

## Detailed Response to Tabulation Upgrade Security Review & Risk Analysis

Section #	Issue	Response
<b>4</b>	<b>Operational Processes and Procedures</b>	
4.1.	Security Plan Review	
4.1.1.	Ballot Security Cage Physical Access Control Logs	Elections is able to access reports on a demand basis but agree they should be more readily available and is working with King County Security on a solution.
4.1.2.	Storage of Video Surveillance Tapes	Elections will explore options for storage of tapes and will work with King County Security on options.
4.1.3.	Access Control Deprovisioning Procedures	Elections current processes will strengthened and formalized.
4.1.4.	Insufficient Security Training	Security training is part of the comprehensive pre-election training for all temporary staff, however, this training was not observed by Anitian. Additionally Elections has Help America Vote Act funding for training purposes and will explore the options available for additional security training for managers and supervisors.
4.1.5.	Insufficient Review of Ballot Print Logs	Only authorized permanent Voter Services staff has access to the blank ballot stock to issue ballots. Blank ballot stock used to print OTC ballots is tracked by a stub numbering system and a stub audit log, which includes the date ballots were prepared, the beginning and ending stub numbers, and the signature of two authorized permanent Voter Services employees involved in the ballot preparation. This stock remains in secured locked storage. At close of business each day, two employees each perform an end of the day audit and sign the Ballot on Request OTC Daily Reconciliation and Daily Detail logs. The Program Manager and/or Supervisor are notified of any discrepancies or the inability to balance. The Daily Detail Logs, ballot stubs and spoiled ballots are placed in an envelope and the Ballot on Request OTC Daily Reconciliation Log is stapled to the outside of the envelope and placed in secured locked storage.
4.1.6.	No Criminal Background Check on Temporary Employees	Elections disagrees with the implementation of this recommendation. Given the technical and procedural safeguards in place it is not necessary to perform criminal background checks on temporary employees. Further, given the magnitude of temporary employees hired in order to conduct elections, it would be extremely costly and a significant administrative burden to implement. Managers and IT staff do have background checks done at the time of hiring.

## Detailed Response to Tabulation Upgrade Security Review & Risk Analysis

Section #	Issue	Response
4.1.7.	AVU Proofing Policy Inaccurate.	This procedure will be corrected.
4.2.	Operational Procedures Review	
4.2.1.	No Security Concerns	
4.2.2.	Procedures Needing Revision	The procedures identified in this list have either already been updated or are being updated at this time.
4.2.3.	Procedures with Security Concerns	
4.2.3.1	Insecure Ballot Data Exchange	Manager will ensure that this procedure is followed.
4.2.3.2	Lack of Observation and Supervision of Ballot Creation	Elections disagrees with this recommendation. Given the ballot proofing, testing and oversight conducted during the course of ballot building and testing it is not necessary to have a staff person observe the technician that performs the ballot build in GEMS. Limited staff resources can be applied to other areas to realize a more significant security advantage in the elections environment.
4.2.4.	Lack of Security Agreements with Printing & Inserting Vendor	The contract for this vendor expires this year and a security agreement will be negotiated as part of a new contract or contract extension.
4.2.4.1	AVC Memory Compartment Handling	The procedures will be reviewed and amended as recommended. The procedures for closing AVUs exists and was not reviewed by Anitian.
4.2.4.2	Handling of Memory Cards from Provisional Ballot AVU	Memory cards for the provisional ballot AVUs are clearly labeled. These procedures exist and will be reviewed and updated as necessary. It should be noted that Elections collaborated with the Office of the Secretary of State on the process and procedures for the provisional ballot AVU operation upon initial implementation of the solution.
4.3.	Disaster Planning and Recovery	
4.3.1.	Authority for Building Emergencies	The authority in the case of building emergencies will be formalized and documented.
4.3.2.	Emergency Management Responsibilities	Elections will work to establish procedures as recommended in the report.
4.3.3.	Insufficient Uninterruptable Power Systems	An uninterruptible power supply solution for the scanning environment has been purchased, is on site, and has initially been test and comprehensive testing will happen soon.
4.3.4.	On Site Storage of System Backups	An offsite storage solution will be explored.

## Detailed Response to Tabulation Upgrade Security Review & Risk Analysis

Section #	Issue	Response
4.4.	KCE Facility	
4.4.1.	Visitor Check-in Process Deficiencies	Visitor check-in processes have already been revised. During election periods, elections will work with onsite Sheriff deputies to conduct security sweeps at the end of night to augment the security sweeps already conducted during operating hours. Further security is provided by motion detectors and other security measures. Every staff has received training on these procedures. Based on the election calendar the badges expire after certification of the election and have hours limitation for exterior doors.
4.4.2.	Color Coded Network Cables Are Visible In Public Areas	Elections disagrees with this recommendation. The visible color coded network cables are intentional resulting from a decision made during the construction of the building to provide transparency on the advice of elections and security experts.
4.4.3.	Weaknesses in Physical Access Controls	This is an issue of balancing efficiency, security and cost. Elections has evaluated these concerns and believes that current practices are more than adequate considering the layers of security in place. Elections and King County Security are working with the security system vendor on previously identified issues that were observed by Anitian. Since Anitian's inspection, numerous issues have been resolved. All alarms are responded to by Elections managers and supervisors.
4.4.4.	Fire Suppression System Concerns	The fire suppression system in Elections facility is consistent with nearly every elections office across the country. Alternative systems are cost prohibitive and could pose a potential health hazard to staff.
4.6.	Mock Elections Review	
4.6.1.	Lack of Vendor Support	Elections has worked with the vendor on support issues and resolved concerns experienced during the mock election. However, this is an issue that requires ongoing diligence and Elections will continue to work with the vendor and other jurisdictions on this issue.

## Detailed Response to Tabulation Upgrade Security Review & Risk Analysis

Section #	Issue	Response
4.6.2.	Test Environment Not Exact Duplicate of Production	The staff that performed the acceptance testing was consistent with our plan and always intended to do so. Procedures were developed during the acceptance testing process and further tested and refined during the trial election. It should be noted that the acceptance process conducted by Elections was one of the most rigorous ever conducted upon a voting system. Elections researched best practices and retained an expert consultant to develop test plans. The acceptance testing was not intended to test the system in full scale election mode. The point of the mock election was to test all the capabilities of the system required to conduct an election in the order they need to occur.
4.6.3.	Variation From Acceptance Testing Plan	
4.6.3.1	Adjudication of Ballots	The number and ballots adjudicated during the mock election was altered to conform to testing expectations of the Office of the Secretary of State. Rigorous testing of adjudication was done during the volume test and during the trial election.
4.6.3.2	UPS Testing	A UPS solution has been delivered and initially tested successfully. Further testing will continue.
4.6.3.3	Production Rates	This was done during the volume test.
4.6.4.	Lack of Procedural Development	While Anitian did not observe a formalized effort to use the Mock Elections to evaluate and refine the processes and procedures, this did occur. The technical staff and ballot processing staff on the vote by mail team did extensive work on procedural development throughout the acceptance testing process which included taking screen shoots, taking extensive notes, and revising procedural processes extensively. It was communicated by Premier that documentation would not be finalized until certification of the system at the federal level.
4.6.5.	Hardware/Software Integration Success Metric	Anitian recommended additional testing was conducted.
4.7.	Ballot Scanner Process Review	Elections will examine the recommendations offered in this section and implement those that enhance the security of the environment.
4.7.1.	Ballot Processing Log	
4.7.2.	System Authentication	
4.7.3.	User Rights Provisioning	
4.7.4.	Ballot Flow Management	

## Detailed Response to Tabulation Upgrade Security Review & Risk Analysis

Section #	Issue	Response
4.7.5.	The Commit Process	
4.8.	Electronic Duplication Process Review	The draft procedures initially reviewed by Anitian have already been updated. Elections will examine the recommendations offered in this section and implement those that enhance the security of the environment.
4.8.1.	Recommendations	
<b>5</b>	<b>Technical Review</b>	
5.1.	Mock Election Observations	
5.1.1.	Code Changes	Elections will discuss with Premier the possibility and advisability of addressing these in a future release. For the present, KCE will mitigate through internal procedures and training.
5.1.2.	Procedural Changes	Elections does not believe this is a security issue.
5.1.3.	Acclimation to the System	Elections conducts extensive training before each election in order to mitigate these issues. Further, the conduct of the mock election, volume test and trial election has provided us more experience with the equipment and staff has learned how to manage these issues.

## Detailed Response to Tabulation Upgrade Security Review & Risk Analysis

Section #	Issue	Response
5.1.4.	Errors Reported	Eleven specific errors are reported in this section and a response, clarification or resolution is detailed below. 1. DTNP doesn't actually use SSL or perform any SSL handshake,- the problem is caused by a bug in Windows XP related to cryptographic key containers that has since been corrected. 2. The multiple issues here have been resolved. In the case of the system freezing, which still occurs on occasion when the application is restarted, the operator can pick up where they left off with no loss in data. 3. This is an issue that we are requesting Premier work with DRS to resolve. 4. This issue was corrected. 5. This has been resolved- if a workspace is locked and not editable, a new work space token can be created.6. Same as # 2 above. 7. Pink lines on the display image of the ballot were often the result of a dirty scanning unit. When the units were cleaned, these issues were mostly mitigated. In some instances calibration or more detailed diagnostics were necessary to resolve these issues. 8. This issue was corrected. 9. Redundancy measures in the system mitigate this issue. 10. This issue was corrected. 11. Each of these instances were sent by the system to adjudication. In a live election the ballot reconciliation would have been off for each of these batches further alerting us to the issue and the batch would have been rescanned.
5.2.	General Threats	
5.2.1.	Third Party Software Uses Older, Deprecated Versions	We will request that Premier update third party software as soon as possible within future certification parameters.
5.2.2.	Windows Hosts Insufficiently Hardened	We will work with Premier to implement one of these tools to improve Assure system hardening.
5.2.3.	Windows Firewall	Elections will investigate the benefits and ramification of these recommendations considering that the environment for the system is entirely closed.
5.2.4.	Incomplete System Documentation	Elections now has final versions of all documentation from Premier.
5.2.5.	Critical Windows Patches Not Applied in a Timely Manner	The Office of the Secretary of State confirms that it is acceptable in Washington State to install vendor approved Operating System Security patches and/or service packs. Elections will work with Premier to test critical patches in a timely manner.
5.2.6.	Network Time Protocol (NTP) Service Not Running	Elections will explore this issue with Premier and work to synchronize clocks on all the computers on the network.

## Detailed Response to Tabulation Upgrade Security Review & Risk Analysis

Section #	Issue	Response
5.2.7.	Insufficient Event Log Collection	As part of ongoing election activity log data is collected. Elections will review options with Premier for a central logs server.
5.2.8.	Windows Security Policies Distributed by a Third Party	Elections will request that Premier provide their own security policy as part of ongoing contract discussions
5.2.9.	Untrusted Publisher Security Warning Displayed when PCS Runs	The certificate is added to the trusted list in the final version to be certified.
5.3.	Accessible Voting Unit Threats	
5.3.1.	Memory Card Tampering – Redirect Results To an Incorrect IP Address	This issue is mitigated by the multiple layers of security employed in the elections environment. The only AVU that uses network communications is the upload terminal connected to the GEMS server. This unit is located in a room protected by biometric key cards with an extremely limited number of authorized individuals having access rights. This room is also under 24x7 recorded video surveillance. Physical security measures prevent or provide detection of unauthorized access to memory cards. Further, the reconciliation process for votes cast on AVUs at the Accessible Voting Centers would detect any misdirection of result accumulation in GEMS. Elections will officially request of Premier that all files on the memory card are hashed.
5.3.2.	Memory Card Tampering – Instruction Modification	This issue is mitigated by the multiple layers of security employed in the elections environment. Physical security measures prevent or provide detection of unauthorized access to memory cards. Elections will officially request of Premier that all files on the memory card are hashed.
5.3.3.	Memory Card Tampering – Script Injection	This issue is mitigated by the multiple layers of security employed in the elections environment. Physical security measures prevent or provide detection of unauthorized access to memory cards. Elections will officially request Premier that all files on the memory card are hashed.
5.3.4.	Memory Card Tampering – No Audit Logs	Elections will officially request that Premier improve the audit logs for the AVUs. Elections will implement procedures to log all none standard events when working with AVUs.
5.3.5.	Dedicated Workstation for Encryption Key Generation	This was a misinterpretation or misunderstanding. The laptop identified by Anitian does not have the Key Card Tool application on it or a card reader necessary for this

## Detailed Response to Tabulation Upgrade Security Review & Risk Analysis

Section #	Issue	Response
		operation. The laptop had been a shared resource at one time so it was accompanied by a password on a post-it note, that is no longer valid.
5.4.	PCS Threats	The DTNP protocol does not use DCOM. The system does not use a Microsoft Access database file format. The 2GB limitation is not an issue.
5.4.1.	Weak Workstation Authentication Measures	Elections will work with Premier on the option of limiting application logins. However, keeping the card in the station used for tallying results is not an option with the tally token. We do not necessarily want the card to stay in the reader. We will review our procedures with the Office of the Secretary of State to ensure security.
5.4.2.	Required Cards Are Not Enforced	It is not Premier's instruction to close a deck using ender cards. Elections agrees that the step of closing an open deck of ballots on the scanner with a Deck Ender Card operationally should match the screen, we have tested the closing of a deck both ways and do not see this a major issue.
5.5.	GEMs Threats	
5.5.1.	Decks and Audit Logs Can Be Deleted	Deck data is maintained in two distinct software applications in the tabulation system. While data can be deleted in the legacy GEMS program, the PCS program still maintains the data in a secure, encrypted format. Furthermore, deletion of any deck would be detected through Elections' rigorous reconciliation process. Elections will formally request that the vendor correct this issue in GEMS.
5.5.2.	Encoded Timestamps	Elections does not see this as an issue, the date and time of the logs are displayed correctly through the application.
5.6.	ASM Threats	
5.6.1.	ASM Logs Lack Detail	We concur that the log lacks detail, and will officially request Premier enhance the ASM logs in the next release of the software.
5.6.2.	ASM Token Pin Creation is Displayed in Plain Text	This process is now done in the secure server room which has highly limited access. Election will official request to Premier to make this change.
5.6.3.	ASS is Running as Local System.	Premier has indicated that they will do more research on this issue, however, Assure is a local system and can only be changed by administrators on windows or the Assure Security Service.
5.7.	Photostripe Scanner Threats	

## Detailed Response to Tabulation Upgrade Security Review & Risk Analysis

<b>Section #</b>	<b>Issue</b>	<b>Response</b>
5.7.1.	Hardware Failures Caused Sorting Profiles to Be Lost	Administrative procedures have been put in place to mitigate this issue. Elections is requesting that Premier allow us to set the default sort profile so that if the profile is lost upon rebooting the machine the correct profile would be set.
5.7.2.	Loss of Configuration Key When Units Are Repaired	Elections will work with Premier so that the keys are available when needed.