PENNSYLVANIA DEPARTMENT OF STATE

ATTACHMENT E TO THE DIRECTIVE FOR ELECTRONIC VOTING SYSTEMS

PA VOTING SYSTEM SECURITY STANDARD

1. SUMMARY

The Pennsylvania Election Code authorizes the use of electronic voting systems and sets requirements for them. The code also requires the Secretary of the Commonwealth to examine all electronic voting systems used in any election in the commonwealth and file a report stating whether they meet the requirements and can be safely used by voters.

This document outlines the security testing standard developed as part of continuing efforts to enhance certification testing in Pennsylvania and intended for use in the Pennsylvania state certification examination. The standard aims to provide a consistent means of examining and certifying voting systems in PA. The tests provide a means to assess the required security properties of the voting system under examination and ascertain compliance with Pennsylvania Election Code requirements, including 25 P.S. §§ 3031.7(11), (12), (16), and (17). The security tests specifically address confidentiality, vote anonymity, integrity, availability, and auditability of the voting systems. The Department of State will evaluate the test results, and recommendations will be used to determine whether a specific system meets Pennsylvania's requirements and how it will be fielded during elections.

Pennsylvania state certification requires that voting systems be evaluated by a federally recognized independent testing authority, or voting system test laboratory (VSTL), and certified by the U.S. Election Assistance Commission (EAC) according to federal voting system standards. The security testing standard in this document assumes successful completion of EAC certification testing for conformance with either the 2005 Voluntary Voting System Guidelines 1.0 or the Voluntary Voting System Guidelines 1.1 published by the EAC, or any subsequent iteration of federal voting system standards.

Due to the nature of security testing, there may be overlap in previously completed security testing as part of the EAC certification or other state testing efforts. The Department of State will work with the vendor and testing team to ensure there is minimal overlap. The vendor can submit documentation and test reports from other state certifications or third-party security testing authorities to aid in making the

determination of testing approach. The Department of State, in consultation with the security testing team, can select some or all of the tests from the test standard. The selection of the tests to be performed will be based on the documentation of previous testing submitted as part of the request for PA certification examination.

The test specifications that follow cover documentation review, design, software security, network capabilities, audit logging, physical security and penetration testing.

2. ASSUMPTIONS

1) No components of the voting system shall be connected to any modem or network interface, including the Internet, at any time, except in a standalone **wired** local area network configuration in which all connected devices are certified voting system components. Transmission of unofficial results can be accomplished by writing results to media, and moving the media to a different computer that may be connected to a network.

2) All voting systems purchased on or after February 9, 2018 in PA must be of the type that employs a voter-verifiable paper ballot or a voter-verifiable paper record of the votes cast by a voter.

3. SCOPE OF THIS DOCUMENT

The standard and tests suggested in this document are applicable only for Security Testing of voting systems. The public examination and functional test protocol are not part of this standard.

4. TEST SPECIFICATIONS

4.1 Documentation Review

1. Confirm that the voting system documentation includes physical security recommendations and polices regarding physical access to the devices and recommendations and guidance for personnel security, locks, security seals and other tamper evident mechanisms.
2. Confirm that the voting system vendor/manufacturer identifies published, reviewed, and industry-accepted design methodologies, coding conventions, and quality assurance testing standards. The published standards must allow the testing team to verify compliance.
3. Confirm that the voting machine vendor has shared the following with Department of State. Review the submitted documentation to evaluate the overall security posture of the

system and the vendor's approach to voting system security.

a. Full copy of the Technical Data Package
b. System security architecture and network/communication capabilities
c. System configuration and hardening instructions
d. Recommended security practices
e. Risk analysis/Vulnerability assessment
f. SCAP (Security Content Automation Protocol) Checklist
g. Reported field issues/anomalies
h. VSTL deficiency reports supplied to the vendor during EAC campaign
i. Penetration testing reports on voting system conducted inhouse or by a third party
j. Third party or in-house organization security assessment/audit reports and/or organizational IT policies. Documentation on network/communication capabilities of the system and how the system can be configured disabling network functionalities if needed.
k. Any additional relevant information that demonstrates the voting system security (vendor can submit any additional relevant documentation, or the Department can request any specific information that they believe is necessary for testing).

4. Evaluate how the security features described in the documentation align or comply with applicable Commonwealth IT policies. The applicability and compliance must be evaluated by the examiner or testing team and discussed with Department staff. The Department must provide copies of applicable IT policies for evaluation.
5. Confirm that the vendor documentation includes explanation of any failover mechanisms included in the system and how availability is maintained when a failover happens.
6. Confirm that the voting system documentation includes an explanation of how the implemented controls work together to detect, prevent and respond to any data inconsistency or compromise.
7. Confirm that vendor documentation details methods and measures taken to prevent unauthorized access to sensitive information. The tests must include, but not be limited to evaluation of the following components of the voting system: vote data, username/passwords, audit log information, physical ballot records, external drives, and system hardware, software, operating system etc.

8. Confirm that the voting system vendor has documented suggestions for specialized training for election officials to ensure data is securely maintained.
9. Confirm that the voting system vendor has suggestions and/or documented processes detailing best practices for installation, secure configuration and management of data.
10. Verify that the voting system vendor documentation includes processes associated with the transport of system media, including but not limited to: USB flash drives, CF cards, and paper ballots.
11. Verify that the vendor documentation includes processes associated with restricting the transport of system media to authorized personnel only.
12. Confirm that the vendor documentation includes an explanation of system event logging capabilities, error code meanings and/or explanation with suggested corrective action, and methods on how to export logs for safekeeping and analysis.
13. Confirm that the vendor documentation includes details about the system adherence to any industry accepted Common Data Formats.
14. Confirm that the vendor can provide information on decommissioning and disposal process to any county purchasing the voting system with a copy to the Department. The vendor must also agree to adhere to any standards on decommissioning and disposal published by the county or Department.

Note: The documentation review must evaluate the documentation for accuracy, clarity and completeness, and the test results must identify any shortcomings to allow additional documentation and/or process controls that the voting system vendor, Department, and county election officials can undertake for safe and secure elections.

4.2 Design

1. Confirm the system design demonstrates it can maintain consistency, accuracy, and trustworthiness of data during Election processes. *(The testing team must use their expertise and refer to best practices to evaluate robustness of the system design.)*
2. Confirm that the voting system design
    a) is geared towards reducing attack surfaces and demonstrates the rationale for including every individual component and feature.
    b) provides multiple controls whenever possible to ensure that the system works as expected and any deviations can be detected.

c) provides the ability for election officials to submit test ballots in order to verify the end-to-end integrity of the voting system
d) provides a mechanism to detect problems and allows election officials to verify the election outcome in a manner transparent to everyone.

3. Confirm that the voting system components provide security access controls that limit and detect access to critical system components to guard against the loss of system integrity, availability, confidentiality, and accountability.
4. Confirm that the voting system provides an alternate mode of operation and data recovery in the event of any component failure (hardware or software) that provides the same functionality of a conventional electronic voting system without losing a single vote and providing a complete audit trail of the failure events and the recovery action as applicable.
5. Confirm that the voting system includes methods to help facilitate the opening and closing of polls enforcing the execution of steps in proper sequence if more than one step is required.
6. Confirm that the voting system design has appropriate checks and balances orcontrols to detect and avoid any unauthorized data access and modification.
7. Confirm that the voting system design has appropriate controls to reduce the probability of human errors during
    a) pre-voting steps like ballot preparation, election programming, ballot installation, logic and accuracy testing, poll opening, verification of the central count scanner etc.
    b) post-voting steps like close of polls, tabulation, producing reports, post-election maintenance and storage
    c) voting process (The voting system must ensure that the voter is guided appropriately through the process with proper completion signal.)
8. Confirm that the voting system provides a mechanism for the voter to validate the contents of the ballot before it is cast irrespective of the mechanism used for casting the vote. The system must support a voter verified paper ballot or voter verifiable paper record which can be used by election officials to verify the election results.
9. Confirm that any notifications, instructions, warnings, and screen display provided by the voting system does not compromise the confidentiality or the privacy of the ballot or voter in anyway.

Note: The validations required can be done either by analysis of documentation/test reports and/or by executing tests if needed. The results must provide the testing team's opinion on the overall robustness of the system design. The testing team shall also document any design enhancements and process controls that will aid in reducing the identified shortcomings.

4.3 Software Security

Software

1. Confirm that the voting system software and firmware are protected from tampering. The system must allow modification to software/firmware only using the vendor documented installation instructions.
2. Confirm that the voting system is protected against execution of software that is not considered part of the voting system. The testing team/examiner can determine appropriate tests to evaluate kiosk mode operation, whitelisting, malware protection, protection from unauthorized boot devices and other external devices, secure configuration/hardening, authenticated updates, port access, and root access. Additional tests may also be conducted as they are deemed necessary.
3. Confirm that the voting system meets secure configuration recommendations based on best practices and standards set by a recognized standard setting body.

Access Control

1. Confirm that the voting system provides robust access control implemented to prevent unauthorized access to the system. The system must follow standards set by a recognized standard setting body (e.g. NIST, EAC) and industry best practices.
2. Confirm that system can authorize actors with minimum necessary access to perform the required functions. This shall be reviewed for personnel, devices, software, and firmware.
3. Critical operations must have enhanced access control and protection. Critical operation includes, but is not limited to: software and firmware updates, system configuration, result tabulation and reporting, open/close of polls, adding users/configuring passwords, exporting logs, etc.
4. The voting system configuration must enforce best practices in password management such as enforcing default password change, account lockout, minimum password complexity, etc.

Encryption

1. Confirm confidentiality of the data is maintained during transmission of sensitive data through the use of encryption.
2. Confirm any data at rest cannot be modified by unauthorized actors. The tests must evaluate access control, encryption, physical security, and chain of custody, and ensure that layers of security exist to prevent unauthorized access to and/or modification of data.
3. Confirm the system cannot transmit non-encrypted and non-authenticated data. The test must include any network transmissions and any transmissions via physical media. The testing team must evaluate the entire data life cycle starting with election preparation until canvassing.
4. Confirm the system uses encryption and cryptographic standards set by recognized standard setting body (NIST, EAC) and industry wide best practices.

Note: Testing can involve documentation review, test case execution, review and analysis of previous security testing reports by other federal or state government agencies or designees or third-party security testing organizations. The testing team may evaluate the reports and decide on a testing approach. The tests must consider every individual component of the voting system as well as the system as a whole. The results must provide details of the test cases, test results and any shortcomings identified.

4.4 Network

1. Confirm when voting system election management software (EMS) includes network capabilities, it is for a closed network, only.
2. Confirm the voting system uses air-gapped computer networks, disconnected storage devices, or hard copy ballots for tabulation and/or results compilation.
3. Confirm the voting system provides the capability for voters to continue casting ballots in the event of a failure of any network functionality.
4. Confirm the voting system does not allow a component that is not part of the voting system to be connected to the local closed wired network, if used.
5. Confirm the system updates and/or install do not involve any connections to insecure networks. The install and/or update must happen via secure physical media or air-gapped networks.
6. Confirm the only enabled physical ports and network capabilities of the voting system are those necessary for proper functioning of the system. The test must also ensure that the

system default configuration adheres to what was reported in the documentation and cannot be tampered with.

4.5 Audit Logging

1. Confirm that the voting system maintains a secure date/time stamped permanent record of system events and audit data. Data will be used for auditing and investigating fraudulent or malicious activity. System logging cannot be disabled.
2. Confirm the voting system's real-time audit record provides operators/officials continuous updates on machine status.
3. Confirm the audit log records any attempts to connect to the system and any further actions performed. Even with connectivity disabled there may be situations where ports are left open, an intruder attempts to enable disabled ports, etc.
4. Confirm the voting system log does not enable identification of an individual voter from the logs. The log must prohibit associating the voter's identity with the voter's ballot.
5. Confirm the system allows for printing, exporting, and saving of the logs in a human readable format. The export of and access to logs must be authenticated. Evaluate log processing capabilities like combining and filtering etc. to ascertain capability to access the specific information to be audited.
6. Confirm the integrity of any log files, log file exports or reports by determining that they cannot be altered or tampered with.
7. Confirm the voting system implements appropriate checks and balances to ensure that the logs are exported and saved before the system is prepared for a new election.
8. Confirm the event logs have specific identification information to ensure that each device's logs are identifiable. If the system allows logs for multiple elections to be saved, election logs must also be easily identifiable without any ambiguity.

Note: Testing must involve a thorough evaluation of system audit logging capabilities, and the results must include the testing team's evaluation of the system audit logging capabilities in reference to identifying operational problems and fraudulent activity.

4.6 Physical Security

1. Confirm the voting system physical security recommendations suggested in the manufacturer documentation can be implemented for fielded systems and provide the required security.
2. The system must not have any unprotected physical access points. The test must evaluate

every physical access point and evaluate the strength of the protection mechanism.

Note: Testing must identify every possible access point to the system and ensure that it is appropriately protected. The test results must document every access point, location of the access point, vulnerability, and how well the physical security recommendations provide system security.

4.7 Guidelines for Penetration Testing

Penetration Testing: Penetration testing is an attempt to bypass or break the security of a system or a device. Penetration testing is conducted without the confines of a pre-determined test suite. It instead relies heavily on the experience and expertise of the team members, their knowledge of the system, its component devices and associated vulnerabilities, and their ability to exploit those vulnerabilities.

The scope of penetration testing includes but is not limited to the following:

1. Voting system security;
2. Voting system physical security while voting devices are:
    A. In storage;
    B. Being configured;
    C. Being transported; and
    D. Being used.
3. Voting system use procedures

The focus of penetration testing is to seek out and exploit vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voters' ability to cast ballots and have their votes counted accurately, or compromise the secrecy of vote.

The test must evaluate whether the voting system under examination possesses the security properties to be successfully used in Pennsylvania. The test results must allow the Department of State to assess the system security posture and to determine best practices while in use for elections. The purpose of the testing is for the testing team to consider the system being tested as an official election environment and ensure that the physical and logical controls in place cannot be exploited to adversely affect the election. The Department also aims to use the results from the test to identify conditions and/or recommendations to be specified in the Secretary's approval report to mitigate any risks identified.

Penetration Testing Steps	Requirements	Deliverables / Output
The penetration testing team shall work with DOS, the Voting System examiner (if applicable) and the Voting system vendor to prepare for the testing effort.	Confirm that penetration testing team understands the purpose of the penetration test done as part of the PA Voting System certification process. Confirm that penetration testing team is familiar with EAC certification for Voting Systems and understands the level of security testing performed during EAC certification. Confirm the staffing of the penetration testing team - The testing team SHALL have at least one member with 6 or more years of experience in the area of software engineering, at least one member with 6 or more years of experience in the area of information security, at least one member with 6 or more years of experience in the area of penetration testing and at least one member with 6 or more years of experience in the area of voting system security. The penetration testing team SHALL have at least one member with at least 8 years of experience in election management.	a) Statement of Work for penetration testing. This can be a combined SOW with functional testing if both tests are being performed by the same organization. b) Any legal documentation including non-disclosure agreements etc. c) Details of voting system configuration and supplies required for penetration testing. d) Documentation of risks that the penetration test team anticipates during the testing process. e) Communication protocol

Penetration Testing Steps	Requirements	Deliverables / Output
	Confirm that penetration testing team understands the parameters for the testing effort. Total testing duration must not exceed one month. This includes all activities in the test process including test plan, testing and result documentation. The team can plan the schedule and timeline. An example schedule is listed below. week 1 for system study and discovery week 2 and 3 for risk assessment and exploitation week 4 for analysis and reporting The team must come up with a planned schedule and timeline and communicate them as part of the SOW, or prior to the start of the testing. All required test materials must be identified as much as possible before the testing starts. In the event there is a request for additional test material, it must be completed within a week from the start of the test.	
	Confirm the location of the penetration test.	
	Confirm that the penetration testing team, voting system vendor, and voting system examiner is clear on the roles and responsibilities.	

Penetration Testing Steps	Requirements	Deliverables / Output
	Confirm the communication protocol for the penetration testing project, such as status update, progress tracking, and reporting issues.	
The penetration testing team SHALL have access to • **the manufacturer supplied Technical Data Package (TDP), source code and User documentation** • **voting devices configured for use in an election** • **all other material and tools necessary to conduct a thorough investigation.**	Confirm that the penetration testing team has materials to assist in the testing, including: a) Security architecture describing how threats to the voting system are mitigated; b) Threat analysis describing threats mitigated by the voting system; (the manufacturer prepared documentation submitted for EAC testing) c) High level design of the system; d) Documentation provided to DOS for examination and to the EAC testing laboratory; e) Source code; f) Test reports from the vendor and from the testing laboratory including previous penetration testing results; g) Tools sufficient to conduct a test lab build; h) Supplies, ballots and election definitions if necessary, locks, seals etc. (This list will need to be provided by the team as part	a) List of reports/documentation gathered. b) Voting System equipment and supplies inventory

Penetration Testing Steps	Requirements	Deliverables / Output
	of the SOW.) i) Procedures specified by the manufacturer as necessary for implementation and secure use. Confirm that penetration testing team has all the components of the voting system to be certified available for the test. The voting system software and firmware trusted build must be installed on the systems. A clean copy of the trusted build must be secured and kept for reinstallation if needed.	
	Confirm that the penetration testing team has access to PA Election Code and directives prepared by Secretary of State and Commonwealth IT policies.	
	Confirm that the penetration testing team has access to a risk assessment plan to help prioritize the vulnerability/threat pairs for exploitation. A sample risk assessment is added as Appendix A to this document. The sample plan was adopted form Report # PNN-306-STRP-01 created by SLI Global Solutions as part of a consulting agreement with Department of State.	

Penetration Testing Steps	Requirements	Deliverables / Output
The penetration testing team SHALL prioritize testing efforts based on: **a. threat scenarios for the voting system under investigation;** **b. the penetration testing team's determination of easily exploitable vulnerabilities;** **c. the penetration testing team's determination of which exploitation scenarios are more likely to impact the outcome of an election, interfere with voters' ability to cast ballots or have their votes counted during an election, or compromise the secrecy of the vote.** **d. the penetration testing team's understanding of the voting system application from the user's perspective**	Confirm that all threat scenarios are plausible in that they should not be in conflict with the anticipated implementation, associated use procedures, or the development environment specification as supplied by the manufacturer in the TDP.	a) Assets Evaluated b) Risk Assessment matrix created following the risk assessment plan. The matrix must describe the vulnerability/threat pairs identified, prioritized and exploited. c) Test results if applicable – For example copies of the logs, reports, physical devices that were tampered etc.
	Confirm that penetration testing does not exclude threat scenarios involving collusion between multiple parties including manufacturer insiders. It is acknowledged that threat scenarios become less plausible as the number of conspirators increases.	
	Confirm that it is assumed that attackers may be well resourced and may have access to the system while under development;	
	Verify that threats that can be exploited to change the outcome of an election and flaws that can provide erroneous results for an election have the highest priority;	
	Verify threats that can cause a denial of service during the election should be considered very high priority;	
	Verify that threats that can compromise the secrecy of the vote should be considered high priority;	

Penetration Testing Steps	Requirements	Deliverables / Output
e. Previous penetration testing reports if any **f. the availability of time and resources** ***The penetration testing team shall utilize the EAC test vulnerability assessment and any additional threats the team feels important and classify it based in threat/vulnerability classifications used in the risk assessment plan.***	Confirm that if the voting device uses COTS products, the penetration testing team investigates publicly known vulnerabilities;	
	Confirm that the penetration testing team does not consider the voting device vulnerabilities that require internet connectivity for exploitation if the voting device is not connected to the Internet during the election or otherwise. However, if the voting device is connected to another device which in turn may have been connected to the Internet (as may be the case of ePollbooks), Internet based attacks may be plausible and should be investigated.	
	Confirm that the penetration testing team reviews any previous penetration testing reports available for the system under test as well as prior versions of the system under test.	

Penetration Testing Steps	Requirements	Deliverables / Output
The penetration testing team must re-evaluate the risk assessment matrix after it has been compiled to **a. Analyze the exploited vulnerabilities and suggest mitigation strategies taking into consideration the complete election protocol** **b. Analyze whether any identified vulnerability indicates a weakness in design, development, process, or documentation that may lead to a similar vulnerability that was not identified as part of the testing, and suggest mitigation strategies.** **c. Re-evaluate the risk assessment matrix based on the analysis and make any changes.**	Confirm that penetration testing team does a thorough analysis of Vulnerability/Threat pairs with "Very High" and "High" ratings to ensure that there is proper rationale for the categorization. The team must evaluate whether implementation of any additional controls will reduce the risk exposure.	List of vulnerability/threat pairs prioritized and exploited and analysis on each exploitation attempt. • For exploited vulnerabilities, the testing team's assessment of the test and any additional controls suggested. • For vulnerabilities that failed exploitations, the testing team's assessment of the test.

Penetration Testing Steps	Requirements	Deliverables / Output
	Confirm that the penetration testing team does a thorough analysis of vulnerability/threat pairs with "Moderate", "Low" and "Very Low" to suggest appropriate risk mitigation strategies to avoid attacks on a fielded system.	
The penetration testing team must provide reporting and documentation for the findings in a formatted report.	Confirm that the penetration testing team can provide test results in a standard format report. The report must clearly identify the vulnerability/threat pairs where a break in was attempted and the team's evaluation of the test. In addition to the results of the penetration testing, the Department expects the following items to be added as part of the report as required. The penetration testing team's opinion on a) System Security Posture b) System Logging Capabilities c) Capability to support post-election audits d) Adherence to Common Data Format e) Best practices in fielding the equipment	Penetration testing report

6 REFERENCES

a) SLI Global Solution LLC Deliverables prepared as part of PO 4300561059 - 19_SLI Testing Standards_BCEL
b) VVSG 1.1, 2015 Voluntary Voting System Guidelines

Appendix A

Risk Assessment Plan

Purpose

Risk assessment is a tool to help protect the efficiency, accuracy and integrity of elections conducted on a specific voting system. To evaluate the severity of risk; a determination of the likelihood of a threat and the impact the threat can have on the system has to be done.

The process uses the following steps to systematically determine each risk level.

1. **Describe the Assets:** Identifies the resources in need of protection.
2. **Describe the Threats:** Identifies who or what constitutes a threat, as well as from where and why.
3. **Describe the Vulnerabilities:** Identifies the weaknesses and assets that are exposed.
4. **Determine Likelihood:** Quantifies the chance a threat will successfully exploit a vulnerability.
5. **Determine Impact:** Quantifies the maximum effect a threat has after exploiting a vulnerability.
6. **Determine Risk**. Calculates a relative score based on Likelihood and Impact

Calculated risks are used to determine a system's greatest vulnerabilities and areas in which additional protections are to be considered. There are many approaches to mitigating risk ranging from recommended policies and procedures, to hardware implementation configurations, to hardened operating systems.

Term and Acronyms

Key Terms

Term	Description
Asset	Item or System that needs protection
Impact	A relative rating for the maximum effect a threat has after exploiting a vulnerability
Likelihood	A relative rating for a threat successfully exploiting a vulnerability
Risk	A relative rating based on the likelihood and impact of a threat exploiting a vulnerability
Threat	Anything capable of attacking an asset
Vulnerability	A Weakness in a system that allows a threat to succeed

Definitions

Term	Description
Actor	The agent that threatens the system
Ballot on Demand (BOD)	The system component from which a blank paper ballot is produced at election office headquarters or a polling place
Cast Vote Record (CVR)	Permanent record of all votes produced, electronic or paper, by a single voter. Also *ballot image* when used to refer to electronic ballots
Central Count Scan (CCS)	Device converting selections on marked paper ballots into digital data via high speed scanner
Controller (If applicable)	The system device in a daisy-chain configuration and operated by a poll worker to assign the correct ballot style to a voter
Data at Rest (DAR)	Data stored either temporarily or permanently
Data in Transit (DIT)	Data in transit either electronically or physically
Denial of Service DOS	Cyber-attack where heavy demands are made on the targeted information infrastructure to cause overload resulting in blocked system access.
Election Management System (EMS)	System used to define, develop and maintain election data to establish election definitions, format ballots, count votes, consolidate and report results, and generate and maintain audit logs.
External	Agent(s) with no authorized access to the system or its data. Examples: hackers, weather and other natural phenomena, etc.
In Person Voting Device (IPVD)	Voting device used by individual voters to vote and cast a ballot in person (e.g. paper ballot scanner, direct record electronic (DRE), marked ballot printer (MBP)).
Internal Actor	Agent(s) with operational access to the system and data (login authorization, warehouse keys, etc.) Examples: Poll workers, voter, ballot printers, etc.

Term	Description
Privileged Actor	Agent(s) with role-based unfettered access to sensitive components and data of the system (encryption keys, passwords, source code, etc.) Examples: high level election officials, Voting vendor engineers, etc.
Random actor	Any person or thing capable of indirectly affecting the system (e.g., a driver crashing a vehicle delivering voting equipment or severe weather that damaging a polling place)
Technological actor	An automatic program (e.g., a virus) can impose a threat, a programming error or design flaw; or a failure of the technology (e.g. an age or duty cycle related failure)
Transported	Anything moved or conveyed from one point to another by any means

Risk Analysis

Assets

Next to human safety, the confidentiality, integrity and accessibility of an election are of the highest concern. The protection of any data or device necessary in conducting an unbiased election are the main priority. An attack on or failure of any of these assets can call the integrity of an election into question.

Assets are listed below:

- **Physical Security**
  - Safety of Poll Workers and Voters
  - Device security in storage facilities, in transit and at the polling place
- **Data Assets**
  - Cast Vote Records (primary, backup and secured during a retention period)
  - Election definitions
  - Log files for the OS, voting devices and EMS applications
  - Reports
  - EMS application programs, operating system software, and configuration files.
  - Vote tabulation files
  - Polling place documents including those with voter- specific information, (e.g., securing anonymity)

- Paper ballot supply (blank and voted

- **Non-Data Assets**
  - Voting system availability
  - Intangible assets (e.g. State and jurisdiction reputation, public trust in voting and government)
- **Physical Infrastructure**
  - Electrical power
  - Environmental control
  - Secure storage area for EMS and voting devices
  - Functional voting equipment
- **Support Infrastructure**
  - Technical support
  - Trained elections professionals
  - Secure equipment delivery and storage
  - Contingency planning

Threats

A threat is classified as anything capable of negatively affecting an election. Threats can be intentional or accidental, a disgruntled employee or natural disaster are examples. Each threat has three distinct characteristics which help describe the level of impact; actor, motive, and location/origin of threat.

An actor has the potential to threaten the system, regardless of motive. Actors are grouped into seven (7) categories:

1. **Government Sponsored:** These groups are well funded and often build sophisticated, targeted attacks. They are typically motivated by political, economic, technical, and military agendas.
2. **Organized Crime:** Most often, these cybercriminals engage in mass attacks driven by profits. They are typically looking for Personally Identifiable Information (PII) such as social security numbers, health records, credit cards, and banking information.
3. **Hacktivists:** These attackers have a political agenda and create high-profile attacks and distribute propaganda to cause damage to organizations they are opposed to in order achieve their cause or gain awareness for their issue.
4. **Insider Threat:** Insider attackers are typically disgruntled employees or ex-employees looking for revenge or some type of financial gain. They sometimes collaborate with other threat actors in exchange for money.
5. **Opportunistic:** These attackers are usually script kiddies driven by the desire for notoriety, but they are also sometimes security researchers/professional hackers

looking to profit from finding and exposing flaws and exploits in network systems and devices.

6. **Internal User Error:** Users making mistakes with configurations which may bring down critical resources such as firewalls, routers and servers causing wide-spread or departmental company outages. Oftentimes, this is the result of providing an individual with privilege that exceeds their technical skill level.
7. **Natural / Unpredictable**: Events or accidents outside of human control that may bring down critical resources. These may include natural disasters, or fires, floods, or inclement weather.

Determining the level of an actor's motivation can be both difficult and subjective. No extra effort will be used to determine the specific motive by Actor Category. Motives are, defined as either intentional or accidental.

Location defines the point of origin of a threat. Three possible origins are defined: privileged, internal and external.

- A ***privileged*** actor is granted unrestricted access to the system, its components, and/or the election data with the fewest safeguards to bypass before causing harm. Examples include: Administrators, Voting vendor representatives, election official's examples of privileged actors.
- ***Internal*** actors are granted limited access to the election system to administer an election. Their presence is expected and typically unquestioned. Safeguards and security measures exist to restrict activities. Ballot layout specialists, voters and technical support agents are examples of internal agents.
- ***External*** actors have no authorized access to the election system. Natural / Unpredictable events, viruses and system hackers are examples of external agents.

The above characteristics are used in conjunction with the general categories of threats listed below to create a comprehensive list of threats evaluated against the vulnerabilities later in the analysis.

Categories	Description
Attacks on physical security	Anything that disrupts the operation of the equipment and/or the election. Picketing/demonstrations, theft vandalism, etc.
Attacks on Data in Transit (DIT)	Anything that modifies data in transit from asset to asset prior to being recorded, or as it is being tabulated or aggregated, resulting in changing or blocking election results.
Attacks on Data at Rest (DAR)	Anything that attempts to either modify, delete or copy stored data including the OS, application binaries and CVRs.

Indirect Attacks	Anything that attempts to affect the execution or integrity of an election. DOS at any stage of the election, attacks on the company or products reputation are examples.
Attacks on the Physical Infrastructure	Anything that attempts to affect the necessary infrastructure for running a successful election.

Vulnerabilities

Any characteristic that allows an attack to be successful is a vulnerability in the system or asset. The relative Classification of vulnerability is defined by the ease with which it is exploited, as well as the amount of damage caused. For example, an easily exploited weakness in the system leading to little or no impact on the outcome is of far less importance than a weakness requiring more effort and allows the attacker to dictate a change in tabulated results.

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective

Probability

Probability, or likelihood, of occurrence, is the chance a threat will successfully exploit a vulnerability. It is a combination of the force a specific threat can bring to bear on an asset and how often we can expect the threat to succeed. The level of force is determined by three major characteristics of a threat as described in Section 3.2. How often a threat is successful, is based on external factors such as professional experience, evaluation of current threats, voting manufacturer company history, and where available, published historical information.

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Greater than 95% probability of occurrence. Almost certain it will happen or is already happening
High	80-95	8	Between 50% and 75% probability of occurrence. Very likely. Will occur in most circumstances (next 12 months).
Moderate	21-79	5	Between 25% and 50% probability of occurrence. Probability of occurring 1-5 years.
Low	5-20	2	Less than 25% probability of occurrence. Unlikely, may occur at some point (5-10 years).
Very Low	0-4	0	Never happen, may occur in exceptional circumstances. No material probability of occurrence, possible but would be very surprising.

Impact

Impact is a relative score describing how much an election affected. An impact rating of a 1 is not considered material while 4 or higher is considered a significant impact. The table below describes each range and provides examples to give a flavor of the impact each range represents.

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Damage to broad regions of service or every system in use. Releasing voter information linked to votes. Tampering or “hacking” that effects election results and is not reported until after the election. Financial and reputation damage can be serious.
High	80-95	8	Damage that involves broad regions of service and which may prevent an election from being conducted successfully. Reputation and financial damage can be significant.
Moderate	21-79	5	Damage that involves broad regions of service and which may prevent an election from being conducted

			successfully. Reputation and financial damage may occur.
Low	5-20	2	Impact that briefly interrupts service or which takes a critical but replaceable system offline, or which compromises ongoing security.
Very Low	0-4	0	None, or damage that does not interfere in operations, service, or security

Adverse Impacts Examples

Examples of Adverse Impacts for the State Pennsylvania:

Type of Impact	Impact
Confidentiality	Inability to maintain the confidentiality of the contents cast vote record.
Vote Anonymity	Inability to maintain the anonymity of the voter after a Cast vote record is created.
Integrity	Inability to assure the voter that his/her ballot choices are being recorded, counted, and reported as marked and cast. The voting system permits undetectable changes or errors that cause an undetected change or Error in an election outcome
Availability	The voting system is unavailable to the voter during normal periods of established voting hours. The voting system has a single point of failure that could result in information loss or lost cast vote records.
Auditability	The voting system does not log events including: ▪ Voter Events – particularly the admission of a voter to the machine, the selection of ballot style, the casting of each ballot. Data must be retained in a form as close to that originally generated by the voter as possible. ▪ System Events – hardware and software failures, resource exhaustion or near exhaustion. ▪ Poll Worker Events – actions performed on a voting system requiring special privilege, such as cancelling a ballot, opening and closing the system for voting. ▪ System Administrator Events – performing tests, changing configuration, erasing parts of memory, etc.

Type of Impact	Impact
Accountability	Inability for the election officials to re-examine voter actions or marks in order to confirm the voter's intention. The inability of a recount ability to provide assurance that the outcome of an election was determined correctly.

Risk

A risk level is the probability a vulnerability is exploited by a threat and the impact it could have on an election. Using the Probability score and the Impact score, an overall Risk score is calculated. Each risk will have to be investigated to determine the appropriate level of risk there is a potential to have a high-risk rating that is not critical, and a low risk rating that is critical.

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on State or Commonwealth election process, State or Commonwealth voting assets, Pennsylvania voting code violations.
High	80-95	8	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect State election process, State or Commonwealth voting assets, Pennsylvania voting code violations.
Moderate	21-79	5	Moderate risk means that a threat event could be expected to have a serious adverse effect on State election process, State or Commonwealth voting assets, Pennsylvania voting code violations.
Low	5-20	2	Low risk means that a threat event could be expected to have a limited adverse effect on State election process, State or Commonwealth voting assets, Pennsylvania voting code violations.
Very Low	0-4	0	Very Low risk means that a threat event could be expected to have a negligible adverse effect on State election process, State or Commonwealth voting assets, Pennsylvania voting code violations.

Risk Exposure Matrix

Risk Exposure Matrix: Combination of Likelihood, and impact will determine the level of risk.

Likelihood (Threat Event Occurs in adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Suggested Actions

Suggested Actions Based upon Exposure:

Risk Exposure Rating	Description	Action	Examples
Very High	Indicates a vulnerability and/or threat that has a ***Very High*** Impact and likelihood that the election process or systems will be compromised.	Suggested action is to recommend that the voting system is not certified for elections in the Commonwealth of Pennsylvania.	▪ Normally this would constitute a threat or vulnerability that would require the voting system manufacturer to have to make core changes to the voting system. ▪ Unknown vulnerability exposes the ability to affect the outcome of an election. ▪ Election system encryption has been compromised either through an unrelated attack or an attack directly targeting the voting system.

Risk Exposure Rating	Description	Action	Examples
High	Vulnerability or threat that has a ***High*** impact and likelihood that the election process or systems will become compromised.	Suggested action is to recommend that he voting system is not certified for elections in the Commonwealth of Pennsylvania.	▪ Unless there are appropriate mitigating controls that are in place to reduce the risk of such threats or vulnerabilities to an acceptable level agreed upon by the Commonwealth. ▪ Distribution of a flawed or infected configured item software upgrade).
Moderate	Vulnerability or threat that has a ***Moderate*** impact and likelihood that the election process or systems will become compromised.	Suggested actions is to determine on a case by case basis if the exposure is serious enough to affect the system as a whole.	▪ Broken production software build that could be installed on a large number of devices. ▪ Previously unknown software flaw that went unpatched. ▪ Malware infection that is controlled that may cause slight outages. ▪ Appropriate mitigating controls are often instituted by the Manufacturer or State in the form of processes and procedures.
Low	Vulnerability or threat that has a ***Low*** impact and likelihood that the election process or systems will become compromised.	Suggested actions is to determine on a case by case basis if the exposure is serious enough to affect the system as a whole. Normal outcome would be to recommend the certification of voting system for use in Pennsylvania.	▪ Dropped or broken device that is inoperable. ▪ Vulnerabilities that are mitigated by System or Commonwealth processes and procedures. ▪ Most exposures of the low variety are general threats or vulnerabilities that warrant documentation and observation, however

Risk Exposure Rating	Description	Action	Examples
			are usually not critical to the Commonwealth election code or election process.
Very Low	Vulnerability or threat that has a ***Very Low*** Impact and likelihood that the election process or systems will become compromised.	Recommendation action is to document risk and accept the risk. Normal outcome would be to recommend the certification of voting system for use in Pennsylvania.	▪ Brief electrical outage, covered by a UPS. ▪ Informational vulnerability detailed by a vulnerability scanner.