

**Opening Comments by the**

**Acting Auditor General**

**Public Accounts Committee**

**IT Security – Public Interest Report**

**26 February 2016**

Mr. Chairman, members of the Public Accounts Committee, officials from the Ministry of Finance, ladies and gentlemen in the gallery. Good morning.

**Introduction**

1. I have with me today Mr. Martin Ruben, the audit director responsible for performance audits. Thank you for the opportunity to make some opening remarks.
2. The Cayman Islands Government is highly dependent on information technology for the management of its business and the delivery of public services. It operates a large and complex computer network that stores critical and sensitive information to enable government to function. Information is a key asset for the CIG, which needs to be managed well. This information needs to be effectively collected, processed, stored, and transmitted. Failure to protect the confidentiality, integrity and the availability of CIG’s information at any stage where it is handled can result in significant reputational, operational, legal and potentially national security risks.
3. As a result of the significant concerns we had from our review of IT Security in 2012, we requested Deloitte to conduct a follow-up review in 2015. While we felt it was not in the public interest to report the results of the 2012 study and provide an opportunity for Government officials to act on its recommendations, the results of our recent review indicated that we needed to raise our concerns publicly in order for them to be acted upon by Government.

**Findings**

1. We found that the confidentiality, integrity, and availability of the Government’s IT systems and information continue to face significant risks and threats from attack.
2. We noted that IT governance and security has not been a priority for Government managers. Government needs to ensure that IT and information governance and security is afforded the priority it requires, and that it is seen as fundamental component in the efficient and effective management of government business and delivering public services.
3. Government needs to develop a clear strategy for IT and information management, establish appropriate governance structures with accountability for IT and information security, allocate the necessary resources to implement, monitor progress and periodically report to the Legislative Assembly on how well it is doing.
4. I also want to highlight significant governance issues that were identified:
	1. Roles and responsibilities are not well defined for who has ownership of IT Development across Government, and in particular for IT and information security.
	2. There is a lack of risk management practices in the Computer Services Department and across government when considering IT security.
	3. The development and acquisition of IT systems cross government is not guided by a strategic plan leading to ad-hoc development/purchase of IT systems.
	4. There is no overall investment plan that captures all of the IT purchases across government, which ties into Government’s mission in regards to IT infrastructure.

**Conclusion**

1. In conclusion, we found that IT security has not been a priority for the Government and that is something that needs to be addressed urgently to ensure that government systems and data are protected against potential threats.
2. With Government wanting to move to E-Government and to deliver public services more efficiently, effectively and with increased customer focus, the demand for information technology with increased functionality and availability will continue to increase within this ever changing global environment. Therefore, it is becoming more critical that government protects its systems and data against cyber threats.
3. Our report includes six recommendations that, if properly implemented, should address our concerns and help protect the Cayman Islands Government IT systems and information in the future.
4. Thank you.