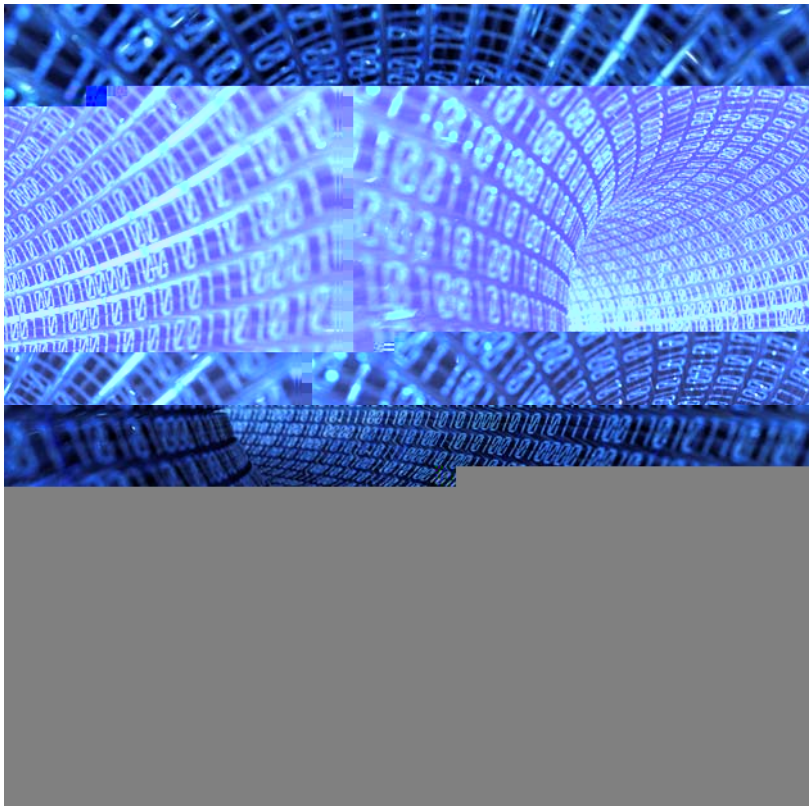

ES&S SYSTEM

MICROSOLVED, INC.

TECHNICAL DETAILS REPORT

CONFIDENTIAL[1]

[1] This report is released by Ohio Secretary of State Jennifer Brunner consistent with the Ohio Public Records Act, Ohio R.C. 149.43. The reader of this document is advised that any conduct intended to interfere with any election, including tampering with, defacing, impairing the use of, destroying, or otherwise changing a ballot, voting machine, marking device, or piece of tabulating equipment, is inconsistent with Ohio law and may result in a felony conviction under, among other sections, Ohio R.C. 3599.24 and 3599.27.

Table of Contents

Table of Contents

Overview

This report details the technical vulnerability findings of the MicroSolved, Inc. (MSI) penetration testing team. Our team was engaged by the Ohio Secretary of State to review the electronic voting systems used in Ohio as a part of the larger EVEREST project. Our testing took place from November 5th, 2007 through November 16th, 2007. As a part of our testing, significant security issues were identified in the ES&S system at both a holistic level as well as at the lower level of many of the system components.

Purpose of this Report

This report is intended to be a catalog of the identified vulnerabilities within the ES&S system and its components. Overall security implications and details of the engagement are contained in additional reports delivered to the Secretary of State's office.

The primary audience for this report is the technical staff or product management staff tasked with the mitigation of the identified security issues. Every effort has been made to make the findings of this report clear and the mitigation suggestions real-world based. Should additional information be desired, please do not hesitate to contact us through the Secretary's office for further discussions as appropriate.

Format of this Report

Each vulnerability will be discussed in reference to the impacted component of the overall ES&S system. Each component has a specific section dedicated to it, with issues that impact several components in the final section named "General Multiple Component Vulnerabilities".

For each identified security issue, the following information is given:

Reference ID - Simply a unique reference to the specific issue. This is included to allow the readers a point of reference without complicated name issues.

Summary of the Vulnerability - A brief summary of the issue identified is included to give the reader the specific information needed to understand and locate the vulnerability.

Risk Rating - High, Medium or Low - We sorted the vulnerabilities at these levels to simplify their understanding and ease of association. High risk vulnerabilities are vulnerabilities that lead to the ability to modify the component's configuration, execute arbitrary code, modify election data or settings and/or introduce malware to the system. Medium risk vulnerabilities allow the attacker to gain additional information or examine the system in a way that could lead to further compromise. Low risk vulnerabilities are issues that impact the general performance or operation of the system, but yield little specific return when executed alone.

Impacted Pillar(s) - Confidentiality, Integrity, Availability - These three categories are often referred to as the pillars of information security. Security mechanisms must be created to prevent attacks that impact any of these three facets or reduce the impact of attacks against these categories to manageable levels.

Attack Pre-Requisites - What things must the attacker possess to exploit the vulnerability. Common prerequisites are things like specific knowledge, specific components or tools and access to specific parts of the system.

Attack Scenario - This section explains how or what an attacker might to do to leverage the vulnerability and what the potential impact is of successful exploitation.

Mitigation Suggestion - This section explains what specific mitigation strategies or tasks are suggested for minimizing the risk or mitigating the issue.

A Warning About Cascading Failures

It should be noted that the risk rating identifies the potential risk of the vulnerability in isolation. However, attackers often use a process called "vulnerability chaining" to leverage multiple vulnerabilities in a system for further access or damage. Such a system of cascading failures obviously can change the impact and risk of specific vulnerabilities as they are combined and leveraged in new ways. Too many combinations and variables impact this situation to allow for comprehensive risk rating of each vulnerability in a cascade. Thus the risk and impact of specific issues may vary, depending on the attacker expertise, access and the presence of other vulnerabilities on the system that could be included.

System Components Included in this Report

This report includes vulnerabilities identified in the following ES&S system components: iVotronic DRE units (3 models (Supervisor, precinct DRE with audio, precinct DRE without audio)), m100 Precinct Optical Scanner, m650 Central Optical Scanner, Windows 2003 Small Business Server, Windows XP Pro workstation, Unity software and the Automark unit. Other components of the system were tested, but either had no identified issues or are simply subsystems whose issues are included in their larger components. For example, the actual paper ballots were tested as a part of optical scanner testing and relevant findings are included in those sections. The memory card media was also tested, but the findings are included in the larger components where impact is likely to occur such as the DRE components, Unity software, etc.

DRE System Vulnerabilities (3 Models)

In our testing, these devices were found to exhibit the same issues. Note that they are the same hardware platform with different configurations and deployment scenarios.

ID #	DRE - 1
Vulnerability Summary	Printer and connection are not protected from tampering, causing exposure of printed records, which are the record of law in Ohio, to tampering, forgery and destruction.
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the DRE system and its printer connection, a mobile device configured to print to a serial printer (laptop or PDA, etc.), knowledge of the printing layout for tampering

Attack Scenario	Attackers could leverage this vulnerability to use the DRE printer if unattended to print their own records. They could also destroy the existing printed records by printing over them and rendering them illegible.
Mitigation Suggestion(s)	Ultimately, the design of the DRE stand should be changed to protect the printer connection and power connections. Implementing tamper tape on the printer to DRE connection or a cable lock would also minimize the risk if performed properly.
ID #	DRE - 2
Vulnerability Summary	Unhanded exceptions are present in the application, particularly around interaction with the CF card, and file handling. Such unhandled exceptions could possibly be exploited to cause denial of service issues or possibly to execute arbitrary code on the DRE.
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the DRE system and memory card slot (which is usually protected by tamper seal)
Attack Scenario	An attacker can modify the files on the card or remove it at inopportune times. These actions cause unhandled exceptions in the application. The unhandled exceptions may make exploitation possible for the execution of arbitrary code, including malware. While this could not be determined in our testing, it is a possibility - based on our experience with other systems.
Mitigation Suggestion(s)	Proper exception handling, graceful exits and recovery mechanisms should be implemented throughout the application source code. Proper handling of the exceptions and recovery, if possible, will prevent the denial of service attacks from this issue in most cases. In addition, proper bounds checking should be performed on all file I/O. If the application performs proper validation of the input files prior to their being used by the application, then this would preclude file-based attacks from being executed. Bounds checking and proper validation of input files would prevent arbitrary code from being executed by the system through overflow type exploits.
ID #	DRE - 3

Vulnerability Summary	Magnetic switch can be activated to boot system and allow interaction using a simple magnet instead of the PEB device.
Risk Rating	Low
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Magnet, Access to the component
Attack Scenario	Attackers could use this capability to probe the component, explore the available interfaces and otherwise interact with the component.
Mitigation Suggestion(s)	None available, this is a mechanism built into the system architecture. Further security against these probes could be obtained if the system performed IR validation of the PEB device prior to activating the video touch screen and other interfaces, but this would likely impact troubleshooting and other component capabilities.
ID #	DRE - 4
Vulnerability Summary	Insert magnet and hold vote button down when the component is waiting for a voter and the component reboots.
Risk Rating	Low
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Magnet, Access to the component when it is waiting for voters
Attack Scenario	Attackers could use this process to probe and investigate the system
Mitigation Suggestion(s)	Operation should be changed to generate an audible alert on the presence of the unknown PEB. The system should not reboot, but a valid PEB should be required in order to continue operation of the component and halt the audio alert mechanism. This would serve as a type of intrusion/tamper detection mechanism.

m100 Precinct Optical Scanner Vulnerabilities

ID #	POS - 1
Vulnerability Summary	Paper ballots are not serialized and can be scanned multiple times.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the scanner and/or to the ballots themselves, failure of general auditing processes
Attack Scenario	Because the ballots themselves are not serialized and no system detection of duplicate ballots takes place it is possible for duplicate ballots to be scanned by the system. Currently, Boards of Election audit the ballot counts and perform some level of inspections and dual-access controls to overcome these issues, but inclusion of electronic mechanisms would make this work less resource intensive and more accurate.
Mitigation Suggestion(s)	Optical scanning and paper ballot systems should become serialized to prevent tampering and rescan of ballots without notification. Proper memory and management systems should be implemented into the system to allow for this.
ID #	POS - 2
Vulnerability Summary	Users can close the polls by pressing two buttons simultaneously. They can also reopen and zero the totals if they know the password which defaults to [default

Attack Scenario	Attackers could leverage these vulnerabilities to interfere with the election, and possibly remove some ballots from being properly counted. While this attack is unlikely to interfere with a large scale race in a meaningful way, it could affect a close local race.
Mitigation Suggestion(s)	Further auditing of the paper tape record is required to determine if this attack has been performed. This auditing should be implemented in all uses of the component. Passwords should be different per component and harder to guess than [redacted] [defaulted password]. Access to close the poll should be done with the key only in the supervisor position. Zeroing vote totals should never be possible when the component is in the voting mode.
ID #	POS - 3
Vulnerability Summary	Write protecting the memory card during voting does not create an alert. If the polls are closed with the card write protected, the printed reports are valid, but the electronic records of the votes that occurred while the write protection was in place are lost from electronic counts.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the memory card, which requires access to the ballot box cover key, if the ballot box is being used
Attack Scenario	Attackers with access, such as poll workers, could enable and disable the write protection on the cards throughout the election process. This could impact the integrity of the electronic voting data. Such an attack is likely to go undetected if smaller margins are maintained by the attacker, especially since the printed tape appears correct. The only audit measure would be to hand count the number of ballots in the ballot box versus the number read from the memory card at the central Board of Elections.

Mitigation Suggestion(s)	Access to the memory cards must be controlled using both keys and tamper tape. Ideally, the system should check the status of the write protection with every vote cast and if it detects a write protected card it should log and generate an audio alert that requires the poll worker administrative key to restore the component to operation and end the audio alert. Again, this would provide an additional level of tamper detection.

m650 Central Optical Scanner Vulnerabilities

ID #	COS - 1
Vulnerability Summary	Paper ballots are not serialized and can be scanned multiple times.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the scanner and/or to the ballots themselves, failure of general auditing processes
Attack Scenario	Because the ballots themselves are not serialized and no system detection of duplicate ballots takes place it is possible for duplicate ballots to be scanned by the system. Currently, Boards of Election audit the ballot counts and perform some level of inspections and dual-access controls to overcome these issues, but inclusion of electronic mechanisms would make this work less resource intensive and more accurate.
Mitigation Suggestion(s)	Optical scanning and paper ballot systems should become serialized to prevent tampering and rescan of ballots without notification. Proper memory and management systems should be implemented into the system to allow for this.
ID #	COS - 2
Vulnerability Summary	Manipulation of the *.pr file on the zip disk can cause tabulation errors, illicit counter values and firmware failure. Proper bounds checking is not performed on the input. This could likely be exploited to cause denial of service attacks or data corruption of the ballots being counted by the component.

Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the zip disk and that disk must be used to load vote totals onto the m650
Attack Scenario	Attackers could tamper with the zip disk contents to cause failure of the machine or impact the integrity of the current count causing availability issues and impacting the timeliness of the election process.
Mitigation Suggestion(s)	Proper bounds checking should be implemented on all inputs, regardless of their source, if they are exposed in any way to possible user manipulation. Additionally, reports generated when the counting subsystem has identified an overflow or roll-over should contain verbiage as such to indicate the presence of the counting problem.

Windows 2003 Small Business Server Vulnerabilities

ID #	SRVR - 1
Vulnerability Summary	Windows is not configured in accordance with industry standard best practices. Examples: BIOS passwords are not enabled. Password policies are not properly configured. Windows is not configured with adequate security settings.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Physical access to the component
Attack Scenario	Attackers who gain physical access to the component or malicious users can easily compromise the component, install malware or perform other illicit operations.

Mitigation Suggestion(s)	The component should be deployed in accordance with industry standard best practices as defined by NIST, SANS or the Center for Internet Security. Hardening the component to comply with these baselines would mitigate much of the exposures available for exploitation.
ID #	SRVR - 2
Vulnerability Summary	Component does not have a firewall or anti-virus software in place
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the component or the network on which it resides
Attack Scenario	Attackers could leverage these weaknesses to obtain illicit access to the component, escalate their privileges and/or install malware.
Mitigation Suggestion(s)	ES&S should adopt and deploy a common set of up to date tools for protecting the Windows 2003 Server and other components. At the very least a basic anti-virus package should be installed and used along with the Windows firewall. Boards of elections should adopt procedures for ensuring that these defensive tools and the operating system of the Windows Server 2003 stay up to date. They should identify mechanisms for doing this that DOES NOT INCLUDE exposing these systems to the Internet or any other populated network.
ID #	SRVR - 3
Vulnerability Summary	Integrity checking tools and intrusion detection/prevention tools are not deployed on the component
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the component or the network on which it resides

Attack Scenario	Attackers could utilize this lack of protection to replace the binaries, install malware or perform other nefarious actions against the component and its software.
Mitigation Suggestion(s)	The SoS should deploy Digital Guardian on the Windows components of the ES&S system as well as the other systems used for elections processes in Ohio. If properly installed, configured and managed to enforce a white list of specific applications allowed on the component, the security of the overall system would be improved.
ID #	SRVR - 4
Vulnerability Summary	The component is configured to operate with unneeded applications running. This exposes additional avenues of attack for exploitation. Examples: Internet Information Services (IIS) Exchange Terminal Services
Risk Rating	Low
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Network or local machine access
Attack Scenario	Any vulnerabilities discovered in the unnecessary services could be exploited by a local or remote attacker to potentially disclose information, perform denial of service, or compromise the component.
Mitigation Suggestion(s)	Disable services that are not used and harden components in accordance with an established best practices-based standard.

Windows XP Professional Workstation Vulnerabilities

ID #	WKS - 1
Vulnerability Summary	Windows is not configured in accordance with industry standard best practices. Examples: BIOS passwords are not enabled. Adequate logging is not in place. Password policies are not properly configured. Autorun is enabled. Windows is not configured with adequate security settings.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Physical access to the component
Attack Scenario	Attackers who gain physical access to the component or malicious users can easily compromise the component, install malware or perform other illicit operations.

Attack Scenario	Attackers could leverage these weaknesses to obtain illicit access to the component, escalate their privileges and/or install malware.
Mitigation Suggestion(s)	ES&S should adopt and deploy common up to date anti-virus software for protecting the Windows XP Professional Workstation and other components. Boards of elections should adopt procedures for ensuring that these defensive tools and the operating system of Windows stays up to date. They should identify mechanisms for doing this that DOES NOT INCLUDE exposing these systems to the Internet or any other populated network.
ID #	WKS - 3
Vulnerability Summary	Integrity checking tools and intrusion detection/prevention tools are not deployed on the component
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the component or the network on which it resides
Attack Scenario	Attackers could utilize this lack of protection to replace the binaries, install malware or perform other nefarious actions against the component and its software.
Mitigation Suggestion(s)	The SoS should deploy Digital Guardian on the Windows components of the ES&S system as well as the other systems used for elections processes in Ohio. If properly installed, configured and managed to enforce a white list of specific applications allowed on the component, the security of the overall system would be improved.
ID #	WKS - 4
Vulnerability Summary	The component is missing critical security patches
Risk Rating	High

Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Network or local machine access
Attack Scenario	An attacker could use publicly available vulnerability or exploit data to compromise the component and achieve access to modify or destroy the elections data.
Mitigation Suggestion(s)	Processes for installing missing patches and ensuring that operating systems and applications are maintained with current code should be developed and implemented. These processes should include the mechanisms needed to patch the components without exposure to any populated network or form of Internet access. Additionally, ongoing assessments or audits of the patch levels could be performed to ensure compliance with the established processes and to protect and preserve the integrity of the component's overall security posture.

Unity Software Vulnerabilities

ID #	SW - 1
Vulnerability Summary	Voting data can be edited directly in the Unity Software without additional access controls.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Physical access to the system, Access to the Unity Software
Attack Scenario	Attackers who gain access to the Unity Software can directly edit the results of the election without additional access controls. An insider who gains access to this function and the system could change vote totals and influence election results. While this functionality is logged to the database, an attacker with sufficient knowledge would likely be able to remove the log entries or create malware to remove the entries.

Mitigation Suggestion(s)	This functionality is intended to be a safety mechanism for recounts and other needs to modify apparent totals. However, access to these functions should require additional passwords, token use or other means of authentication. Use of this function should also be identified to the users and auditors of the election processes in multiple ways and be apparent on all election reports. Such oversight would minimize, but not eliminate the danger of this capability. Additionally, the vendor might consider removing this capability from the software and implement it in some other way or a different stand-alone application that requires additional levels of access and authentication to prevent its exposure during normal processing.
ID #	SW -2
Vulnerability Summary	Passwords are visible in the plain text of binary applications
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the binary applications
Attack Scenario	An attacker could view the string data contained in the binary applications, and extract passwords and other sensitive system information that could be used to compromise the elections software and data.
Mitigation Suggestion(s)	All strings of important security value should, at the very least, be obfuscated in the application code. Items such as passwords, encryption keys and other highly sensitive information should not be stored in the application, especially in plain text. ES&S should implement obfuscation of the strings in their application source code and/or move the items to some other location on the component (such as the registry), where they can be better protected and stored in an encrypted manner.
ID #	SW - 3
Vulnerability Summary	Various applications in the Unity Software package fail to perform input validation, file validation and proper bounds checking. This results in unhandled exceptions and possible exposure to overflow and other input-based attacks.

Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the component or to data read by the component
Attack Scenario	Attackers could potentially leverage one or more of these input validation issues to cause the execution of arbitrary code such as malware on the system. The attack could also likely impact the integrity and availability of the software applications needed to perform elections processing.
Mitigation Suggestion(s)	All applications in the Unity package should undergo a complete application source code review. Input validation and bounds checking should be verified on all user and file system exposed inputs to the applications. The application should also undergo rights reduction to eliminate the need for Administrator-level privileges. Such changes to the required operational context will reduce the impact and exposures of the identified input vulnerabilities.

Automark Unit Vulnerabilities

ID #	AM - 1
Vulnerability Summary	Attackers who disassemble the component can access the windows CE operating system just using a USB keyboard. Such access could result in the complete compromise of the component.
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the system to disassemble it, Security bit for the screws

Attack Scenario	Attackers could disassemble the system, gain access to the operating system and install malware that could impact the availability of the machine or possibly change the markings on ballots. However, since the voter physically sees the ballot as marked before moving to the optical scanner - discovery is quite likely. Such an attack would likely pose little threats to the integrity of the overall election, and would require a high level of insider knowledge for very little return.
Mitigation Suggestion(s)	Disabling the USB port and hardening the Windows CE installation in accordance with industry standard best practices would minimize the risks from this vulnerability. Additional placement of internal tamper seals would also allow easy detection of the access (especially during storage of the devices).
ID #	AM - 2
Vulnerability Summary	The audit log file for the system is loaded from the CF card, so tampering evidence could be easily destroyed.
Risk Rating	Low
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the Automark and CF memory card slot
Attack Scenario	Attackers could obtain access to the Automark and CF slot, then use their own CF cards to probe and attack the component. Results of the attempts to tamper with the system are logged to the CF making it easy for them to remove or destroy.
Mitigation Suggestion(s)	Logs should be preserved for some length of time on the internal storage of the component to allow forensic analysis of attempts to tamper with the device.
ID #	AM - 3
Vulnerability Summary	The password for the maintenance of the system is well known and is shown on-screen when it is being typed in.
Risk Rating	Low
Impacted Pillars	Integrity, Availability

Attack Prerequisites	Access to the Automark component
Attack Scenario	Attackers could observe the password or learn it from available sources and then use that knowledge and access to probe the system.
Mitigation Suggestion(s)	Passwords should be unique for each deployed component and should not be shown on screen when entered.

General Multiple Component Vulnerabilities

ID #	GMC - 1
Vulnerability Summary	Physical locks on the various components are easily circumvented using common lockpicking techniques. Keys are common among components and commonly available over the Internet. Affected components include: optical scanners, DRE units and ballot sorting/storage units and the Automark unit.
Risk Rating	Medium
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the system, knowledge of lockpicking, tools
Attack Scenario	Attackers with physical access to the devices and components could steal ballots, tapes, memory cards and other items. They could also tamper with or destroy components causing delays or other availability issues.
Mitigation Suggestion(s)	The locks need to be upgraded to more secure hardware. Keys should be system/device specific and access to the key sets should be controlled by strong processes. Where possible, tamper seals should be utilized in a common fashion to minimize the risks from this threat.

ID #	GMC - 2
Vulnerability Summary	Components lack tamper alarms to identify and alert on physical access attempts.
Risk Rating	Low
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Unattended access to components, Some components require security bits to remove cases
Attack Scenario	Attackers with physical access to the devices could open the cases of the electronic equipment and tamper with the internals, damage or destroy internal mechanisms or even implant Trojan hardware or firmware.
Mitigation Suggestion(s)	Electronic components should be engineered with sensors that alert the users of the component that cases have been opened or tampered with. Removal of those alerts should be controlled through an administrative function. This tamper detection/prevention mechanism is common in most secure devices today and should be engineered into the next generation of devices from ES&S. In the meantime, tamper seals should be placed on the equipment at critical points and used as a visual means to detect obvious tampering and attacks against the hardware during storage, transit, etc.

Summary

This report is intended to be a catalog of the identified vulnerabilities within the ES&S system and its components. Overall security implications and details of the engagement are contained in additional reports delivered to the Secretary of State's office.

Significant issues were identified during our review. Most of these issues seem to stem from a lack of adoption of industry standard best practices. Configuration changes, modification of default implementations and significant changes to the application and system architectures are required to mitigate the identified issues. These mitigation suggestions should be implemented as soon as possible to minimize the opportunity for exploitation by attackers. Additional mitigations or minimization of risks is likely possible through policy and process changes. This is explored in additional report documents delivered to the Secretary of State.