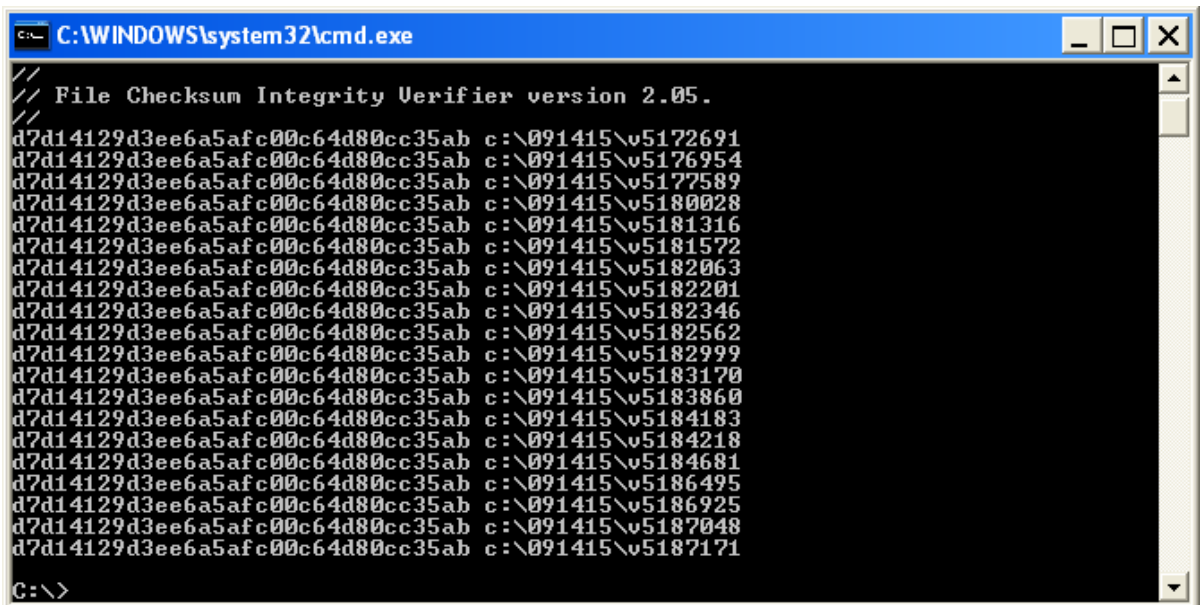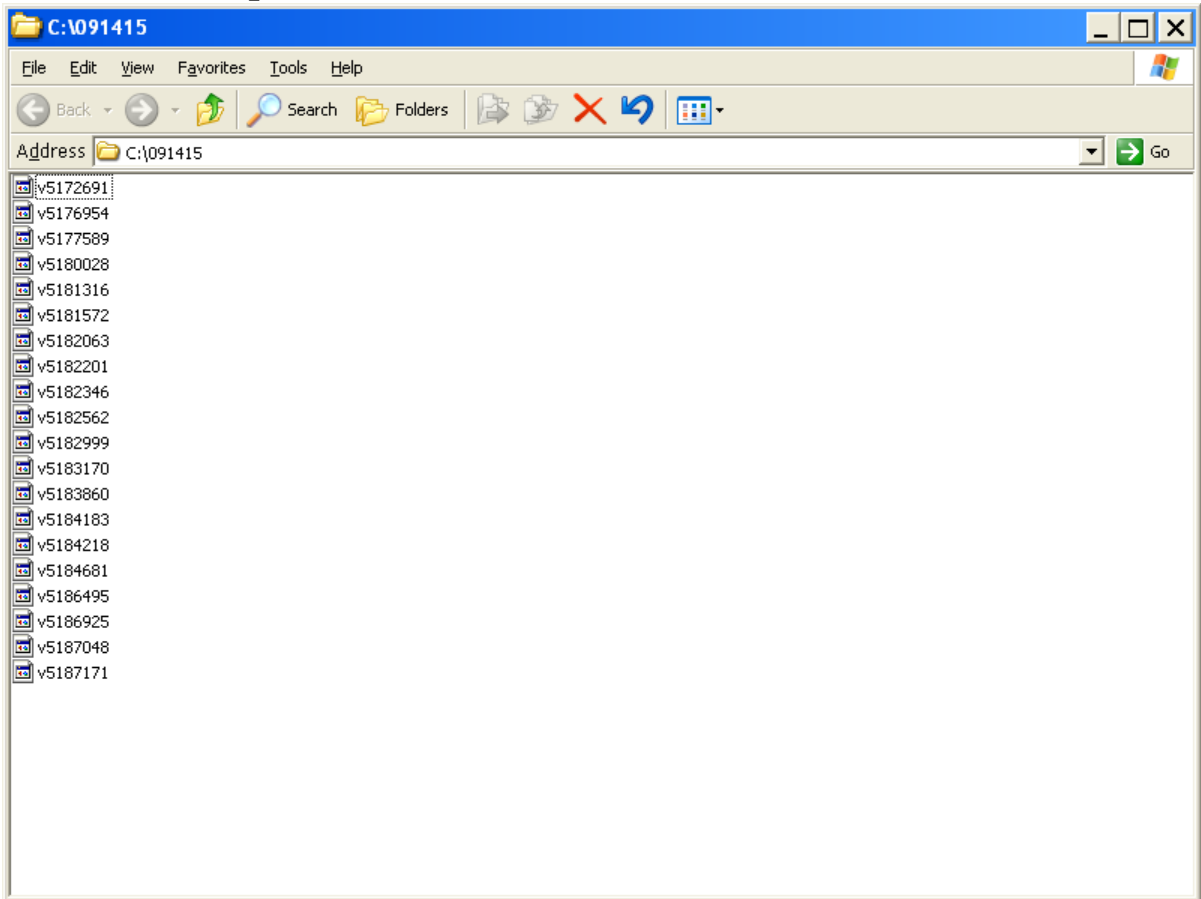
3.2 September 14, 2015 Collective Firmware Files

```
C:\091415                                                    _ □ ×

File   Edit   View   Favorites   Tools   Help

  Back        Search   Folders

Address  C:\091415                                          Go

  v5172691
  v5176954
  v5177589
  v5180028
  v5181316
  v5181572
  v5182063
  v5182201
  v5182346
  v5182562
  v5182999
  v5183170
  v5183860
  v5184183
  v5184218
  v5184681
  v5186495
  v5186925
  v5187048
  v5187171
```

```
C:\WINDOWS\system32\cmd.exe                                 _ □ ×

//
// File Checksum Integrity Verifier version 2.05.
//
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5172691
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5176954
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5177589
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5180028
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5181316
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5181572
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5182063
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5182201
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5182346
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5182562
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5182999
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5183170
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5183860
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5184183
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5184218
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5184681
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5186495
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5186925
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5187048
d7d14129d3ee6a5afc00c64d80cc35ab c:\091415\v5187171

C:\>
```

4. FINDINGS

GRP Consulting Group was engaged by the Allegheny Division of Elections on site at 901 Pennsylvania Ave., Pittsburgh, PA on September 14, 2015; the purpose of the engagement was to apply the '*Allegheny County iVotronic Firmware Verification Protocol'* to verify the ES&S iVotronic firmware version 9.1.4.1 is resident on the Allegheny County iVotronic population.

On September 14, 2015, the GRP Consulting Group analyst completed the verification process of the firmware residing on twenty (20) Allegheny County ES&S iVotronics Direct-Recording Entry electronic voting machines chosen at random from the population of approximately 4700 iVotronic Direct-Recording Entry (DRE) electronic voting machines. It is the findings of GRP Consulting Group that the firmware version 9.1.4.1 residing on the twenty (20) randomly chosen DRE electronic voting machines, do represent the population, and furthermore; the firmware version as resident on the U1 designated Electronic Erasable Programmable Read Only Memory (EEPROM) chip is an exact, true, and unaltered version of the NVLAP federally certified trusted build as held in archive at SysTest Labs in Denver, Colorado and in escrow by the Pennsylvania Secretary of State in Harrisburg, PA.

5. APPENDIX A - TERMS AND ABBREVIATIONS

These terms and abbreviations will be used throughout this document:

Table 2 - Matrix of Terms & Abbreviations

Terms & Abbreviation	Description
Binary	The system of representing text or computer processor instructions by the use of a two digit number system. This system is composed of only the number zero, representing the off state, and the number one, representing the on state, combined in groups of 8. These groups of 8 bits can represent up to 256 different values and can correspond to a variety of different symbols, letters or instructions.
DOE	Division of Elections
DRE	Direct-Recording Entry - touch screen voting device
Firmware	Firmware is the programmable content of a hardware device, which can consist of machine language instructions for a processor or configuration settings for a fixed-function device, gate array or programmable logic device. A common feature of firmware is that it can be updated post-manufacturing, either electronically, or by replacing a storage medium such as a socketed memory chip.
Hardware	Hardware refers to the physical artifacts of a technology such as the physical components of a computer system
Hash Code	A hash function is a well-defined procedure or mathematical function for turning binary code into a relatively small integer that serves as a unique mathematical footprint.
ITA	Independent Test Authority
iVotronic	ES&S touch screen voting terminal
Protocol	Rules governing process conduct to a written instruction.
Trusted Build	Unaltered, true, and certified complied binary code.
SHA-1	Algorithm used to define the hash code value.
Software	Computer software is human interfacing computer programs, procedures and documentation that perform defined task on a computer system. The term includes application software that performs productive tasks for users, system software such as operating systems, which interface with hardware to provide the necessary services for application software.
Voting System Components	The units of equipment (server platform, DRE voting terminal, ballot scan device) when used together create a voting system.
Verification	The act of reviewing, inspecting, and/or testing to establish and document

Terms & Abbreviation	Description
	that a product, service, or system meets the regulatory, standard, or specification requirements.

End of Report