Executive Summary

Business and Technical Threat Risk Assessment for: Electronic Voting

City of Edmonton
Office of the City Clerk, Elections and Census

Document ID: 2476

December 10, 2012

Confidential

Revision History

Version	Date	Description of Revision	Authored/Modified By
1.0	November 22, 2012	Initial Release	K. Grant
2.0	December 10, 2012	Final Release	K. Grant

1.0 Executive Summary

During October and November, 2012, Seccuris Inc. completed a business risk and technical risk assessment of the Jellybean Election system (from Scytl Canada). The scope for the assessments was not solely the Internet Registration and Voting solution used for the Jellybean Election; the assessment also considered the risks if the City were to use this same solution in an official election.

The business risk assessment was conducted through reviews of the City of Edmonton's business drivers and processes for an internet election system as well as interviews with business and technical staff. Seccuris also interviewed the internet election system provider, Scytl, as well as conducted an in-depth review of current documentation relating to the Jellybean Election.

The technical risk assessment was performed using technical scanners to review the security and controls on the public-facing website provided by Scytl. The public-facing website was only used to host the Jellybean Election system. This assessment and testing was conducted to determine the level of impact of any discovered vulnerabilities that could adversely affect systems or the network, and provided recommendations to correct or mitigate these vulnerabilities.

In order to conduct a business and technical risk assessment, existing business drivers, business processes and the current technical system architecture are used as inputs to identify potential threats, (i.e. what can go wrong), identify the possible risks, (i.e. what is the risk to the business should the threat occur and the probability of the occurrence), and the impact of these same possible risks to the City if these identified risks would be successfully exploited.

The items listed below highlight the highest priority areas to reduce the City's business and technical risks to an acceptable level, if the same internet voting solution is implemented. From a business process perspective, we recommend that the following be implemented to address these areas:

- Prior to the Jellybean Election and the Seccuris assessment, the Elections Team completed a Privacy Impact Evaluation on the Jellybean Election, which was reviewed with City FOIP staff. The Elections and FOIP teams determined that a Privacy Impact Assessment was not required for the Jellybean Election. Due to the importance of an official election, a more comprehensive privacy review is recommended which can help determine if current controls related to highly sensitive personal information are sufficient and effective. Recommendations in the Privacy Impact Assessment should be implemented, as required.

- Once all of the manual processes are formalized and documented, a test of those processes should be performed to ensure that voters' highly sensitive private and confidential information (e.g., scanned driver's licence and passport) is protected accordingly.

- The City should fully document robust administrative and procedural processes and carry out a formal training process for staff working in a real election.

From a technical perspective, the following recommendations should be implemented to address areas to provide robust security and privacy protections:

- Activation of selected features (that we observed were not activated for the Jellybean Election system) such as encryption in storage and transmission, and audit logs features. We further recommend the enactment of formal processes to review all audit logs generated by the election system to ensure that any incidents are reviewed and followed up using a formal incident response process. These features can provide robust security and privacy protections.

- Certification and accreditation of the vendor's software and the system setup should be conducted in order to detail the security posture of the systems and the mitigation remedies. This process comprehensively evaluates technical and non-technical features of the system in its environment so that it can be determined whether or not the system can operate at the accepted level of risk based on the implementation of an approved set of technical, managerial, and procedural safeguards.

- Separation of the physical and logical internet voting environment (the actual machine, and logical access to the machine, that houses the City's election system) so that it is not shared with Scytl's other clients.

The results of these assessments have provided recommendations that, once implemented, maximize or enhance the protection of confidentiality, integrity, and availability of the system and associated processes while still providing functionality and usability.

It is the opinion of Seccuris that once the City applies the recommendations for technical, security and process improvements, the City will have a system with robust security, the required formally documented processes and well-trained staff to potentially run a production internet voting option during an election.

