GOVERNMENT OF BERMUDA

CABINET OFFICE

INFORMATION TECHNOLOGY OFFICE

6 September 2016

Sir Anthony H.M. Evans
Chairman, Commission of Inquiry
Box 20
Swan Building
26 Victoria Street
Hamilton HM12

Dear Sir,

Re: ITO Response to the Commission of Inquiry

The ITO was asked if we agreed with the IT deficiencies and whether they have been addressed. When responding it is important to explain that some of the IT deficiencies and recommendations were addressed to the Accountant General. Where the deficiencies and recommendation were addressed to the ITO, the ITO generally agrees with and has addressed the deficiencies, but it should be recognized that IT security remains a challenge in the modern business environment.

Accordingly, IT Security has been identified as priority in the ITO business plan and consequently the procedures and technology for the management of IT Security have been improved as recommended in the closing sentence of the section entitled "3.17 Information Technology (IT) deficiencies" of the Auditors Report. An IT Security Programme has been established to monitor risks, set priorities and implement. A Security Manager and Security Analyst have been hired. The Security policy has been updated and approved by Cabinet. Separate budget line items have been established for the management and improvement of IT Security.

Following is the ITO response to each deficiency.

1. Weaknesses in access rights/privileges
    a. The ITO controls rights/privileges for the Network Accounts and the Accountant General controls rights/privileges to the E1 system. The details in the report referred to the E1 system. One must first sign on to the Network in order to then select and sign on again to the E1 system.
    b. The rights/privileges regarding Network Accounts are reviewed and updated by the ITO on a monthly recurring basis for selected departments. This means that the full list of accounts for each department are reviewed annually. Routine account changes are authorized by Department Heads and logged through the ITO Service Desk. The account authorization forms are attached to the ITO Service Ticket. Annex A contains the Ticket details for the last review of the Accountant Generals Department.

Channel House 12 Longfield Road
St. Georges DD03 Bermuda
Phone (441) 297-7733 Fax: (441) 295-2948 Email:moatley@gov.bm

2. Lack of password policies
    a. The Password policy has been established by the IT Security Policy and is enforced for the Network Accounts at sign-on time. Paragraph 6.2.5 of the IT Security Policy (See Annex B) stipulates that computer devices and applications must be protected by a password that meets the standard set by the Director of the ITO.
    b. The current Complex Password Standard approved by the Director of the ITO (See Annex C) is posted on the ITO Intranet site along with the IT Security Policy.
3. Formal change management and problem/incident management procedures were not in place.
    a. The ITO manages changes, problems & incidents for the IT System Infrastructure that hosts the E1 application. The Accountant General manages the changes, problems and incidents for the E1 Application. The ITO processes for Change, Problem and Incident management are long standing and well established.
        i. The ITO maintains a Change Management Process for IT System changes and the Change Advisory Board reviews changes weekly. A flowchart of the Change process is at Annex D. Annex E shows a print screen of current Change Tickets.
        ii. The ITO maintains Problem and Incident management processes (See Annex F and G) respectively. Annex H and I contain print screen example of Problem & Incident Tickets.
4. Disaster Recovery Plans and Business Continuity Plans were not finalized and updated.
    a. The ITO maintains DR Documentation for the Financial Management System E1 that is normally reviewed and revised annually as part of a DR Exercise carried out in cooperation with the Accountant General. Annex J contains the latest version of the DR Documentation and DR exercise.
    b. In recent years a number of activities have been carried out that demonstrate DR capability for the E1 System. A total restore of the E1 System was carried out as part of relocating the System to a new High Availability Data Center in October 2013 and this restore was accepted by the Auditor General as proof of recovery capability. A DR exercise was carried out in cooperation with the Accountant General on the 8th August 2014. The DR site was relocated during 2015/16 to realize cost savings and processes are being refined to reflect the new location. A test exercise of the new DR site in cooperation the Accountant General is scheduled for 30 September 2016.
5. One open-ended contract resulted in significant modification costs as well as undue reliance on one individual.
    a. The ITO is not aware of the basis of this observation.
        i. There are no open ended support contracts in the ITO.
        ii. The ITO is challenged with key man risks from time to time that emerge when working with minimum human resources. However, the challenge with respect technical support of the IT Systems infrastructure that hosts the E1 Application were addressed by reorganization and recruitment in 2011. The ITO compliment includes more than one person to support the key systems including the E1 Application.

6. Weaknesses in the Virtual Private Network
    a. Account Administration has been improved to secure and log Department Head authorization of VPN account setup. The VPN account setup form includes an automatic expiration date. Annex K contains an example of the VPN Account Form.
    b. As an additional measure, the routine annual department account list review referred to above in paragraph 1.b. will close Network Accounts not authorized by a department and this activity will also close access to VPN accounts.
    c. The Security Programme includes additional risk mitigation measures to audit VPN account administration and monitor the network for suspicious or anomalous activity.
7. Security Policy not implemented
    a. The Security Policy has been updated and approved by Cabinet Conclusion 15(43)4. The policy is at Annex B.
    b. A number of activities are ongoing related to implementing the Policy. Some are: the Security Policy is published on the ITO Intranet site; awareness and training is included as part of the new employee induction training; Department Heads were informed of the policy via a presentation at Department Head meeting; the routine ITO service management meetings with Departments maintains awareness of the Security Policy and important risk mitigation measures/practices that deserve attention or action; the ITO broadcasts email alerts of general risk mitigation actions required by all users.
    c. A "banner message" is displayed at logon time and informs users of the need to comply with the Security Policy. (Annex L contains the banner message).
    d. A new application has been procured and installed that will be used to secure and log agreement with the IT Security policy by management and key technical personnel in the Civil Service.
8. Operations and emergency procedures not documented.
    a. Annex M contains: the Operations & Support documentation prepared by the ITO and the Accountant General; Appendix A to that document that contains the Operations Procedures & Troubleshooting documentation; and, the latest update (2015) of the E1 configuration documentation prepared by Denovo for the Accountant General which is the company that provides support for the E1 application.
9. A Risk Assessment and Risk Assessment Plan have not been prepared
    a. A Risk Register was developed in accordance with industry standards and has been reviewed by Cabinet.
    b. The ITO senior management team reviews a Risk Register monthly to monitor developing situations and determine priority for action.
10. Lack of a policy on disposal of IT devices.
    a. The Security Policy addresses disposal of IT devices. See Annex A, paragraph 6.7.2 of the Security Policy.
    b. Hard drives are removed from devices and physically destroyed.

The ITO has tried to respond concisely and include Annexes to demonstrate progress with addressing the Auditors Observations and Recommendation.

The response is respectfully submitted for your information.

Sincerely,

MJOM.

Michael J. Oatley
Director - ITO

Annexes:

A – Ticket last review of Network Accounts for the ACG

B – IT Security Policy

C – Complex password

D – Change Management flow chart

E – Example of Change tickets

F – Problem Management process

G - Incident Management process

H - Example of Problem Tickets

I – Example of Incident Tickets

J – Disaster Recovery Documentation

K – Example VPN Account Form

L – Sign on banner message

M – JDE E1 Operations and Support documentation