Forensic Audit Report

Report Number: MCA-21001-AR-01

Dominion Voting Systems, Democracy Suite 5.5B

Report Rev 1.0

[February 23, 2021]

Prepared for: **Maricopa County Elections Department**

Prepared by:

SLI Compliance®
4720 Independence St.
Wheat Ridge, CO
80033
(303) 422-1566
www.SLICompliance.com

SLI Compliance, a Division of Gaming Laboratories International LLC

Revision History

Date	Release	Author	Revision Summary
February 23, 2021	1.0	M. Santos	Initial release

Disclaimer

The observations and conclusions reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items evaluated.

All evaluation conducted for this engagement has been done outside of the U.S. Election Assistance Commission's (EAC) Test and Certification Program. In no way does this report represent an EAC certification against the Voluntary Voting System Guidelines (VVSG) or any other standard.

The audit activities referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items evaluated. Actual results in other environments may vary.

Contents

1 Introduction

SLI Compliance is submitting this report as a summary of forensic auditing efforts, solicited by Maricopa County Elections Department. The forensic audit conducted consisted of an analysis and review of the voting system equipment used in the November 3rd, 2020 presidential election and records from that election, to extract facts about the use of the Dominion Voting Systems Democracy Suite 5.5B voting system.

The Maricopa County forensic audit was conducted on the Dominion Democracy Suite (DS) 5.5B system and included examination of the following items per direction given by Maricopa County Elections Department:

- 100% (9) of the County's central count tabulators (ICC) (4 Hi-Pro high-speed scanners and 5 Cannon high-speed scanners), which are used for processing large quantities of ballots.
- 100% (4) workstations and (2) servers used to operate the election management system (EMS), which includes pre-election functions for creating the election definition for the specified election, as well as post-election activities including accumulating, tallying and reporting election results.
- 10% sample (35) of the County's 350 precinct-based tabulators (ICP2s) that were utilized in the election, at the polling centers.
- 20% sample (4) of 20 adjudication stations, which allow ballots with exceptions or outstack conditions such as over-votes, blank ballots, write-ins and marginal marks, to be resolved**.**

This effort included verification of the following items:

1. Verifying that the software installed on the tabulation equipment is the same as the software certified by the U.S. Election Assistance Commission and the Arizona Secretary of State.

   This item is applicable to ICP2 (precinct scanner), EMS (election management system – workstations and servers), ICC (central count system) and Adjudicator (ballot resolver).

2. Verifying that no malicious software is running on the component.

   This item is applicable to ICP2 (precinct scanner), EMS (election management system – workstations and servers), ICC (central count system) and Adjudicator (ballot resolver).

3. Verifying that the components are not connected to the internet and that they have not been connected to the internet during the period of July 6, 2020 through November 20, 2020.

This item is applicable to ICP2 (precinct scanner), EMS (election management system – workstations and servers), ICC (central count system) and Adjudicator (ballot resolver).

4. Performing a physical audit of the components to verify there is no unexpected hardware (a sample of 5 ICP2 precinct scanners).

   This item is applicable to ICP2 (precinct scanner).

Below is a listing of when each item above was completed for each relevant component.

For Item #1, verifying **component hashes against EAC generated hashes**:

- Item #1 was complete for ICP on Day 1
- Item #1 was complete for EMS workstations on Day 3
- Item #1 was complete for EMS servers on Day 5
- Item #1 was complete for ICC on Day 3
- Item #1 was complete for Adjudicator on Day 3

For Item #2, verifying **that no malicious software is running on the component**:

- Item #2 was complete for ICP on Day 3
- Item #2 was complete for EMS workstations on Day 4
- Item #2 was complete for EMS servers on Day 4
- Item #2 was complete for ICC on Day 5
- Item #2 was complete for Adjudicator on Day 4

For Item #3, verifying components **are not connected to the internet**:

- Item #3 was complete for ICP on Day 3
- Item #3 was complete for EMS workstations on Day 4
- Item #3 was complete for EMS servers on Day 5
- Item #3 was complete for ICC on Day 5
- Item #3 was complete for Adjudicator on Day 4

For Item #4, verifying **physical audit of the ICP component**:

- Item #4 was complete for ICP on Day 1

This audit was performed at a Maricopa County Election Department facility, located at 510 South 3rd Avenue, Phoenix, Arizona, over a five day period, from February 8th to February 12th, 2021.

- Attachments included are as listed:
  - Attachment A – Hashes by Component
  - Attachment B – User Activity and Malicious Software Review
  - Attachment C – Networking Review Criteria

2 Process

SLI Compliance conducted the forensic audit in a way that maximized efficiencies in examining the election artifacts.

The process included creation of raw disk images that allowed the examiners to audit and analyze the systems without the risk of changing the original system environments. Once the system media was imaged using a bit-to-bit copy of each item of system media, the examiners were able to mount and use forensic tools to inspect the systems for indicators of internet connectivity, as well as indicators of malicious or unauthorized software present on the systems.

Due to the County's strict policies regarding maintenance of the election infrastructure air gap, where election related devices are not allowed to be connected to non-election devices, SLI Compliance had to demonstrate the ability to prevent write back to any election media or resources. To fulfill this requirement, SLI Compliance utilized the WriteProtect™-BAY technology to prevent contamination of any of the election media during the forensic audit.

The WriteProtect™-BAY technology provides read-only, write blocking technology at a hardware layer, preventing inadvertent modification of election media during the audit. The WriteProtect™-BAY provides multiple write protected ports that allow for a wide variety of storage media to be connected in a read only write protected manner.

Examination for Item #1, verification of hashes, included usage of

- Md5deep hashing application, resident on auditing workstation with a Win10 operating system, for hashing extracted files utilizing a Sha256deep algorithm
- MS Excel spreadsheet utilizing comparison formulas, for comparing and determining if files have matching hash codes

Examination for Item #2, checking for malicious software, included usage of

- ClamWin Antivirus checks for software threats including viruses and spyware (utilizing engine version 0.99.4)
- Malwarebytes protection against software threats like viruses, malware, and spyware (utilizing component package version 1.0.1157, update package version 1.0.1157)
- Microsoft Defender Antivirus protection against software threats like viruses, malware, and spyware (utilizing security intelligence version 1.331.708.0)
- ESET Endpoint Antivirus protection against software threats including malware, viruses, worms and spyware (ESET Antivirus 7.3.2044.0)
- OSForensics, a digital examination tool that extracts data, including hidden data, from a PC
- Manual review utilizing a malicious software review checklist
- For the EMS servers, due to their configuration, a different antivirus, Avast, was utilized for examination

Examination for Item #3, internet connectivity check, included usage of

- OSForensics, a digital examination tool that extracts data, including hidden data, from a PC
- Manual review utilizing an internet connectivity review checklist

Examination for Item #4

- Four ICP2 devices were opened to show the internal components resident within
- A fifth ICP2 device was opened and all components removed from the chassis for a full examination of each internal component

3 Examination

This section details the proceedings of the examination, as conducted onsite at the Maricopa County Elections Department facilities.

Day 1

- Out of a pool of 315 available ICP2 precinct scanners (35 had been examined in a previous audit), SLI Compliance examined each and selected 35 ICP2s, based, in part, on any anomalies noticed on devices. This included missing labels or seals. Note: Due to defective batteries that would not attain the 10% minimal charge needed to operate the device, five of the ICP2s originally selected would not power up, so they were replaced by five other ICP2s.

- Out of a pool 16 available Adjudication workstations (4 had been examined in a previous audit), SLI Compliance selected 4 Adjudication workstations.
- SLI Compliance auditors then recorded serial numbers of each of the 35 ICP2s, 4 adjudication workstations, all 9 of Maricopa County's ICC central count stations and all 4 Maricopa County EMS workstations, and 2 EMS servers. All labels and seals which had an associated serial number were recorded as well.
- To capture a full data set of the environments being examined, and to prevent contamination of the environments, SLI Compliance performed cloning operations on all workstations and all Administrator SD cards collected from the ICP2 devices.
- Dominion voting system files were extracted from the 35 ICP2s to validate against EAC generated hash codes, which are used to validate that each file's content has not been modified.
- The files were then hashed and compared to the EAC generated hash codes and verified to match. This verified **Item #1** for the 35 evaluated **ICP2** components.
- Cloning of the 4 Adjudicator workstations was initiated and completed.
- Cloning of the 9 ICC workstations was initiated.
- Physical audit of 5 ICP2s was conducted to verify no unexpected hardware was resident within the device. This verified **Item #4** for the **ICP2** components.
- The ICP2 contains an internal SD card that contains all information resident on the ICP2. That card was removed and examined to verify that no unexpected or malicious items were resident. Contents were also compared to artifacts that were extracted earlier as part of the Dominion file extraction process. All artifacts matched as expected.

Day 2

- Cloning of the 9 ICC workstations was completed.
- It was determined that the audit log (needed for review for determination of any connections to the internet) was resident on both the Administrator SD card and the Pollworker SD card. As the Pollworker card is the card pulled during election activities for results determinations, SLI Compliance auditors utilized the Administrator SD card. These cards were pulled and cloned, and then the audit log was obtained.
    - Note that six of the sampled ICP2 devices did not have SD cards. Maricopa County personnel informed the auditors that when a device needs to be replaced, the cards are pulled and utilized in the replacement device. Documentation was provided by the County for five of the ICP2 devices as

being replaced in the field. These devices were replaced due to tabulators not powering on, or needing to be replaced due to ball point pens being used which smeared the mylar screen on the scanner. The County indicated that the sixth device was prepared as a spare unit, but was never utilized in the election, and thus never had SD cards inserted.

- Review of ICP2 logs for any internet connections was initiated.
- Review of ICP2 files for any unknown/malicious software was initiated.
- Review of Adjudicator workstation logs for any internet connections was initiated.
- Review of Adjudicator workstation files for any unknown/malicious software was initiated.

Day 3

- Dominion voting system files were extracted from the four Adjudicator workstation cloned images to validate against EAC generated hash codes, which are used to validate that each file's content has not been modified.
- The Adjudicator workstation files were then hashed and compared to the EAC generated hash codes and verified to match. This verified **Item #1** for the 4 evaluated **Adjudicator** workstation components.
- Dominion voting system files were extracted from the nine ICC workstation cloned images to validate against EAC generated hash codes, which are used to validate that a files content has not been modified.
- The ICC workstation files were then hashed and compared to the EAC generated hash codes and verified to match. This verified **Item #1** for the 4 evaluated **ICC** workstation components.
- Review of ICP2 files for any unknown/malicious software was completed. This verified **Item #2** for the **ICP2** components.
- Review of ICP2 logs for any internet connections was completed. This verified **Item #3** for the **ICP2** components.
- Dominion voting system files were extracted from the four EMS workstation cloned images to validate against EAC generated hash codes, which are used to validate that each file's content has not been modified.
- The EMS workstation files were then hashed and compared to the EAC generated hash codes and verified to match. This verified **Item #1** for the 4 evaluated **EMS workstation** components.

Day 4

- Review of EMS files for any unknown/malicious software was completed. This verified **Item #2** for the **EMS workstation** components.
- Review of EMS logs for any internet connections was completed. This verified **Item #3** for the **EMS workstation** components.
- Dominion voting system files were extracted from the two EMS servers to validate against EAC generated hash codes, which are used to validate that each file's content has not been modified.
- The EMS server files were then hashed and compared to the EAC generated hash codes and verified to match. This verified **Item #1** for the 2 evaluated **EMS server** components.
- Review of Adjudicator files for any unknown/malicious software was completed. This verified **Item #2** for the **Adjudicator** components.
- Review of Adjudicator logs for any internet connections was completed. This verified **Item #3** for the **Adjudicator** components.

Day 5

- Review of EMS server files for any unknown/malicious software was completed. This verified **Item #2** for the **EMS server** components.
- Review of EMS server logs for any internet connections was completed. This verified **Item #3** for the **EMS server** components.
- Review of ICC files for any unknown/malicious software was completed. This verified **Item #2** for the **ICC** components.
- Review of ICC logs for any internet connections was completed. This verified **Item #3** for the **ICC** components.

4 Audit Findings Determinations

This section identifies the determinations for each review criterion, covering the relevant DS 5.5B components.

Item #1 Verifying that the software installed on the tabulation equipment is the same as the software that was certified by the U.S. Election Assistance Commission and the Arizona Secretary of State.

ICP2 (precinct scanner)

Each of the 35 ICP2s that were examined had the voting system files extracted following the Dominion prescribed procedure. Those files were then hashed, with the md5deep tool, and compared to the relevant EAC hash codes, which determined that the Dominion Voting Systems files remained unmodified from the certified files.

For the five ICP2s that were opened for Item #4, the internal SD cards were compared to the extracted files and were verified to match.

The Internal SD cards were bit-by-bit cloned, and then the image was restored onto duplicate SD cards for examination with Kali Linux 2020.4. This allowed the examiners to determine that the files contained on the internal SD storage cards matched those that were extracted using the Dominion defined hash verification methods.

EMS (election management system – workstations and servers)

Each of the six EMSs that were examined had all voting system files extracted. Those files were then hashed with the md5deep tool and compared to the relevant EAC hash codes, which determined that the Dominion Voting Systems files remained unmodified from the certified files.

Each of the four EMS client systems were first bit-by-bit imaged, and then the images were mounted read-only for file extraction and verification. This allowed the examiners to maintain a clean snapshot of the EMS client systems under evaluation.

The EMS servers contained encrypted raid drives that didn’t allow for bit-by-bit media imaging, so the EMS servers had to be examined under the close scrutiny of County officials, including maintaining strict air-gap policies for introduction of clean media into the environment. This included monitored use of brand-new USBs (witnessed to be removed from original packaging) to obtain election software for verification.

ICC (central count system)

Each of the nine ICCs that were examined had all voting system files extracted. Those files were then hashed with the md5deep tool and compared to the relevant EAC hash codes, which determined that the Dominion Voting Systems files remained unmodified from the certified files.

Each of the nine ICC client systems were first bit-by bit-imaged, and then the images were mounted read-only for file extraction and verification. This allowed the examiners to maintain a clean snapshot of the ICC client systems examined. It should be noted that additional hardware was required to process and image M.2 NVMe drive technology. All ICC systems were successfully imaged using the WriteProtect™-BAY technology.

Adjudicator (ballot resolver)

Each of the four Adjudicators that were examined had all voting system files extracted. Those files were then hashed with the md5deep tool and compared to the relevant EAC hash codes, which determined that the Dominion Voting Systems files remained unmodified from the certified files.

Each of the four Adjudication client systems were first bit-by-bit imaged, and then the images were mounted read-only for file extraction and verification. This allowed the examiners to maintain a clean snapshot of the Adjudication client systems examined.

No modifications were found by SLI Compliance to the installed Dominion software from the EAC certified release.

Item #2: Verifying that no malicious software is running on the component.

ICP2 (precinct scanner)

All files on each of the ICP2s were examined to determine if any malicious files were resident. Four different antivirus scanners were utilized (Windows Defender, ESET Endpoint Protection, ClamWin and Malwarebytes), as well OSForensics, a digital forensics tool, to examine the contents of each component.

No instance of malicious software was found on any of the devices.

In addition to using multiple forms of antivirus and malicious software detection software, the verification of all of the systems' software against trusted hash repositories stored by the Election Assistance Commission determined that no unexpected files or processes were present on the ICP2 Systems.

EMS (election management system)

All files on each of the EMSs were examined to determine if any malicious files were resident. On the four workstations, four different antivirus scanners were utilized (Windows Defender, ESET Endpoint Protection, ClamWin and Malwarebytes), as well OSForensics, a digital forensics tool, to examine the contents of each component.

In addition to using multiple forms of antivirus and malicious software detection software, manual examination of the systems was conducted to identify malicious or unauthorized software on the systems. These inspections included:

1) Inspection of the system registry. This included items such as Windows 'Run' entries, most recently used programs, recent documents, and Windows Explorer last visit.

2) Inspection of the system file system and installed programs: installed programs, autorun commands, shellbag entries, Windows userassist, download history, and USB history.

3) Inspection of the system audit logs. Includes Windows event logs, browser history, search terms, website logins, Windows timeline events, and host system antivirus logs.

On the two servers, Avast antivirus was utilized, as well OSForensics, a digital forensics tool, to examine the contents of each component. The examination of the EMS servers was performed manually, and all information for the EMS servers was pulled manually, for export and examination with the OSForensics tool on a separate system.

No instance of malicious software was found on any of the devices.

ICC (central count system)

All files on each of the ICCs were examined to determine if any malicious files were resident. On the four workstations, four different antivirus scanners were utilized (Windows Defender, ESET Endpoint Protection, ClamWin and Malwarebytes), as well OSForensics, a digital forensics tool, to examine the contents of each component.

In addition to using multiple forms of antivirus and malicious software detection software, manual examination of the systems was conducted to identify malicious or unauthorized software on the systems. These inspections included:

1) Inspection of the system registry. This included items such as Windows ‘Run’ entries, most recently used programs, recent documents, and Windows Explorer last visit.

2) Inspection of the system file system and installed programs: installed programs, autorun commands, shellbag entries, Windows userassist, download history, and USB history.

3) Inspection of the system audit logs. Includes Windows event logs, browser history, search terms, website logins, Windows timeline events, and host system antivirus logs.

No instance of malicious software was found on any of the devices.

Adjudicator (ballot resolver)

All files on each of the ICCs were examined to determine if any malicious files were resident. On the four workstations, four different antivirus scanners were utilized (Windows Defender, Endpoint, ClamWin and Malwarebytes), as well OSForensics, a digital forensics tool, to examine the contents of each component.

In addition to using multiple forms of antivirus and malicious software detection software, manual examination of the systems was conducted to identify malicious or unauthorized software on the systems. These inspections included:

1) Inspection of the system registry. This included items such as Windows ‘Run’ entries, most recently used programs, recent documents, and Windows explorer last visit.

2) Inspection of the system file system and installed programs: installed programs, autorun commands, shellbag entries, Windows userassist, download history, and USB history.
3) Inspection of the system audit logs. Includes Windows event logs, browser history, search terms, website logins, Windows timeline events, and host system antivirus logs.

No instance of malicious software was found on any of the devices.

SLI Compliance found no malicious software components on the installed software.

Item #3: Verifying that the components are not connected to the internet and that they have not been connected to the internet during the period of July 6, 2020 through November 20, 2020.

ICP2 (precinct scanner)

Manual examination and usage of the tool OSForensics, a digital forensics tool, were used to examine the activities of each ICP2 component, looking to determine if any connections were made to the internet, with primary focus on the time period of July 6, 2020 through November 20, 2020.

Manual examination and the OSForensics software were used to inspect the systems to identify if there were any instances of the systems being connected to an internet routed network. These inspections included:

1) Manual examination of the ICP2's storage partitions including the "ICP2-Boot" and "ICP2-Data" for logfiles, connection strings, ethernet callouts.
2) Inspection of the system file system and installed programs, extraction and examination of the squashfs system files.
3) Inspection of the system audit logs including the election logs, system logs and the system's diagnostic logs.
4) Searched for ethernet, modem, and wireless connectivity settings.
5) Examination and research for WLAN, ethernet and modem connectivity, logs, configuration, and usage.

No evidence of internet connectivity was found.

EMS (election management system)(workstations and servers)

OSForensics, a digital forensics tool, was used to examine the activities of each EMS component, looking to determine if any connections were made to the internet, with primary focus on the period of July 6, 2020 through November 20, 2020.

OSForensics software was used to inspect the systems to identify if there were any instances of the systems being connected to an internet routed network. These inspections included:

1) Inspection of the system registry. This included items such as Windows 'Run' entries, most recently used programs, recent documents, and Windows Explorer last visit.
2) Inspection of the system file system and installed programs: installed programs, autorun commands, shellbag entries, Windows userassist, and download history.
3) Inspection of the system audit logs; includes Windows event logs, browser history, search terms, website logins, and Windows timeline events.
4) USB history, to determine if there were any unauthorized wireless or USB ethernet devices plugged in and to determine if the systems were connected to an unauthorized network connection via a USB device.

In the case of the EMS server systems for which the OSForensics tools could not be utilized due to the air-gap policy, all of the information was manually examined.

1) Inspection of the system registry. This included items such as Windows 'Run' entries, most recently used programs, recent documents, and Windows Explorer last visit.
2) Inspection of the system file system and installed programs: installed programs, autorun commands, shellbag entries, Windows userassist, and download history.
3) Inspection of the system audit logs; includes Windows event logs, browser history, search terms, website logins, and Windows timeline events.
4) USB history, to determine if there were any unauthorized wireless or USB ethernet devices plugged in and to determine if the systems were connected to an unauthorized network connection via a USB device.
5) Examination and research for WLAN connectivity.
6) Verification of the server's ARP tables, routing lists, established connections, DNS server configurations, and netstat information.

No evidence of internet connectivity was found.

ICC (central count system)

OSForensics, a digital forensics tool, was used to examine the activities of each ICC component, looking to determine if any connections were made to the internet, with primary focus on the time period of July 6, 2020 through November 20, 2020.

OSForensics software was used to inspect the systems to identify if there were any instances of the systems being connected to an internet routed network. These inspections included:

1) Inspection of the system registry. This included items such as Windows ‘Run’ entries, most recently used programs, recent documents, and Windows Explorer last visit.
2) Inspection of the system file system and installed programs: installed programs, autorun commands, shellbag entries, Windows userassist, and download history.
3) Inspection of the system audit logs; includes Windows event logs, browser history, search terms, website logins, and Windows timeline events.
4) USB history, to determine if there were any unauthorized wireless or USB ethernet devices plugged in and to determine if the systems were connected to an unauthorized network connection via a USB device.

One ICC had a log entry of a connection attempt, with no corresponding DNS failure message, on August 26, 2020. The connection attempt itself was a search for how to adjust screen brightness. Examination of all other log files on that machine did not provide evidence of a successful internet connection.

No evidence of internet connectivity was found. Such evidence would have been found if the system had been connected to the internet.

Adjudicator (ballot resolver)

OSForensics, a digital forensics tool, was used to examine the activities of each Adjudicator component, looking to determine if any connections were made to the internet, with primary focus on the time period of July 6, 2020 through November 20, 2020.

OSForensics software was used to inspect the systems to identify if there were any instances of the systems being connected to an internet routed network. These inspections included:

1) Inspection of the system registry. This included items such as Windows ‘Run’ entries, most recently used programs, recent documents, and Windows Explorer last visit.
2) Inspection of the system file system and installed programs: installed programs, autorun commands, shellbag entries, Windows userassist, and download history.
3) Inspection of the system audit logs; includes Windows event logs, browser history, search terms, website logins, and Windows timeline events.
4) USB history, to determine if there were any unauthorized wireless or USB ethernet devices plugged in and to determine if the systems were connected to an unauthorized network connection via a USB device.

No evidence of internet connectivity was found.

SLI Compliance found there to be no internet connectivity occurring within the specified time period (July 6, 2020 through November 20, 2020) on any of the examined components.

Item #4: Performing a physical audit of the components to verify there is no unexpected hardware (5 ICP2 precinct scanners).

Physical examination of the ICP2 component included removal of the outer cover, as well an inner cover to expose the resident circuit boards and accompanying components on four ICP2s. A fifth ICP2 precinct scanner was taken even further, such that all components were completely removed from the chassis for examination.

The examination showed that there were no physical components resident that were not expected to be there.

SLI Compliance's findings indicate that the installed hardware is the hardware that was certified as part of the EAC certification and that none of the examined components contains any malicious or unexpected hardware components.

5 Summary Findings

SLI Compliance has completed the audit of the Dominion Voting Systems Democracy Suite 5.5B voting system components as prescribed by the Maricopa County Elections Department.

SLI Compliance maintained the integrity of the audited system components by performing a bit-by-bit image of all systems examined by SLI Compliance, except for the two EMS servers that were live systems. Unused media from original packaging was used to remove or extract data from the live systems. In all instances when removing or examining system storage media, the County required that proof of write back protection be demonstrated, to protect the election infrastructure's air-gapped environment.

Physical examination of the County election infrastructure indicated that the physical setup of the systems is arranged so that all network connectivity is clearly marked and delineated. This means that, at any time, observers can examine and determine that the election systems are connected only to authorized networking. Separate cable runs are positioned to clearly identify all network cabling to and from election devices, and cables are color coded for easy identification. In addition, the entire election area is fully covered by cameras that may be used for observing the election process and maintaining a historic record of events on the election processing floor.

While the systems examined showed no malicious or networking related USB devices being connected, the systems examined didn't provide a physical or a digital method of preventing unauthorized USB devices to the systems. In this particular case, County policy drives control of USB connectivity.

For the four items being examined,

1. Verifying that the software installed on the tabulation equipment is the same as the software that was certified by the U.S. Election Assistance Commission and the Arizona Secretary of State.

This item is applicable to ICP2 (precinct scanner), EMS (election management system – workstations and servers), ICC (central count system) and Adjudicator (ballot resolver).

SLI Compliance's findings indicate that the installed Dominion software remains unmodified from the EAC certified release.

2. Verifying that no malicious software is running on the component.

   This item is applicable to ICP2 (precinct scanner), EMS (election management system – workstations and servers), ICC (central count system) and Adjudicator (ballot resolver).

   SLI Compliance's findings indicate that the installed software does not contain any malicious software components.

3. Verifying that the components are not connected to the internet and that they have not been connected to the internet during the period of July 6, 2020 through November 20, 2020.

   This item is applicable to ICP2 (precinct scanner), EMS (election management system – workstations and servers), ICC (central count system) and Adjudicator (ballot resolver).

   One ICC had a log entry of a connection attempt, with no corresponding DNS failure message, on August 26, 2020. Examination of all other log files on that machine did not provide evidence of a successful internet connection. No other component examined had any anomalies.

4. Performing a physical audit of the components to verify there is no unexpected hardware (5 ICP2 precinct scanners).

   This item is applicable to ICP2 (precinct scanner).

   SLI Compliance's findings indicate that the installed hardware is only the hardware that was certified as part of the EAC certification and that none of the examined components contains any malicious or unexpected hardware components.

End of Forensic Audit Report