Technical Evaluation Report

Pinal County Arizona Audit of the Election Systems & Software (ES&S) EVS 6300 Voting System

Approved by: Michael L. Walker

Michael L. Walker, Program Manager

October 8, 2024

Disclaimer: This campaign was tested by an EAC accredited VSTL to applicable standards of the VVSG. All testing and references were performed outside of the EAC Test and Certification Program.

v. TR-01-03-SAW-01.01

1.0 INTRODUCTION

The purpose of this report is to document the procedures that Pro V&V, Inc. followed to perform a technical evaluation of the Election Systems & Software (ES&S) EVS 6.3.0.0 Voting System for Pinal County, Arizona. Pro V&V has prepared this report as a summary of the technical evaluation efforts as detailed in Pro V&V Quotation No. 01-03-SAW-2024-01.

This effort included verification of the following items:

1. Verifying that the software installed on the county DS950 and DS850 tabulators is the same as the software certified by the U.S. Election Assistance Commission and the State of Arizona and exported and reviewed audit logs.

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

3. Verifying that the components were properly connected to their local network and were not maliciously connected to any other network..

4. File and activity analysis. Verify no files were maliciously manipulated either manually or electronically through file and activity analysis.

1.1 References

The documents listed below were utilized in the development of this Report:

- Pro V&V Quotation No. 01-03-SAW-2024-01
- Election Assistance Commission Testing and Certification Program Manual, Version 2.0
- Election Assistance Commission Voting System Test Laboratory Program Manual, Version 2.0
- National Voluntary Laboratory Accreditation Program NIST Handbook 150, 2020 Edition, "NVLAP Procedures and General Requirements (NIST Handbook 150)", dated July 2020
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2017 Edition, "Voting System Testing (NIST Handbook 150-22)", dated July 2017
- Pro V&V, Inc. Quality Assurance Manual

1.2 Terms and Abbreviations

The terms and abbreviations applicable to the development of this Test Report are listed below:

"EAC" – United States Election Assistance Commission

"EMS" – Election Management System

"ESS" – Election Systems & Software

"QA" – Quality Assurance

"VSTL" – Voting System Test Laboratory

1.3 Background

Snell and Wilmer Law Office contracted with Pro V&V to conduct a technical evaluation of the deployed back-office configuration components of the EVS 6.3.0.0 Voting System. These components are used to operate the election management system (EMS) that provides end-to-end election management activities for EVS6300. These activities include pre-election functions for creating the election, defining contests, candidates and ballot formats and performing post-election results processing including accumulating, tallying and reporting election results.

The components evaluated were the EMS Server, Backup EMS Server, and two EMS Workstations components.

For the evaluation, the following information is pertinent:

- Expert's name, address, and qualifications

  Mancy Hammond of Pro V&V
  6705 Odyssey Drive NW
  Suite C
  Huntsville, AL 35806
  CompTIA A+, Network+, Security+, and Linux+ certified

- Subject matter of the report

  Technical analysis of hard drives from election machines.

- Substance of the facts and opinions of the expert

  After reviewing the results from the data that was extracted from the hard drives, I determined there was nothing out of the ordinary. No component ever connected to an outside network. Also, no unknown external storage devices were detected. Without seeing their entire SOP surrounding the machines security, I believe whatever they have in place is working.

- Summary of the grounds for each opinion

  The technical analysis did not discover any internet connection nor unknown USB connection.

- Compensation for this case

Pro V&V, Inc. is being compensated a total of $21,357.26 per the above referenced quotation. This price includes the on-site analysis, follow-up analysis, and test report.

- A list of all other cases you have testified in during the past 4 years

No technical evaluation cases within the past four years have required testimony.

1.4 System Description

ES&S Voting System 6.3.0.0 (EVS6300) is a modification to the previous EAC certified ES&S Voting System 6.2.0.0 (EVS6200) release.

1.5 Audit Details

The evaluation consisted of the following tasks:

- Set up the technical evaluation environment
- Complete Chain of custody provisions for transfer of equipment between Pinal County and Provider
- Conduct an inventory of the systems, obtain pictures taken by county photographer (no phones allowed in technical evaluation environment), record serial numbers, examine tamper evident seals
- Clone server hard drives
- Clone workstation hard drives
- Clone Toolbox laptop hard drives
- Clone tabulator hard drives
- Analysis
    - Verification of system hashes
    - Compare EAC certified listing of expected software against software installed
    - Malicious software analysis / scanning using multiple signature-based Virus/malicious software detection software
    - Internet connectivity analysis
    - Variable analysis work
        - File and activity Analysis: in-depth analysis of File system Changes to the HDD volume, analysis of time and frequency of applications run on the systems

- Images/file analysis of potentially deleted images or files
- Registry analysis
- Deleted file/evidence recovery

1.6 General Information

The on-site cloning of the components was performed by Pro V&V on-site under the observation of Pinal County employees, a Republican and Democratic observer from the county, representatives from the SOS office, ES&S, and attorneys from Snell and Wilmer. The onsite activities were performed at Pinal VOTES center located at 320 West Adamsville Road, Florence, AZ 85132. During the cloning process, Pro V&V retained complete physical access to all components.

The audit and evaluation were conducted under the guidance of Pro V&V by personnel verified by Pro V&V to be qualified to perform the evaluation. Analysis was conducted at the Pro V&V test facility located in Cummings Research Park in Huntsville, Alabama. Pro V&V currently maintains custody of all clones and images.

2.0 AUDIT OVERVIEW AND RESULTS

The audit process included creation of raw disk clones using a bit-to-bit copy of each hard drive. An additional image was created by Pro V&V in Huntsville, Alabama, for analysis. This allowed the examiner to audit and analyze the components without compromising the original system environments and original clone discs. Once the system media was imaged, the examiner used technical evaluation tools to inspect the systems for indicators of internet connectivity and malicious or unauthorized software present on the systems.

The evaluation addressed each of the previously stated verification objectives in the following manner:

Table 2-1: Testing Overview

Objective #	Test Objective	Test Evaluation
1	**Verifying that the software installed on the county back-office tabulators is the same as the software certified by the U.S. Election Assistance Commission and the State of Arizona and exporting audit logs.**	Examination for Item #1, verification of hashes, included usage of: • Pro V&V version of the ES&S verification scripts and procedures

2	**Verifying that no malicious software is running on the components.**	Examination for Item #2, checking for malicious software, included usage of: • ClamAV (Version 1.4.1) • Microsoft Defender Antivirus (Antimalware Client Version 4.18.24070.5, Engine Version 1.1.24080.9, Antivirus Version 1.419.64.0, Antispyware Version 1.419.64.0) • OSForensics (Version 11.0.1010)
3	**Verifying that the components were properly connected to their local network and were not maliciously connected to any other network.**	Examination for Item #3, internet connectivity check, included usage of: • Manual review utilizing OSForensics.
4	**File and activity analysis. Verify no files were maliciously manipulated either manually or electronically through file and activity analysis.**	Examination for Item #4, file and activity analysis, included usage of: • Manual review utilizing OSForensics.

2.1 Summary Findings

2.1.1 Objective 1

Verifying that the software installed on the county back-office tabulators are the same as the software certified by the U.S. Election Assistance Commission and the State of Arizona.

Summary Findings:

Each of the four DS950 tabulators and the DS850 tabulator were examined and had a bit-by-bit clone of the hard drive. The examiners then used the Pro V&V version of the ES&S verification scripts and procedures to perform the Hash Value Verification on the software installed on the tabulators.

All related files matched the verified hash values from Pro V&V for the ES&S System.

In addition, the audit logs were exported from the tabulators. These were reviewed and it was verified that no abnormal entries from normal operational use were present.

The 2024 Primary Election was not loaded onto the DS850 tabulator. The only item showing loaded onto the DS850 was titled 'Favorite Things', which occurred on August 26, 2024.

The results from the DS950 were run to place on a thumb drive on August 1, 2024 for serial numbers 9523090682, 9523090683, and 9523090684) and on August 3, 2024 for serial number 9523090681.

2.1.2 Objective 2

Verifying that no malicious software is running on the components.

Summary Findings:

Each of the two EMS Servers, two EMS Clients, four DS950s, the DS850, and the ToolBox laptop were examined and had a bit-by-bit clone of the hard drive. All files on each of the two EMS Servers, two EMS Clients, four DS950s, the DS850, and the ToolBox laptop were examined to determine if any malicious files were resident. Two different antivirus scanners were utilized (ClamAV and Microsoft Defender Antivirus), along with OSForensics, 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:

- *Inspection of operating system artifacts. This included items such as most recently used objects, installed programs, event logs, and recycle bin.*
- *Inspection of internet artifacts. Including items such as downloads, browser history, form history, and bookmarks.*
- *Inspection of external device usage. Includes history of USBs, mounted volumes, and mobile backups.*

The only ES&S software loaded onto the Toolbox laptop was ES&S Toolbox.

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

2.1.3 Objective 3

OSForensics was used to examine the activities of each EMS server, client, and toolbox, looking to determine if any connections were made to the internet. 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:

- *Inspection of operating system artifacts. This included items such as event logs, UserAssist entries, jump lists, and shellbags.*
- *Inspection of internet artifacts. Including items such as website logins, chat logs, peer-to-peer, and WLAN connections.*

- *Inspection of external device usage. Includes history of USBs, mounted volumes, and mobile backups*

No evidence of internet connectivity was found. Only proper zero tunnel connections were made.

2.1.4 Objective 4

File and activity analysis.

Summary Findings

OSForensics was used to examine the file system activities of each EMS server, client, and toolbox, looking to determine if anything seemed inconspicuous. These inspections included:

- *Inspection of user activity. This included items such as recycle bin, shellbags, jump lists, UserAssist entries, and event logs.*
- *Inspection of deleted files. These are deleted files no longer in the recycling bin.*
- *Review of the provided ElectionWare audit logs did not reveal any irregularities.*

No evidence of malicious or unexpected activity was detected on the systems.

3.0 RECOMMENDATIONS

At audit completion, Pro V&V developed the following recommendations based on the findings. None of the findings have any impact on the election count from the Pinal County election.

- During the analysis conducted in the Pro V&V lab, the EMS servers seemed to be set to RAID 1. In this configuration drives three through six are not being used. However, the RAID could be configured to RAID 5, utilizing all the hard drives in the EMS server expanding system redundancy.

A detailed technical report is provided under separate cover.