SECURITY ASSESSMENT SUMMARY REPORT
FOR
ES&S
EVS 5.0.0.0 VOTING SYSTEM

Appendix A.10

TABLE OF CONTENTS

Page No.

1.0 INTRODUCTION

The NIST Handbook 150-22, Section 1.5.3 states in part that, "the core voting system tests in the VST LAP include […] security tests." The purpose of the VSTL security testing was to analyze the overall security capabilities of the defined voting system to the applicable specifications and requirements found in the appropriate standards to ensure the integrity of the voting system.
(Reference VVSG v1, Purpose and Scope)

The first step in voting system security testing was to define the scope of the effort. In this step, the boundaries of the system were identified, along with the resources and the information that constitute the system. To this, the VSTL required adherence to those assignment conditions that were necessary for proper development and reporting. (Reference NIST Special Publication 800-30, Risk Management for Information Technology Systems)

This security testing campaign was for national certification and was performed to the U.S. Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG-2005).

On December 13, 2005, the EAC unanimously adopted the Voluntary Voting System Guidelines of 2005 (VVSG-2005). The VVSG-2005 increased security requirements for voting systems." As per the VVSG-2005, "voting system security is achieved through a combination of **technical capabilities** and sound **administrative practices."** All voting 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.
- Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.
- Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met.
- Provide safeguards in response to system failure to protect against tampering during system repair or interventions in system operations.
- Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation
- Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled.
- Provide documentation of mandatory administrative procedures for effective system security.
  [Reference VVSG v1, Section 7, Security Requirements]

No predefined set of security standards will address and defeat all conceivable or theoretical threats. The [VVSG] Guidelines articulate requirements to achieve acceptable levels of integrity and reliability. The objectives of the security standards for voting systems are:

- To protect critical elements of the voting system
- To establish and maintain controls to minimize errors
- To protect the system from intentional manipulation, fraud and malicious mischief
- To identify fraudulent or erroneous changes to the voting system
- To protect secrecy in the voting process
  [Reference VVSG v1, Section 7.1, Security Requirements, Scope]

The security testing was map back to one or more of the above objectives.

2.0 SCOPE OF TESTING

2.1 Purpose

The purpose of this security testing was to investigate possible technical, physical, and operational security issues involving the voting system. This supplementary report is a synopsis of the testing performed and the noted results. The testing included, but was not limited to, documentation reviews, vulnerability scans, system audits, and Security Test & Evaluations (ST&E). This report is intended to help familiarize stakeholders with the system level technical, physical, and operational testing processes that were used to help check the confidentiality, integrity, and availability of the system and its components.

The security functional testing was performed to verify or validate the accomplishments of a function or a series of functions. [Reference VSTL v1, Appendix A, Glossary]

2.2 Wyle Security Testing Structure

I. WHVS07 Voting Systems Test Procedure
II. Wyle Test Plan
   A. WHVS07.07 (Telecommunications Requirements Testing)
      1. WoP 31 (Telecommunications - Test Requirements 10-13)
   B. WHVS07.8 (Security Testing)
      1. WoP 6, (Security - Acceptance Criteria)
      2. WoP 6a (Security)
      3. WoP 6b (Physical Security)
      4. WoP 6c (Software Security)
      5. WoP 6d (Access Security)
      6. Test Cases
   C. WHVS07.4 Function Configuration Audit
      1. WoP 26 (Functional Configuration Audit)
      2. Test Cases
   D. WHVS07.05 System Integration Testing

The following activities were within the scope of this project:

- Review of supplied documentation.
- Assessment of the physical security of all system components
- Assessment of the configuration and security controls of the DS850.
- Assessment of user access, roles, and permissions.
- Penetration testing of the DS850.

The following activities were NOT part of this security assessment:

- Any Social Engineering techniques.
- Any testing that could irreparably harm the EUT.

2.3 Discovery and Exploratory Functional Security Testing

The functional security testing was broken into two phases. The first phase was the discovery phase. Scans were performed on different components of the EVS 5.0.0.0 at different states targeting initialization, maintenance, and election states. These scans provided information about the ports, protocols, and hardware as well as simulate certain attacks on vulnerable areas of the system. This information was then analyzed by Wyle's security professional. This analysis of the data provided the

method of attack during the second, exploratory, phase of testing. Exploratory testing was performed at Wyle's facilities. A complete report of the testing results was provided to ES&S. The report documented any noted vulnerable areas of the EVS 5.0.0.0 Voting System. Some of the procedures used during testing are as follows:

- Using the appropriate policy, setup inside the switch and conduct Nessus unleveraged scans of all devices.
- Using the appropriate policy, setup inside the switch and conduct Nmap scans of all devices.
- Using inside setup, input the appropriate account information for each system and rescan with Nessus (leveraged)
- Setup on the outside of the backend system and conduct/attempt Nmap scans for any outside facing IPs.
- Depending on the previous results, conduct/attempt Nessus unleveraged scans for any outside facing IPs.
- Depending on the previous results, conduct/attempt Nessus leveraged scans of devices found.
- Analyze scan results and determine if any additional test should be performed using Metasploit.

2.4 Security Testing

The WoP6 Security Testing Suite in part:

- Reviews the TDP to verify and validate the system security overview.
- Reviews the TDP to verify and validate system general security checks.
- Reviews the TDP to verify and validate system access controls.
- Reviews the TDP to verify and validate system physical security measures.
- Reviews the TDP to verify and validate system logical security measures.
- Test the defined security management.
- Tests the various system defined security roles and permissions.
- Tests the various system defined physical security measures
- Tests the various system access controls, detection capabilities, and logging.
- Verifies and validates the resident system software and firmware.
- Performs various penetration and exploitation testing.

The Functional Configuration Audit in part:

- Validated and verified system security measure limits.
- Exercised audit, logging and penetration detection features.
- Exercised system access controls.
- Verified System capabilities including security features
- Maintenance, Transportation, and Storage Capabilities.
- Validated and verified system voting capabilities including security measures.

The System Integration Tests in part:

- Validated the fully integrated components including security measures.
- Verified and validated resident software, firmware.

2.5 References

The media listed below were utilized as part of this test:

- Parikh, Clay U., CEH, CHFI, CISSP. Wyle Security Test Summary of ES&S Voting System Version 3400. Letter. May 21, 2012. Print.

- Parikh, Clay U., CEH, CHFI, CISSP. Wyle Security Test Summary of ES&S Voting System Version 5.0.0.0 (EVS 5.0.0.0). Letter. May 15, 2012. Print.
- United States Election Assistance Commission. 2005 Voluntary Voting System Guidelines, Volume I, Version 1.0. New York, Washington D.C., 2005, Print
- United States Election Assistance Commission. 2005 Voluntary Voting System Guidelines, Volume II, Version 1.0. New York, Washington D.C., 2005. Print
- United States Election Assistance Commission. Testing and Certification Program Manual, Version 1.0. New York, Washington, January 1, 2007. Print
- United States Election Assistance Commission. Voting System Test Laboratory Program Manual, Version 1.0, New York, Washington, effective date July 2008. Print
- United States Department of Commerce, National Institute of Standards and Technology. National Voluntary Laboratory Accreditation Program, NIST Handbook 150, 2006 Edition, NVLAP, Washington, February 2006. Print
- United States Department of Commerce, National Institute of Standards and Technology. National Voluntary Laboratory Accreditation Program, NIST Handbook 150-22, 2008 Edition, NVLAP, Washington, May 2008. Print
- Help America Vote Act (HAVA) of 2002, Pub. L. no. 107-252. October 2002. Web
- Wyle Laboratories. Quality Assurance Program Manual, Revision 4. Print
- ANSI/NCSL Z540-3, Calibration Laboratories and Measuring and Test Equipment, General Requirements. Web
- United States Election Assistance Commission. Notices of Clarification. Web, EAC.gov
- United States Election Assistance Commission. Requests for Interpretation. Web, EAC.gov
- NIST Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199, February 2004

2.6 Terms and Abbreviations

Table 1-1 Terms and Abbreviations

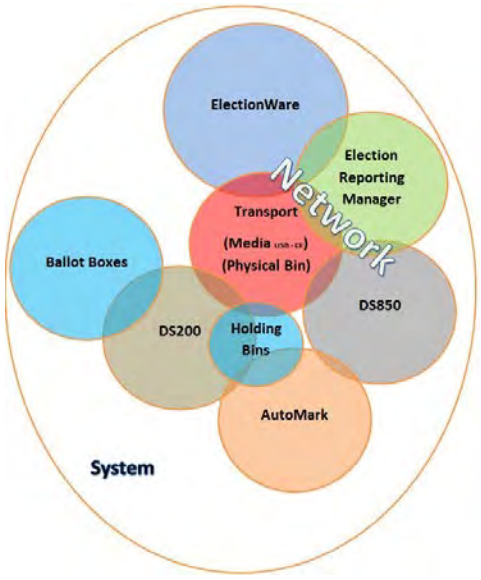
Term	Abbreviation	Definition
United States Election Assistance Commission	EAC	Commission created per the Help America Vote Act of 2002, assigned the responsibility for setting voting system standards and providing for the voluntary testing and certification of voting systems.
Election Manager System	EMS	The Election Management System (EMS) is a set of applications responsible for all pre-voting and post-voting activities in the process of defining and managing elections. The complete EMS software platform consists of client (end-user) and server (back-end) applications.
Equipment Under Test	EUT	The components of the voting system being tested.
Personal Computer	PC	The EMS Windows Operating System (OS) desktop computer and peripherals.
Technical Data Package	TDP	The documents necessary to define the product and its method of operation; to provide technical and test data supporting the vendor's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance.
Transport Media	TM	Universal Serial Bus (USB) Disc Drives and Compact Flash (CF) Cards used by the system to transport election data.
Voluntary Voting System Guidelines	VVSG	---

3.0 TESTED SYSTEM

According to the manufacturer's TDP overview…

The "ES&S Voting System version 5.0.0.0 (EVS 5.0.0.0) is ES&S's first voting system to fully comply with the EAC 2005 Voluntary Voting System Guidelines, Version 1.0. The system includes a number of new products and features including ES&S' newest election management software solution, ElectionWare, and functionality to network multiple ES&S DS850 central ballot scanners to a single reporting PC for high-speed counting and results accumulation.

The ***EVS 5.0.0.0 System Overview*** lists the following core system components and states that "ES&S alters voting system configurations to use some or all of the products listed based on the needs of client jurisdictions." Categorized lists of all system components, including peripherals and required and optional COTS equipment and software are included as attachments to this document. See the Unity EVS 5.0.0.0 Technical Data Packages for a more detailed description of these components and system configurations.



- EVS 5.0.0.0 System (as a whole)
- EMS PC applications and peripherals
- DS200 Precinct Voting Devices
- DS850 Central Count Voting Device
- Network Cable Run
- Transport Media (TM) (USB & CF)
- Ballot Boxes (DS200 and AutoMARK)
- Ballot Tote Bin
- AutoMARK (A100, A200 & A300)
- Technical Data Package (TDP) Documents

Equipment under Security Testing

EVS 5.0.0.0 System Components	Version #	Description	Equipment Identification Number
DS200 Precinct Scanner	hw: 1.2 fw: 2.7.0.0	Precinct Scanner (1) Precinct Scanner (2)	ES0108340085 ES0108340579
AutoMARK Ballot Accessible Marking System (A100, A200 & A300)	hw: v.1.0 hw: v.1.1 hw: v.1.3 fw: v.1.8.1.0	Voter Assist Terminal (1) Voter Assist Terminal (2) Voter Assist Terminal (3)	 AM020644671 AM0308421809 AMTABLE-01
DS850 Central Scanner	hw: v.1.0 fw: v.2.4.0.0	Central Scanner Cart Dot Matrix Printer Uninterrupted Power Supply Printer Cat 5 Cable	DS8511090075 Cart-03 AE72011776C0 JBH03003923 T59087-0x1-004 p/n 198-1215
ElectionWare Election Management System (EMS) (Software for defining content, candidates, and ballot formats and performing results post-processing)	f/w 4.1.0.0	Dell Desktop Dell Monitor Dell Power Edge T710 Dell Power Connect	980-372FQ1 CN…740-0435 JP26VRI 5524:4.0.1.0:AO
Election Reporting Manager (ERM) (Software for results consolidation and report generation)	f/w 4.1.0.0	Dell Desktop Dell Monitor Dell Power Edge T710 Dell Power Connect	980-372FQ1 CN…740-0435 JP26VRI 5524:4.0.1.0:AO
Transport Media	n/a n/a	Compact Flash Cards Universal Serial Bus Drives	p/n 2310 p/n 172-3219 p/n 2298 p/n 2282 p/n 2214
DS200 Ballot Boxes	n/a n/a	Metal Ballot Box Plastic Ballot Box	T59087.01-Box 12 T59087.01–Box 1
AutoMARK Ballot Holding Bins	n/a n/a	Cardboard Ballot Bin Plastic Ballot Bin	AMCARDBOARD-02 AMPLASTIC-01
Ballot Tote Bin	n/a	Ballot collection & tote bin	BIN-01

4.0 TESTING OBSERVATIONS

The EVS 5.0.0.0 is a new system. All of its components were open to testing to the VVSG-2005.

Component Under Test	HW Access Points	Physical Security	Software Validation	Logical Security
AutoMARK (A100, A200, A300)	Passed	Passed	Passed in Final Build Hash	Tested in FCA
Ballot Holding Bin (plastic)	N/A	Passed by TDP Policy	N/A	N/A
Ballot Holding Bin (card board)	N/A	Passed by TDP Policy	N/A	N/A
DS200	Passed	Passed	Passed in Final Build Hash	Tested in FCA
Ballot Box (plastic)	Passed	Passed	N/A	N/A
Ballot Box (metal)	Passed	Passed	N/A	N/A
DS850	Passed by TDP Policy	Passed by TDP Policy	Passed in Final Build Hash	Passed by TDP Policy
Network	Passed by TDP Policy	Passed by TDP Policy	N/A	N/A
Ballot Box (listed in the TDP but N/A)	N/A	Passed by TDP Policy	N/A	N/A
EMS	Passed	Passed by TDP Policy	Passed	Passed
ElectionWare	Passed	Passed by TDP Policy	Passed	Passed
ERM	Passed	Passed by TDP Policy	Passed	Passed
ULS	Passed	Passed by TDP Policy	Passed	Passed
Network	Passed by TDP Policy	Passed by TDP Policy	Passed	Passed
Transport Media				
USB (DS200 / DS850 EQC)	N/A	Passed by TDP Policy	N/A	Passed
USB (DS200 EMD pre)	N/A	Passed by TDP Policy	N/A	Passed
USB (DS200 EMD post)	N/A	Passed by TDP Policy	N/A	Passed
Flash Cards (DS200)	N/A	Passed by TDP Policy	N/A	VOTE_TC-ESS200-15
Flash Card (AutoMARK)	N/A	Passed by TDP Policy	N/A	Passed
USB (DS850 EMD pre)	N/A	Passed by TDP Policy	N/A	Passed
USB (DS850 EMD post)	N/A	Passed by TDP Policy	N/A	Passed
Flash Card (DS850)	N/A	Passed by TDP Policy	N/A	VOTE_TC-ESS200-15
Tote Box	Passed	Passed by TDP Policy	N/A	N/A
Security Seals (band aide)	N/A	Passed	N/A	N/A

4.1 Central Ballot Scanner

The **DS850** is a central ballot scanner for high speed tabulation of mail ballots, absentee ballots or election day ballots. Jurisdictions have the option to network multiple DS850 scanners to a central reporting PC for large central count operations. Despite the fact that the DS850 has been a part of previously certified systems, the DS850 was subjected to a full security testing in accordance with the requirements of Section 7, Volume I and Section 6.4, Volume II of the VVSG. This testing included the WoP6 suite, Functional Configuration Audit tests, and the System Integration testing.

The DS850 is intended to be physically isolated by the controlling jurisdiction through properly implemented physical access controls. The system documentation was reviewed to evaluate the manufacturer's security recommendations and risk assessments. According to the manufacturer's TDP, it is the responsibility of the jurisdiction to first and foremost provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of system hardware.

In addition the TDP states, "Network security is a crucial component of a well-balanced security plan. The network used by EMS, ***which includes any network required to connect tabulators to the EMS***, shall be configured to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. This is extremely important, because the network can be a very vulnerable attack vector. Physical security can mitigate the network's vulnerability, by removing or lessening the ability to tamper with physical network connections.

None the less, EAC RFI 2010-04 states, "administrative practices/procedural safeguards are not solely sufficient to fulfill the normative requirements" of the VVSG.

As such, to test the additional physical and logical security of the DS850, a unit was set up as instructed in the system TDP and it was confirmed to be in working order. Physical security measures were applied as described in the TDP and the unit was then subjected to tests as described in the WoP6 suite. Additional security testing was conducted as part of the Functional Configuration Audit tests and the System Integration testing.

DS850 security test information was also provided to a certified security professional for analysis with summary findings reported to ES&S.

As a result of this testing several sections of the TDP were updated and revised (physical and administrative).

4.2 Election Management System

EVS 5.0.0.0 uses the **ElectionWare** Election Management System software for defining contests, candidates and ballot formats and performing results post-processing; and uses the **Election Reporting Manager** software for results consolidation and report generation.

As part of this testing campaign, the EMS was subjected to security testing in accordance with the requirements of Section 7, Volume I and Section 6.4, Volume II of the VVSG. This testing included the WoP6 suite, Functional Configuration Audit tests, and the System Integration testing.

The EVS 5.0.0.0 EMS is intended to be physically isolated by the controlling jurisdiction through properly implemented physical access controls. The system documentation was reviewed to evaluate the manufacturer's security recommendations and risk assessments. According to the manufacturer's TDP, it is the responsibility of the jurisdiction to first and foremost provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of system hardware.

Additionally the TDP states that jurisdictions must physically secure any computer system that contains ballot definition files, data acquisition software, or reporting software from access by unauthorized persons; however, EAC RFI 2010-04 states, "administrative practices/procedural safeguards are not solely sufficient to fulfill the normative requirements" of the VVSG.
Also the TDP states, "Network security is a crucial component of a well-balanced security plan. **The network used by EMS**, *which includes any network required to connect tabulators to the EMS*, shall be configured to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. This is extremely important, because the network can be a very vulnerable attack vector. Physical security can mitigate the network's vulnerability, by removing or lessening the ability to tamper with physical network connections.

None the less, EAC RFI 2010-04 states, "administrative practices/procedural safeguards are not solely sufficient to fulfill the normative requirements" of the VVSG.

As such, to test the additional physical and logical security of the EMS, a unit was set up (stand-alone and networked) and hardened as instructed in the system TDP. It was then confirmed to be in working order. Physical security measures were applied as described in the TDP and the unit was then subjected to tests as described in the WoP6 suite. Additional security testing was conducted as part of the Functional Configuration Audit tests and the System Integration testing.

Test information was also provided to a certified security professional for analysis with summary findings reported to ES&S.

As a result of this testing several logical abilities and limits were revised and sections of the TDP were updated and revised (logical and administrative).

4.3 Precinct Ballot Scanner

The **DS200** is a paper ballot scanner designed for polling place use. Despite the fact that the DS200 has been a part of previously certified systems, it was subjected to full security testing in accordance with the requirements of Section 7, Volume I and Section 6.4, Volume II of the VVSG. This testing included the WoP6 suite, Functional Configuration Audit tests, and the System Integration testing.

According to the manufacturer's TDP, it is the responsibility of the jurisdiction to first and foremost provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of system hardware.

To test the DS200 physical and logical security the unit was set up in both of its configurations (with a metal and a plastic ballot box) as instructed in the system TDP. The DS200 was then confirmed to be in working order. Physical security measures were applied as described in the TDP and the unit was then subjected to tests as described in the WoP6 suite. Additional testing was conducted as part of the Functional Configuration Audit tests and the System Integration testing.

Test information was also provided to a certified security professional for analysis with summary findings reported to ES&S.

As a result of this testing several sections of the TDP were updated and revised (physical, logical, and administrative).

4.4 Electronic Voter Assist Terminal

The **AutoMARK Voter Assist Terminal** is a ballot accessible marking system that supports audio, touchscreen and tactile keypad inputs for ballot marking. Despite the fact that the AutoMARK has been a part of previously certified systems, it was subjected to full security testing in accordance with the requirements of Section 7, Volume I and Section 6.4, Volume II of the VVSG. This testing included the WoP6 suite, Functional Configuration Audit tests, and the System Integration testing.

According to the manufacturer's TDP, it is the responsibility of the jurisdiction to first and foremost provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of system hardware.

To test the AutoMARK physical and logical security the unit was set up in both of its configurations (with and without a plastic and cardboard ballot bin) as instructed in the system TDP. The AutoMARK was then confirmed to be in working order. Physical security measures were applied as described in the TDP and the unit was then subjected to tests as described in the WoP6 suite. Additional testing was conducted as part of the Functional Configuration Audit tests and the System Integration testing.

As a result of this testing the RJ45 jack was removed from the front of the unit, the use of the USB (type b) port was more properly defined, logical abilities and limits were revived, and several sections of the TDP were updated and revised (physical, logical, and administrative).

4.5 Transport Media

The EVS 5.0.0.0 system utilizes both universal serial bus flash drives and compact flash cards for transport media. The security involved with these devices was tested during many of the function configuration audit test and the system integration testing.

The TDP states, "Administrative procedures must be used to ensure security of AutoMARK media. Maintain chain of custody for any media transported from the election coding center. When not in use, AutoMARK media should be stored under lock and key. All AutoMARK media should be labeled and logged to track custody."

The TDP also states, "Administrative procedures must be used to ensure security of the EQC Media Device. Proper chain of custody must be maintained especially if EQC media are transported to a site other than where they were created. When not in use, EQC media should be secured under lock and key. If a jurisdiction creates more than one EQC device, each device should be labeled and logged to track who has custody."

Finally, "Proper disposal of confidential waste, including paper and electronic media, shall be carried out in a careful and adequate manner to maintain confidentiality."

None the less, EAC RFI 2010-04 states, "administrative practices/procedural safeguards are not solely sufficient to fulfill the normative requirements" of the VVSG.

To test the physical and logical security of the system's transport media, the system was set up as instructed in the TDP during various testing. The transport media was then used as instructed and sample memory content reviewed. This testing was conducted during the WoP6 suite testing, Functional Configuration Audit tests, and the System Integration testing.

As a result of this testing several sections of the TDP were updated and revised (administrative).

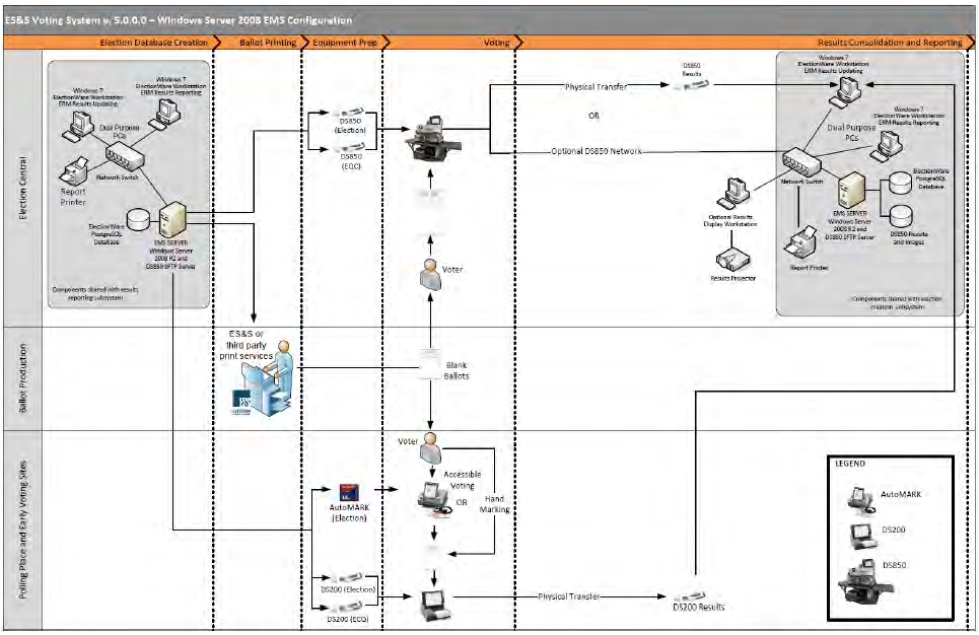
4.6 Ballot Tote Bin

The EVS 5.0.0.0 system includes an option ballot tote bin. This bin can be used in conjunction with the DS200 metal ballot box or as a standalone ballot transport.

To test the physical security of the tote bin, and any impact its use may have upon other system components, a DS200 on a metal ballot box was set up as instructed in the TDP. The tote bin was then added as instructed and sample ballots were cast. This testing was conducted during the WoP6 suite testing.
As a result of this testing sections of the TDP were updated and revised (administrative, physical).

4.7 Network Cables Runs

In addition to the EMS network capabilities, jurisdictions have the option with the EVS 5.0.0.0 system to add multiple DS850 scanners to this closed network for central count operations. This network was illustrated in the System Overview TDP.



The TDP states, "Network security is a crucial component of a well-balanced security plan. The network used by EMS, *which includes any network required to connect tabulators to the EMS*, shall be configured to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. This is extremely important, because the network can be a very vulnerable attack vector. Physical security can mitigate the network's vulnerability, by removing or lessening the ability to tamper with physical network connections.

None the less, EAC RFI 2010-04 states, "administrative practices/procedural safeguards are not solely sufficient to fulfill the normative requirements" of the VVSG.

To test the physical and logical security of the system's network, a DS850 was set up as instructed in the TDP with a network cable run to the EMS. The DS850, EMS, and network were then confirmed to be in working order. Physical security measures were applied as described in the TDP and the cable run was then subjected to tests as described in the WoP6 suite. Additional testing was conducted as part of the Functional Configuration Audit tests and the System Integration testing.

As a result of this testing, sections of the TDP were updated and revised (administrative).

4.8 Security Supplies

The EVS 5.0.0.0 suggests the use of several specific physical security mechanisms. During this testing efforts were made to insure that these devices were utilized as recommended by their manufacturers.

This review resulted in sections of the TDP being updated and revised (administrative).

5.0 TESTING NOTES

Some security related issues were examined as part of other EVS 5.0.0.0 testing performed by Wyle. In such instances any security concerns discovered were addressed as part of those efforts. Also security issues were reported to ES&S as they become known. ES&S then updated their system to address these concerns.

At times the EVS 5.0.0.0 Voting System included additional components and functionalities that were removed by the manufacture during testing. Some security testing was performed on these features. This report however is intended to reflect the final iteration of the EVS 5.0.0.0 Voting System.

6.0 CONCLUSION

Wyle Laboratories security review and testing were performed in parallel with efforts by the manufacture to update and improve their voting system and other Wyle tests. As the results of the security efforts became known, they were communicated to the manufacture in a timely qualified manner. This dialog allowed the manufacture to address concerns and recommendations by updating their system and/or documentation while the test campaign proceeded. This interchange not only allowed for an in-depth testing of the system as originally presented but also allowed for the testing of revisions made by the manufacture. As such the final test results do not simply reflect the eventual test findings but also represent possible reiterated testing.

The security threat and risk assessments for these tests were based upon the initial Test Case Procedure Specification and the relevant VVSG requirements. Ultimately it was determined that all security test concerns were adequately addressed by the manufacture.

Wyle has therefore determined that the EVS 5.0.0.0 Voting System is compliant with the security requirements of the EAC 2005 VVSG.