

**INFORMATION SYSTEMS REVIEW REPORT
OF THE
ELECTORAL COMMISSION OF JAMAICA**

**Auditor General of Jamaica
Auditor General's Department
8 Waterloo Road, Kingston 10
Jamaica, W.I.
www.auditorgeneral.gov.jm**

November 2012

TABLE OF CONTENTS

AUDITOR GENERAL'S OVERVIEW	5
EXECUTIVE SUMMARY	7
KEY FINDINGS.....	8
<i>ELECTOR QUALIFICATION: MINIMUM AGE.....</i>	<i>8</i>
<i>VOTERS' LIST EXCEPTIONS</i>	<i>8</i>
<i>PROCESSING OF DEAD ELECTORS.....</i>	<i>8</i>
<i>ACCESS CONTROLS & ENVIRONMENTAL SECURITY</i>	<i>9</i>
<i>BUSINESS CONTINUITY & CHANGE MANAGEMENT.....</i>	<i>11</i>
<i>IT GOVERNANCE.....</i>	<i>11</i>
<i>CORPORATE GOVERNANCE: BREACHES OF THE ECIA</i>	<i>12</i>
<i>CORPORATE GOVERNANCE: SALARY DISCREPANCIES.....</i>	<i>12</i>
RECOMMENDATIONS	13
PART ONE	16
INTRODUCTION.....	16
BACKGROUND.....	16
AUDIT SCOPE AND METHODOLOGY	18
LIMITATION OF SCOPE	19
PART TWO	21
ELECTOR QUALIFICATION: MINIMUM AGE.....	21
INADEQUATE AGE VERIFICATION PROCEDURES	21
PART THREE	23
VOTERS' LIST EXCEPTIONS	23
VOTERS' LIST CONTAINED NUMEROUS ELECTORS WITH STATUS EXCEPTIONS.....	23
PART FOUR	25
PROCESSING OF DEAD ELECTORS.....	25
ECJ'S DEATH VERIFICATION PROCEDURES WERE INADEQUATE.....	25
PART FIVE	28
ACCESS CONTROLS & ENVIRONMENTAL SECURITY	28
ECJ DID NOT HAVE A COMPREHENSIVE INFORMATION SECURITY POLICY	28
INADEQUATE CONTROLS OVER LOGON IDs AND PASSWORDS	29
INADEQUATE CONTROLS OVER ADMINISTRATOR ACCOUNTS/ACTIVITIES.....	30
INADEQUATE DOCUMENTATION OF SYSTEM PROCEDURES	31
EXCESSIVE USER PRIVILEGES	31
FORMER EMPLOYEES WITH LOGON ACTIVITIES & ACTIVE ACCOUNTS	31
UNACCOUNTED FOR ACTIVE ERS USER ACCOUNTS	32
MULTI-USER NETWORK ACCOUNTS	32
DELETED USER ACCOUNTS.....	32
INADEQUATE CONTROLS OVER ACCESS CARD SYSTEM	33
<i>No Documented Policy.....</i>	<i>33</i>
<i>Inadequate Review of Access Rights</i>	<i>33</i>

<i>Unencrypted Access Codes</i>	34
<i>Re-assignment of Access Cards</i>	34
<i>Employees Not On the Card Credential List</i>	34
INADEQUATE MAINTENANCE OF COMPUTER AND RELATED EQUIPMENT	35
PART SIX	36
BUSINESS CONTINUITY & CHANGE MANAGEMENT	36
INADEQUATE TESTING OF BUSINESS CONTINUITY & DISASTER RECOVERY PROCEDURES	36
INADEQUATE CHANGE MANAGEMENT CONTROLS	37
PART SEVEN	38
IT GOVERNANCE	38
ECJ DID NOT ESTABLISH AN IT GOVERNANCE FRAMEWORK	38
ECJ HAS NO INTERNAL IT AUDIT CAPACITY	39
PART EIGHT	41
CORPORATE GOVERNANCE: BREACHES OF THE ECIA	41
ECJ HAS MULTIPLE OUTSTANDING AUDITED FINANCIAL STATEMENTS	41
NO OATH OF SECRECY WAS SIGNED BY ECJ STAFF	42
PART NINE	43
CORPORATE GOVERNANCE: SALARY DISCREPANCIES	43
UNAPPROVED EMOLUMENTS	43
ECJ IN BREACH OF MOFP SECURITY ALLOWANCE GUIDELINES	44
ECJ IN BREACH OF MOFP GUIDELINES ON QUALIFICATION INCREMENTS	44

AUDITOR GENERAL'S OVERVIEW

The primary objective of the Electoral Commission of Jamaica (ECJ) is to safeguard the democratic foundations of Jamaica by enabling eligible electors to elect, through free and fair elections, their representatives to govern Jamaica. The functions of the Commission include, establishing policies for governing the registration of electors, compiling and maintaining the register of eligible electors and verifying the identity of electors.

Over the years, beginning with the former Electoral Advisory Committee (EAC), the ECJ has sought to address the inadequacies of the elector registration system by embarking on a sustained effort to utilise technology to effect electoral reform. The Commission has since implemented a number of information and communication technology systems in an effort to improve the elector registration and identification process. These systems include an Elector Registration System (ERS) incorporating the use of fingerprint cross-matching technologies and an Electronic Voter Identification and Ballot Issuing System (EVIBIS).


These improvements have led to Jamaica being recognized as having an electoral system that is on par with most modern and mature democratic nations. The use of information technology (IT) in the electoral system leads to greater efficiency in the management and control of the overall electoral process. However, the rapid pace of IT evolution increases the risk that the Commission's control mechanism is not commensurate with the sensitivity and security of elector information that it has in its custody. In this evolving technological environment, existing controls should be regularly reviewed to determine their continued effectiveness.

In keeping with my constitutional mandate, I commissioned an information systems review of the operations of the ECJ to determine whether adequate systems, policies and procedures were in place to preserve the integrity and confidentiality of elector information, the achievement of the Commission's objectives and the safeguarding of its assets.

Our review revealed weaknesses in the ECJ's information technology control environment relating to areas such as corporate and information technology governance, information and system security, elector registration, processing of dead electors and the production of the Voters' List.

This report is intended to assist the Commission to further strengthen Jamaica's highly regarded electoral system. It is therefore crucial that the Commissioners and the management of the Electoral Commission of Jamaica carefully review the recommendations contained in this report with a view to strengthening its control systems by adopting the measures outlined.

I wish to thank the management and staff of the ECJ for the courtesies extended to my staff during the audit.


Pamela Monroe Ellis, FCCA, FCA, CISA
Auditor General

This page was intentionally left blank.

EXECUTIVE SUMMARY

The Electoral Commission of Jamaica (ECJ) was established in 2006 by way of the Electoral Commission (Interim) Act. The functions of the Commission include the compilation and maintenance of the register of eligible electors, the production of the Voters' List for elections and the conduct of Parliamentary and Local Government Elections, By-Elections and Referenda.

The work of the Commission is increasingly reliant on technology to manage and control the electoral process. It aims to utilize technology to improve the efficiency and integrity of the elector registration, identification and voting processes by incorporating the use of fingerprint cross-matching technologies to prevent multiple registrations and voter impersonation.

Our audit focused on assessing the efficiency and effectiveness of the ECJ's general computer controls as well as the application controls relevant to its Elector Registration System (ERS) and Electronic Voter Identification and Ballot Issuing System (EVIBIS) to determine whether systems, policies and procedures were in place to preserve the integrity and confidentiality of elector information processed by the two systems. We also assessed the impact of the ECJ's control environment on its mandate and level of service delivery. Our review concentrated on the adjusted November 2011 Voters' List that was used in the March 2012 Local Government Election.

The audit did not include any review or cross matching of elector fingerprint data, poll book or other election documents that are restricted under the Representation of the People Act. We also did not conduct any network penetration testing or simulation. Our assessment was based on the review of official ECJ documents and records, statutes and other related articles, analysis of the ERS and related data, observations of processes and procedures, and interviews with senior officers and staff of the ECJ.

We identified several weaknesses in the ECJ's information technology control environment relating to areas such as corporate and IT governance, information and system security, elector registration, processing of dead electors and the production of the Voters' List. The key findings and recommendations are outlined below.

KEY FINDINGS

ELECTOR QUALIFICATION: MINIMUM AGE

1. Section 111(3)(a) of the ROPA states that *“no person shall be entitled to vote in any polling division if he is under the age of eighteen years”*. **Nonetheless we found that the Commission did not have an effective system in place to routinely verify the age or date of birth of each applicant.** Applicants were not routinely required to provide proof of age at the time of registration. However, the Commission stated, *“where objections are raised based on age, such persons are summoned to sittings by the Returning Officer and at that time are required to provide proof of age. If they fail to provide proof, or fail to turn up, they are not added to the Voter’s List”*. The ECJ further asserted, *“The ROPA does not give the Director of Elections the authority to demand birth certificates from persons seeking to be registered”*. However, it is our view that the absence of an effective age verification system increases the risk of registering under-age applicants as legitimate electors. This also reduces the reliance that can be placed on the identification cards produced by the Commission that are used as de-facto national IDs.
2. **An analysis of the adjusted November 2011 Voters’ List revealed that there were 48 electors without a date of birth at the time the list was generated.** We were therefore unable to determine if those electors attained the prescribed age at the time of registration.

VOTERS’ LIST EXCEPTIONS

3. **Our review of the adjusted November 2011 Voters’ List revealed that 133,845 electors were flagged as having bad prints, bad photo or missing information in the ERS. While another 3,137 and 2,922 electors were flagged as having wrong fingerprints and no fingers respectively.** However, the ECJ did not have as a standard operating procedure, a mechanism in place to target high risk groups such as these electors for re-verification in order to determine their authenticity. The Commission asserted that *“the system as developed in 1996, created a category for such electors (missed) to facilitate their inclusion on the list once they satisfy all other criteria”*. The ECJ further noted that *“these exception features are a form of identification”*. It should, however, be noted that these exceptions are not displayed on the Voters’ List and could only be used to identify an elector at polling stations where the EVIBIS is used. It is an information system security best practice to have a mechanism in place to review system exceptions especially where the risks associated with these exceptions are assessed to be high.

PROCESSING OF DEAD ELECTORS

4. **We found that the ECJ’s dead electors processing procedures did not take into account any death data from the Registrar General’s Department (RGD) as required by section 8 of the Representation of the People Act (ROPA).** Instead, reliance was placed on death notices published in the press and information from members of the public. The Commission stated, *“While the ROPA requires the RGD to provide the EAC/ECJ every three months with lists of the dead over the age of 18 years, the lists provided before the automation of the RGD records were*

only marginally useful as they included all persons who died without providing dates of birth and ages”.

Since this discrepancy was brought to the ECJ’s attention, the Commission has reportedly obtained death data from the RGD for the period 2006 to March 2012. **We take this opportunity to commend the ECJ for taking steps to implement the necessary corrective measures, which have so far enabled the Commission, since 2012, to remove 10,459 dead electors from the adjusted November 2011 Voters’ List.** Given the requirements of the ROPA and the verification process to confirm and remove a dead elector from the Voters’ List, we believe that it is important that the ECJ formulate an arrangement with the RGD to ensure that the death data is received on a quarterly basis as required by the ROPA.

5. **We found no evidence that the ECJ had the authority to review certain election documents such as the “Poll Book” that is used to record the names of voters** because the relevant section of the ROPA was not amended to refer to the ECJ. Section 52 (8) of the ROPA allowed the former Electoral Advisory Committee (EAC) to inspect the “Poll Book” and other election documents without a court order under certain specific conditions. However, that section of the ROPA was not amended to replace the EAC with the ECJ. Consequently, the Commission’s ability to evaluate the strength of its controls by reviewing the “Poll Book” against the list of dead electors referred to in paragraph 4 above is diminished.

ACCESS CONTROLS & ENVIRONMENTAL SECURITY

6. **The ECJ did not have a comprehensive information security policy that defined management’s intentions on information security and provided general direction for protecting the confidentiality, integrity and availability of its information resources especially access to the ERS and the EVIBIS systems.** This created a situation where greater reliance was placed on the experience of certain key IT/IS personnel within the ECJ rather than on established information security policies. This increases the risk of service disruption in the event of the departure or absence of any of these persons especially at or around the time of major elections.
7. **The ECJ did not implement a comprehensive password policy that established standards for the creation of strong passwords, the protection of those passwords and the frequency of change, to protect the information stored on the Commission’s devices.** We observed that 15 employees’ passwords were set to “never expire”, contrary to the ECJ’s policy of requiring users to change their passwords periodically. Six of these users’ passwords were in excess of five years old. Most of the users noted with unexpired passwords were senior officers of the ECJ who would usually be privy to very sensitive information. Since our audit, steps have been taken to improve the controls over password management and at the time of this report, only one account remained set to “never expire”.
8. **The ECJ did not have a system in place to monitor the activities of privileged users and administrators to ensure that they were not abusing or misusing their access rights.** We identified 21 user accounts with administrator privileges on the ECJ’s network. While the core “Administrators” account with a shared password consisted of four users. Furthermore, the passwords associated with these accounts were not changed periodically. This reduced the

level of accountability within the ECJ's IT environment and increased the risk of unauthorized changes to the Commission's information resources such as sensitive elector information.

- 9. The Commission did not have a mechanism in place to log all the activities conducted on its various servers.** We found that, contrary to the Commission's practice, the accounts of two former employees were deleted from the ECJ's network. One of the accounts belonged to a former senior employee of the Commission who, at the time of his employment, would likely have had unrestricted access to the ECJ's information resources. The absence of systems and related audit logs meant that we were unable to determine which officer was responsible for removing these accounts and it prevented us from reviewing the network/system activities related to these deleted accounts. The Commission has since advised us that permission was granted to remove one of the accounts due to concerns raised about the possibility of the former employee accessing the Commission's systems. The Commission, however, did not provide the reason for the removal of the other account.
- 10. The ECJ had several weaknesses concerning its user activation and de-activation procedures.** These procedures were not adequately documented and the relevant records containing authorization for adding or removing network users were either inadequate or not maintained. The lack of effective monitoring and review of user accounts led to a number of discrepancies. For example, the ERS accounts of four former employees remained active after their departure while **the ERS Election Officer User accounts of 13 former temporary employees of the Commission remained active after their departure from the ECJ.** These weaknesses increased the risk of unauthorized access to the Commission's systems and data, including confidential and sensitive elector information. The ECJ has since advised us that the accounts have been de-activated.
- 11. There were 189 user accounts on the ECJ's network that could be accessed by multiple users because of the ECJ's practice of creating multi-user network accounts.** This reduced the system accountability that was necessary for effective access control within the Commission's information technology environment.
- 12. There was a breakdown in the monitoring and control systems relating to the ECJ's physical security and there were inherent weaknesses in the Commission's access control software.** The Commission did not have a documented policy that outlined the procedures to be followed for the issue, return, activation and de-activation of its access cards. There was no system in place to regularly review the access rights assigned to users to ensure that user credentials were consistent with their job functions and that they complied with the instructions from HR. Additionally, we found that the access codes of certain employees were stored in plain text and could have been viewed by anyone with access to the system. The ECJ has since advised us that the access codes are now encrypted.
- 13. The ECJ did not have a maintenance policy to guide the maintenance activities of its computer and related equipment.** Equipment such as PCs, servers, UPSs and back-up generators, AC units, cameras, alarm systems, and fire extinguishers were not serviced regularly in accordance with a planned periodic maintenance schedule. This increased the risk of unplanned business interruptions due to prolonged use and inadequate maintenance.

BUSINESS CONTINUITY & CHANGE MANAGEMENT

- 14. The ECJ did not have a formal system in place to conduct periodic testing of its disaster recovery plans to ensure that the procedures remain relevant and effective in the event of a disaster.** There was also no formal procedure in place to ensure that the back-up tapes for the ERS and other systems were regularly tested to determine the integrity and completeness of the back-up files. Furthermore, the ECJ's *Information Systems Disaster Recovery Plan* did not provide any guidance on dealing with the occurrence and impact of an unauthorized system penetration (hacking). An unauthorized system penetration could corrupt the ECJ's databases or cause sensitive elector information to be exposed, resulting in a compromise of the Commission's entire operations. Inadequate testing of the disaster recovery plans, procedures and backup tapes may lead to complications and delays in the event of an unplanned system disruption.
- 15. The Commission did not have a documented change management policy to control the authorization, testing and implementation of changes to its information technology infrastructure and applications.** Furthermore, there was no evidence that all critical software updates were tested by the ECJ prior to their implementation. This increased the risk of errors or irregularities due to incomplete or inadequate specifications, systems documents, programme testing and reviews. Unauthorized changes may also go undetected resulting in a compromise of the Commission's systems.

IT GOVERNANCE

- 16. The ECJ did not have a structured IT governance framework or mechanism to ensure that its information technology resources delivered value to the organization while at the same time ensuring that IT risks were effectively managed.** The Commission also did not formally adopt any international IT/IS standards to guide its management and use of its information technology resources. The governance of information technology did not receive the necessary attention from the Commissioners and senior management to ensure that issues such as IT strategic alignment, IT performance measurement, risk, resource management, and value delivery were adequately addressed. This increased the ECJ's exposure to IT risks, including compliance risks. Information security may also be compromised without adequate policies, systems, procedures and monitoring mechanisms that are comparable with industry standards.
- 17. The ECJ's Internal Audit Function did not conduct any form of information technology/information systems audits.** The structure and required skills set of the Commission's Internal Audit Unit has not been reviewed to reflect the changes that have taken place within the Commission over-time relating to the use of technology in its operations. Consequently, the most significant aspects of the ECJ's operations were not subjected to regular, independent reviews to ensure that management was aware of critical risks associated with its information technology systems.
- 18. The ECJ did not have an Audit Committee as required by section 8(1) of the Public Bodies Management and Accountability (PBMA) Act neither did it have an updated approved Internal Audit Charter defining the Internal Audit Function's purpose, authority and responsibility.** The Internal Audit Function should be well positioned to provide independent

advice to the ECJ Commissioners and senior managers to help improve the quality and effectiveness of any IT governance initiatives implemented but these gaps have weakened the ECJ's overall corporate governance mechanism.

CORPORATE GOVERNANCE: BREACHES OF THE ECIA

- 19. We found that since the ECJ commenced operations on December 1, 2006 it has not produced a set of audited financial statements in accordance with section 16 of the Electoral Commission (Interim) Act (ECIA).** The absence of these statements prevented the Parliament from reviewing the Commission's financial performance to determine whether the ECJ's resources were applied for the purposes authorized by the ECIA or other relevant laws. The ECJ's approved estimates of expenditure for the year ended March 31, 2012 was \$2.9B (2011: \$761.7M).
- 20. It was not the practice of the ECJ to require all members of staff to sign the oath of secrecy as required by Section 9 of the Electoral Commission (Interim) Act.** We also observed that the ECJ employees were not required to sign the Official Secrets Act Declaration that is applicable to Public Officers.

CORPORATE GOVERNANCE: SALARY DISCREPANCIES

- 21. We found that the ECJ "bench-marked" the salaries of the Director and the Deputy Director of Elections against the posts of Director General and Deputy Director General of the Office of Utilities Regulation (OUR) without any approval from Parliament or the Minister responsible for electoral matters as required by the Electoral Commission (Interim) Act.** The Ministry of Finance's approval was also not obtained as required by section 20 of the Public Bodies Management and Accountability (PBMA) Act. We found no substantial reasons for the bench-marking to the OUR posts especially since the OUR is a self-financing entity and the ECJ receives most of its income from the Consolidated Fund.
- 22. The Commission disregarded a Ministry of Finance directive to pay the Deputy Director of Elections at a certain level resulting in an excess salary payment of \$4.66M for the period September 2010 to March 2012.**
- 23. The ECJ failed to comply with the Ministry of Finance's guidelines on the payment of security allowance for a senior employee.** We observed that the employee who was in receipt of this benefit did not pay the requisite tax as required by the guidelines.
- 24. The ECJ failed to comply with the Ministry of Finance's guidelines on the payment of qualification increments and seniority allowance resulting in an overpayment of \$162,805.39 for the period September 2009 to April 2012.**

RECOMMENDATIONS

1. **The Commission should seek the requisite legal opinion to determine to what extent the ECJ or the Director of Elections can request proof of age from an applicant at the time of registration.** Documentary proof of age such as a birth certificate would not only establish an applicant's correct date of birth but would also provide the correct spelling of an applicant's name as well as his/her place of birth, which is also useful in establishing a person's nationality.
2. **The cases of electors on the Voters' List without a date of birth should be investigated to determine the possible reasons for these anomalies.**
3. **The Commission should strengthen its ERS exception monitoring and review procedures** to ensure that a system is in place to target high-risk electors who are flagged as exceptions for re-verification in order to determine their authenticity.
4. The ECJ should ensure that going forward, its **processing of dead electors include a structured monitoring system that incorporates a timely analysis of the death data from the RGD** in order to effectively minimize the risk of having a large number of dead electors on the Voters' List going undetected.
5. **The Commission should seek the requisite legal advice to determine the way forward as it relates to its powers under the ROPA in particular section 52(8)** where the Act was not amended to refer specifically to the ECJ.
6. **The ECJ should develop a comprehensive information security policy that provides general and specific guidelines to ensure that the Commission's IT resources are adequately protected.** The policy should establish criteria for assigning technical access to specific IT assets including who will have access and what level of access they will be allowed. The implementation, monitoring and enforcement of such a policy are usually the responsibility of a designated Information Security Officer, who usually reports to the head of the organisation or to an Information Systems Committee on all information security related matters. The Commission has since advised us that their policy will be reviewed in keeping with our recommendations.
7. **The Commission should develop and implement a comprehensive password policy to reduce the risk of system compromise.** This policy should include guidelines on password construction, password security and protection standards, password aging as well as the responsibilities of users and system administrators in relation to compliance and monitoring of the policy. Additionally, no user password should be set to "never expire", all users should be forced by the system to change their passwords periodically. The Commission has since started a review of its password policy in keeping with our recommendations.
8. **The ECJ should reduce the number of users with administrative privileges so as to increase its system accountability.** It should also implement a system to ensure that administrator passwords are changed periodically to avoid mis-use. The practice of creating multi-user accounts as well as the sharing of passwords for certain system accounts such as the administrator account should discontinue and each user should be assigned an individual

account with appropriate privileges to ensure a greater degree of system accountability. Furthermore, all current multi-user accounts should be reviewed with a view to being disabled.

9. **The Commission should move urgently to implement appropriate systems and procedures to ensure that the activities of all users, especially privileged users such as system administrators and all network/systems/database activities including firewall activities are monitored and reviewed on a timely basis.** All activities on the Commission's servers should be logged and an independent officer should regularly review the logs. The Commission should also document the procedures to be followed for the activation and de-activation of all user accounts.
10. **The ECJ should conduct an immediate review of all persons who currently have access to its server room with a view to limiting access to only those persons who need access to perform their duties.** It should also review its access card system with a view to ensuring that the access codes of employees are not at risk of disclosure. A policy relating to the activation, de-activation and management of access cards should also be formalized.
11. **The ECJ should develop a comprehensive asset maintenance policy that identifies maintenance requirements, priorities and resources** in order to protect its computer and related equipment and avoid unplanned business interruptions. The policy should also mandate the development of a scheduled maintenance plan for all types of assets especially those that are critical to operations.
12. **We recommend that the Commission develop a more comprehensive information systems disaster recovery plan** that takes into account the risk of unauthorized system penetration, regular testing of recovery procedures and back-up media, regular back-up of critical systems located at fixed centres as well as security procedures relating to the transporting of back-up tapes to off-site locations. The Commission should test and document the test results of its back-up tapes and disaster recovery plans on a regular basis to ensure that all systems can be effectively recovered and shortcomings adequately addressed prior to a disaster occurring.
13. **We recommend that the ECJ develop and implement a formal change management policy** to provide guidance for changes relating to both internally developed and acquired software, hardware, network equipment and related procedures. The policy should ensure that before changes are implemented an analysis is done to determine the precise reason(s) for the proposed change as well as the financial and non-financial cost and expected benefits of the change.
14. Information technology governance and the effective application of an IT governance framework are the responsibilities of the ECJ senior management and Commissioners. **We recommend that the Commission identify and implement an appropriate IT governance framework such as the *Control Objectives for Information and related Technology (COBIT)* or *ISO/IEC 38500:2008 Corporate Governance of Information Technology*** in order to reduce its exposure to IT risks and improve control and governance over its information and related systems.

15. **The Commission should ensure that its Internal Audit Function is adequately supported by staffing the unit with individuals who possess the requisite IT/IS auditing skills, qualifications and experience.** It should also establish an Audit Committee as required by the PBMA Act and ensure that an updated Internal Audit Charter is prepared, reviewed and approved. This Charter should outline the role of internal audit in the ECJ's overall IT governance framework.
16. The Commission should take the necessary steps to comply with section 16 of the Electoral Commission (Interim) Act and **ensure that its financial statements are audited annually in accordance with the Act.**
17. **The Commission should strengthen its existing mechanisms to ensure that all its employees complete the oath of secrecy and the Official Secrets Act Declaration in accordance with the relevant statutes.** The sensitive nature of the information collected by the ECJ requires that all members of staff adhere to the highest levels of confidentiality in order to preserve the integrity of the Commission's operations.
18. **The ECJ should take urgent steps to regularize the salary anomalies relating to the Director and the Deputy Director of Elections by seeking the appropriate approvals.** It should also recover all unapproved or overpaid amounts identified in this report and ensure that future payments are made in accordance with the relevant guidelines.

PART ONE INTRODUCTION

Background

- 1.1** The Electoral Commission of Jamaica (ECJ) commenced operations on December 1, 2006 subsequent to the passing of the Electoral Commission (Interim) Act (ECIA) by Parliament. The ECJ replaced the Electoral Advisory Committee (EAC), which was established in 1979 to advise the Director of Elections on the performance of his functions under the Representation of the People Act (ROPA). Section 4 of the ECIA established the ECJ as a commission of Parliament.
- 1.2** The ECJ's primary objective is to safeguard the democratic foundations of Jamaica by enabling eligible electors to elect, through free and fair elections, their representatives to govern Jamaica.¹ The functions of the Commission under the ECIA include, establishing policies for governing the registration of electors, compiling and maintaining the register of eligible electors and verifying the identity of electors.² The Commission comprises four selected members, four nominated members and the Director of Elections.³
- 1.3** From as far back as 1991, the EAC began to explore the possibility of developing and implementing a credible computerised voting system to remedy the inadequacies of the elector registration system that existed at the time. A report was submitted to Parliament in 1994 outlining the EAC's proposals to improve the voter registration system. However, it was not until 1997 that the Electoral Office of Jamaica (EOJ) embarked upon a sustained effort to utilise technology to effect electoral reform.

The EOJ has since implemented a number of information and communication technology systems in an effort to improve the elector registration and identification process and reduce the risks of errors and irregularities. These systems include a newly designed Elector Registration System (ERS) incorporating the use of fingerprint cross-matching technologies and the introduction of an Electronic Voter Identification and Ballot Issuing System (EVIBIS).

- 1.4** The main objectives of the Elector Registration System are:⁴
- To provide accurate information on all eligible electors from which to compile a Voters' List every six months.
 - To facilitate the enumeration of voters by continuous registration.
- 1.5** The new ERS aims to collect each elector's demographic data, photograph and fingerprints. It facilitates the cross matching of these fingerprints to prevent multiple registrations thus

¹ Section 5 of the Electoral Commission (Interim) Act, 2006

² Section 6 of the Electoral Commission (Interim) Act, 2006

³ The Electoral Commission (Interim) Act, 2006, Section 1 (**First Schedule**)

⁴ <http://eoj.com.jm/content-73-78.htm>

limiting the possibility that a registered elector can appear on the Voters' List more than once.

- 1.6** The EVIBIS facilitates the identification and verification of registered electors at the polling station by way of fingerprints after which the system should issue authenticated ballots for voting. The main objectives of the EVIBIS are to prevent:
- Impersonation of an elector;
 - Multiple voting by persons;
 - The use of unauthenticated ballots.
- 1.7** Under continuous registration, an updated Voters' List is produced and published every six months (May 31 and November 30). The cut off date for registration is two months before the publication of each Voter's List.
- 1.8** Despite placing a greater reliance on information technology, the ECJ did not establish a mechanism to ensure that an independent review of its information technology systems was conducted periodically.

Audit Scope and Methodology

- 1.9** In keeping with the Auditor General's constitutional mandate, an information systems review of the operations of the Electoral Commission of Jamaica (ECJ) was commissioned to determine whether adequate systems, policies and procedures were in place to preserve the integrity and confidentiality of elector information, the achievement of the Commission's business objectives and the safeguarding of its assets.
- 1.10** The audit involved a review of the ECJ's general computer controls, systems and procedures as well as application controls relating to its Elector Registration System (ERS) and Electronic Voter Identification and Ballot Issuing System (EVIBIS). We assessed the effectiveness of the Commission's control environment and its impact on the ECJ's mission, mandate and level of service delivery.
- 1.11** Our audit was planned and performed in accordance with the following Information Technology/Information Systems Standards for audit, governance and security:
- Information Technology Audit and Assurance Standards and Guidelines issued by the Information Systems Audit and Control Association (ISACA)⁵;
 - International Standards of Supreme Audit Institutions (ISSAI) 5310: Information System Security Review Methodology issued by the International Organization of Supreme Audit Institutions (INTOSAI)⁶;
 - Control Objectives for Information and related Technology (COBIT) issued by the IT Governance Institute⁷;
 - ISO/IEC 27000 family of standards dealing with Information Security Management issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)⁸.

These standards and guidelines enabled us to test and compare the ECJ's general computer controls against international benchmarks and widely accepted best practices within the information and communication technology sector.

- 1.12** The audit focused on the review and testing of controls in the following areas:
- Physical and Environmental Security;
 - Access Controls and System/Network Security;
 - Business Continuity and Disaster recovery;
 - Change Management and Control;
 - Management of Human Resources and Corporate Governance.

⁵ <https://www.isaca.org/Pages/default.aspx>

⁶ http://www.issai.org/media%28421,1033%29/ISSAI_5310_E.pdf

⁷ <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>

⁸ <http://www.iso.org>

- 1.13** We also applied various data analysis and interrogation techniques to test the accuracy, completeness and integrity of the data within the ERS.
- 1.14** Our planning process involved gaining a thorough understanding of the mandate, role and functions of the Electoral Commission of Jamaica and the nature and extent of the use of information and communication technology in its operations. This information allowed us to formulate a risk based approach in determining the specific areas to be targeted for review.
- 1.15** Our assessment was based on the review of official ECJ documents and records, statutes and other related articles, analysis of the ERS and related data, observations of processes and procedures, and interviews with senior officers and staff of the ECJ.
- 1.16** Our review concentrated on the adjusted November 30, 2011 Voters' List, which was used for the March 2012 Local Government Election. The ECJ reported that the list was adjusted under section 38 (1) of the First Schedule of the Representation of the People Act to correct errors that were identified in the list that was used for the December 2011 Parliamentary Election. Subsequent checks by us revealed that the errors identified included *duplicate registrations, electors erroneously classified as dead and incorrect constituency registration*. This adjusted list had 1,648,020 electors broken down in the following categories as shown in **Table 1** below.

Table 1: Adjusted November 2011 Voters' List by Category of Elector

ELECTOR CATEGORY	AMOUNT
Civilian	1,613,302
Election Day Workers	24,362
Police	8,277
Soldier	2,079
Total	1,648,020

Source: ECJ

Limitation of Scope

- 1.17** A scope limitation is a restriction on an audit caused by the deliberate or unintentional actions of the client or caused by issues that are beyond the control of both the client and the auditor. Other events that do not allow the auditor to complete all planned audit procedures in a timely manner may also restrict the scope of an audit assignment.
- 1.18** The field work aspect of the audit was significantly affected by a two months long disruption resulting from the refusal of the ECJ's management to co-operate with the auditors pending an opinion from the Attorney General's Chambers as it relates to the powers of the Auditor General to access certain sensitive information held by the ECJ. The subsequent opinion underscored the right of the Auditor General to access the ECJ's databases in keeping with her constitutional mandate.
- 1.19** Additionally, three of four ECJ officials who were present at an Exit Interview to discuss the findings of the audit refused to sign the minutes of the meeting as is customary to confirm

that the contents of the report were discussed with them. The Commission has, however, provided a written response to the findings of the audit prior to the finalization of this report.

- 1.20** The timely completion of the audit was also affected by the December 2011 Parliamentary Elections and the March 2012 Parish Council Elections.
- 1.21** The audit did not include any review or cross-matching of elector fingerprint data, poll book or other election documents that are restricted under the Representation of the People Act. We also did not conduct any network penetration testing or simulation. Additionally, physical inspections were limited to the ECJ's offices located at Duke Street in Kingston, Red Hills Road in St. Andrew and the St. Andrew East Central Constituency Office located at Molyne's Road, Kingston 10.

Inadequate Age Verification Procedures

- 2.1** The Jamaican Constitution and the Registration of Electors (Prescribed Age) Special Act specifies the minimum age a person must attain in order to be registered as an elector. The minimum or prescribed age is 18 years. Additionally, section 111(3)(a) of the ROPA states that *“no person shall be entitled to vote in any polling division if he is under the age of eighteen years”*. Furthermore, section 6 (1) (e) of the Electoral Commission (Interim) Act requires the Commission to *“verify the identity of every eligible elector”*.
- 2.2** The ECJ has a responsibility to ensure that all applicants are at least 18 years old at the time of registration before they are duly registered as an elector. We, however, observed that the Commission did not have an effective system in place to routinely verify the age or date of birth of each applicant. Applicants were not routinely required to provide proof of age e.g. a birth certificate, at the time of registration. A birth certificate was only requested if the Registration Clerk suspected that the applicant may be under the prescribed age or there was some discrepancy with the applicant’s name or date of birth.
- 2.3** The Commission’s response was that *“the ROPA does not give the Director of Elections the authority to demand birth certificates from persons seeking to be registered. Where objections are raised based on age such persons are summoned to sittings by the Returning Officer and at that time are required to provide proof of age. If they fail to provide proof, or fail to turn up, they are not added to the Voters’ List”*.
- 2.4** In cases where birth certificates were requested, the Registration Clerk was not compelled to record the unique birth certificate number on the *Registration Record Card* (RRC) because this field was optional. Furthermore, the Elector Registration System (ERS) that stores all elector information was not configured to accommodate an elector’s birth certificate number.
- 2.5** This increased the risk of registering under-age applicants as legitimate electors and reduced the ECJ’s ability to verify an applicant’s correct age. This also reduces the reliance that can be placed on the identification cards produced by the Commission that are used as de-facto national IDs.
- 2.6** Our review of the adjusted November 30, 2011 Voters’ List revealed that there were 48 electors without a date of birth and 15,472 electors who were 18 years old at the time the list was generated. Where the dates of birth of these individuals were not verified against a certified copy of their birth certificate, no guarantee can be given that they in fact actually attained the prescribed age at the time of registration.
- 2.7** The Commission should seek the requisite legal advice/opinion to determine to what extent the ECJ or the Director of Elections can request proof of age from an applicant at the time of registration. Documentary proof of age such as a birth certificate would not only

establish an applicant's correct date of birth but would also provide the correct spelling of an applicant's name as well as his/her place of birth, which is also useful in establishing a person's nationality.

- 2.8** If it can be established that the ECJ or the Director of Elections has the right to compel applicants to provide proof of age, such as a birth certificate, at the time of registration, then the RRC form should also be re-designed to force Registration Clerks to record the unique birth certificate number of each applicant. At the same time, the ERS should be updated to accommodate each elector's birth certificate number and this should be a mandatory field within the ERS.
- 2.9** The cases of electors on the Voters' List without a date of birth should be immediately investigated to determine the possible reasons for these anomalies.

PART THREE Voters' List Exceptions

Voters' List Contained Numerous Electors with Status Exceptions

- 3.1** The Elector Registration System (ERS) is the system used by the ECJ to record, store and manage all elector demographic data. It displays the status of each elector by using various codes to categorize them. The official Voters' List was generated from the ERS and should contain only those electors who have been duly registered and approved as valid electors. Electors with an elector status of "APRV" (**Table 2**) are those individuals who were automatically approved as valid electors within the ERS. The other categories of elector status shown in **Table 2** were flagged as exceptions.
- 3.2** We compared the adjusted November 30, 2011 Voters' List with the ERS database to determine whether all electors on the Voters' List were approved as valid electors in the ERS. Our review revealed that of the 1,648,020 persons on the Voters' List, 1,498,120 or 91% had an "Approved Elector Status" or "APRV" within the ERS (**Table 2**).
- 3.3** The remaining 149,900 or 9% of electors had status exceptions indicating that they were not automatically approved as valid electors within the ERS (**Table 2**).

Table 2: Voters' List Elector Status

Elector Status	Description	No. of Records
APRV	The elector is approved as a valid elector	1,498,120
DEAD	The elector is dead	4
MISS	Missing information, bad photo or bad prints	133,845
NOFINGERS	No Fingers	2,922
OCR	This elector has the wrong fingerprints	3,137
PND_NC_SIT	Pending Name Change Sitings	24
REMAIN_SIT	This elector remained on the voters list via sitings	9,968
	Total	1,648,020

Source: Compiled by the AGD from data supplied by the ECJ

- 3.4** Our tests indicated that four electors on the Voters' List had a status of "DEAD" within the ERS (**Table 2**). This was brought to the attention of the ECJ who subsequently reported that those four electors were removed from the original November 2011 Voters' List that was used in the December 2011 Parliamentary Election. The electors were removed after being confirmed as dead by the Commission. However, according to the ECJ *"following the elections they were confirmed to be alive and under Section 38 (1) of the ROPA added to the list for the Local Government Elections"*. Therefore, at the time they were added to the list their status within the ERS was changed from "DEAD" to "APRV". Subsequent checks by us confirmed that their status was changed to "APRV".

- 3.5** The ECJ explained that electors who were added or who remained on the Voters' List by virtue of sittings is allowed under the ROPA after a process of adjudication by a Returning Officer and subsequent approval.
- 3.6** The Commission asserted that while the other categories of electors (*MISS, NOFINGERS and OCR*) were flagged as exceptions by the ERS, the applicants would still have been duly registered once their eligibility was established and they satisfied all other criteria. The ECJ stated that *"the system as developed in 1996, created a category for such electors (missed) to facilitate their inclusion on the list once they satisfy all other criteria"*. Furthermore, *"these exception features are a form of identification"*. It should, however, be noted that these exceptions are not displayed on the Voters' List and could only be used to identify an elector at polling stations where the EVIBIS is used.
- 3.7** It is an information system security best practice to have a mechanism in place to review system exceptions especially where the risks associated with these exceptions are assessed to be high. However, the ECJ did not have a system in place to target these electors who were flagged as exceptions for re-verification in order to determine their authenticity. While we recognize that it is unlikely that every elector will be able to provide a fingerprint to the required ERS standard, it is essential that the ECJ have a system in place to satisfy itself that these cases are genuine.
- 3.8** The fingerprint is used as the primary unique biometric identifier within the system and the absence of this attribute increase the risk of the electoral process becoming susceptible to fraudulent activities. An applicant or elector would be able to circumvent the fingerprint identification procedures because their fingerprints would not have been captured by the ERS due to poor quality prints or no fingerprints. The Commission should, therefore strengthen its ERS exception monitoring and review procedures to ensure that a system is in place to target electors who are flagged as exceptions for re-verification in order to determine their authenticity.
- 3.9** The ECJ reported that *"prior to the 2011 General Elections the Commission purchased 70 flat live scan fingerprint scanners to be deployed to all registration centres in an effort to reduce the present failure rate"*. However, at the time of this report the scanners were not yet deployed. The Commission has also conceded that *"while this will not eliminate the category it will further reduce the number and per cent of electors with poor fingerprints in the ERS"*. Consequently, there will still be a need to closely monitor and review electors who are flagged as exceptions.

ECJ's Death Verification Procedures were Inadequate

- 4.1** The Chief Electoral Officer (Director of Elections) is required to take account of dead electors in preparing the official Voters' List and ensure that their names are removed when a new list is prepared. Section 8 (3) of the Representation of the People Act (ROPA) requires that *"the Registrar General shall, at intervals of three months, transmit to the Chief Electoral Officer a list specifying the names, addresses and occupations, of all adults who have died during that three months."*
- 4.2** Both section 8 (1) of the ROPA and section 35A of the First Schedule of the ROPA places an obligation on the Chief Electoral Officer to take into account the information contained in the quarterly list furnished by the Registrar General pursuant to section 8 (3) of the Act.
- 4.3** During the audit, we requested and obtained from the Registrar General, a list of all adults whose deaths were registered between 2008 and 2011. The information presented included a final list for each of the years 2008 to 2010 and a preliminary list for 2011. We compared each death list with the adjusted November 30, 2011 Voters' List and identified at least 4,240 names of dead persons that were on the Voters' List (**Table 3**).
- 4.4** In conducting the analysis we took into consideration the age, address and occupation of each deceased in order to refine the results of the comparison. It is likely that the actual numbers are higher because we excluded a number of names that appeared on both lists in cases where there were material differences in age, address and occupation.

Table 3: No. of Dead Persons on the Adjusted Nov. 30, 2011 Voters' List

YEAR DEATH WAS REGISTERED	AMOUNT
2008	861
2009	1109
2010	1137
2011	1133
Total	4240

Source: Compiled by the AGD from data supplied by the RGD and the ECJ

- 4.5** We recognize that the Voters' List is likely to contain the names of dead electors because it is published only twice per year and electors may die after the list is published and before a new list is available. However, the risk of having a large number of dead electors on the Voters' List could be effectively minimized with a structured monitoring system that includes the death data from the RGD.
- 4.6** We, however, found that prior to the audit, the ECJ's dead electors processing procedures did not take into account the death data from the Registrar General as required by the ROPA. Instead, reliance was placed on death notices published in the press and

information from members of the public. The Commission reported that in the past, the information that was supplied by the RGD was *“only marginally useful because it included all persons who died without providing dates of birth and ages”*.

4.7 The ECJ further asserted that the Director of Elections met with the Registrar General *“to discuss the inadequacies of the list of dead electors supplied to the EOJ and was assured that following the computerization of their system the RGD would be in a position to provide the information in the format required by the ECJ under the Representation of the People Act (ROPA)”*. Consequently, the Commission did not use the list as part of its dead electors verification procedures.

4.8 The Commission contends that the process of identification and removal of dead electors from the Voters’ List is *“problematic”* because there is *“no unique identifier or national registration system”*. However, we observed that since 2012, there has been a dramatic increase in the number of dead electors not carried forward when compared with previous years. Figures from the ECJ revealed that the number of dead electors not carried forward moved from 2,433 in 2008 to 10,459 in 2012 (**Table 4**) an increase of approximately 330%. This increase may be attributed to the use of the death data from the RGD.

Table 4: Dead Electors Not Carried Forward Since 2008

Year	# of Dead Electors
2008	2,433
2009	4,728
2010	2,544
2011	5,923
2012	10,459
Total	26,087

Source: ECJ

4.9 The process of recording the names of electors who voted in an election was not automated. This information was not available in the ERS but was recorded in a *“Poll Book”*, which was kept by the Chief Electoral Officer in accordance with section 52 of the ROPA. Access to the *“Poll Book”* is restricted under section 52 (2) of the ROPA and it may only be inspected under the order of a judge of the Supreme Court or of the Court of Appeal. We were therefore unable to determine the effectiveness of the Commission’s system of controls over the prevention of electoral fraud.

4.10 Section 52 (8) of the ROPA allowed the former Electoral Advisory Committee (EAC) to inspect the *“Poll Book”* and other election documents without a court order under certain specific conditions. However, we were unable to confirm whether the ECJ now has this power under the ROPA because the relevant section was not amended to refer to the ECJ. Nevertheless, the Director of Elections, who is the custodian of the *“Poll Book”*, should take the necessary steps to initiate a review of the *“Poll Book”* against the list of dead electors to determine whether the Commission’s system of control to prevent electoral fraud was functioning effectively. We believe that the conduct of such a review would greatly assist the Commission in determining the strength of its control systems and procedures.

- 4.11** The system of relying on press notices and other reports from the public was inadequate and re-active. This increased the risk of dead electors remaining on the Voters' List. On the other hand, the ROPA has a built in pro-active mechanism that requires a periodic review of the Voters' List with the records from the Registrar General's Department (RGD).

- 5.1** Controls over access to data are provided by a combination of physical, system and application security with the objective of preventing or reducing the risk of theft, damage and unauthorized access as well as to control the movement of information technology and related equipment and devices. Access to IT resources is established, managed and controlled at the physical and logical levels.
- 5.2** Physical access controls such as badges, cards and locks restrict the entry and exit of personnel to an entity's premises or parts of the premises such as its data centre containing information processing equipment such as a database server. Logical access controls such as passwords, restrict access to transactions, data, programs and applications to authorized users.
- 5.3** Most activities of the ECJ are now heavily reliant on the use of information technology. Therefore, it is vital that the Commission implement and monitor appropriate access controls to safeguard its IT resources. Consequently, we reviewed the ECJ's access and security systems, policies and procedures to determine whether they provided adequate safeguards and were consistent with industry standards and best practices.

ECJ Did Not Have a Comprehensive Information Security Policy

- 5.4** Access control procedures and activities are based on organizational policy. This policy should establish levels of data sensitivity e.g. confidential, classified, secret etc. These levels should be used as a basis for access control decisions and user privileges granted based on their job roles and functions. The ECJ did not have a comprehensive information security policy that defined management's intentions on information security and provided general direction for protecting the confidentiality, integrity and availability of its information.
- 5.5** We found that the ECJ had developed an **"Internet, Email and Computer Usage Policy"** that addressed areas such as the use of electronic mail and the internet, logins and passwords, and back-up procedures. However, the document did not address other critical areas such as data classification, workstation and network security, and remote access usage. Furthermore, the policy did not refer to any risk assessment and monitoring procedures nor did it highlight security policies governing access to the ERS and the EVIBIS. The "Internet, Email and Computer Usage Policy" may also be out-dated having not been reviewed and updated since its creation in 2009. Additionally, the policy was not reviewed and approved by the ECJ Commissioners.
- 5.6** The absence of a comprehensive information security policy created a situation where greater reliance was placed on the experience of certain key IT/IS personnel within the ECJ rather than on established information security policies. This increased the risk of service disruption in the event of the departure or absence of any of those persons especially at or around the time of major elections.

- 5.7** While the ECJ attempted to develop elements of an information security policy, the work done so far was not adequate to address its various IT risks. The ECJ therefore needs to develop a comprehensive information security policy that provides general and specific guidelines to ensure that the Commission's IT resources are adequately protected. The policy should establish criteria for assigning technical access to specific IT assets including who will have access and what level of access they will be allowed.
- 5.8** The implementation, monitoring and enforcement of such a policy are usually the responsibility of a designated Information Security Officer, who usually reports to the head of the organisation or to an Information Systems Committee on all information security related matters. Furthermore, a system should also be developed to ensure that all IT policies are regularly reviewed and updated. The ECJ has since advised us that their policy will be reviewed in keeping with our recommendations.

Inadequate Controls over Logon IDs and Passwords

- 5.9** To protect an organization's information technology assets, logical access controls have become more critical in assuring the confidentiality, integrity and availability of IT resources. The aim of these controls is to prevent the unauthorized access and modification to an organization's sensitive data and the use of system critical functions. These controls are usually applied across all levels of an organization's information systems architecture, including networks, operating systems, databases and application systems. The controls typically include some form of identification and authentication, access authorization, logging and reporting of user activities.
- 5.10** The ECJ adopted the use of *Logon IDs and Passwords* as part of its identification and authentication access control procedures at the operating system and application system levels. However, it did not implement a comprehensive password policy that established standards for the creation of strong passwords, the protection of those passwords and the frequency of change, to protect the information stored on the Commission's devices.
- 5.11** The ECJ's "Internet, Email and Computer Usage Policy" did address aspects of password management, however, due to the nature of the ECJ's operations and its heavy reliance on technology a more comprehensive policy was necessary to deal with the possible risks. The importance of a comprehensive password policy cannot be over-emphasized in the ECJ's information technology security because poorly selected passwords may result in the compromise of the Commission's network.
- 5.12** From a sample of 26 network user accounts selected, we found that 15 users' passwords were set to "never expire", contrary to the ECJ's policy of requiring users to change their passwords periodically. Six of these users' passwords were in excess of five years old. Most of the users noted with unexpired passwords were senior officers of the ECJ who would usually be privy to very sensitive information. Older passwords are more likely to be compromised thus increasing the risk of unauthorized access to the ECJ's information resources.

- 5.13** It is critical that the ECJ develop and implement a comprehensive password policy to reduce the risk of system compromise. This policy should include guidelines on password construction, password security and protection standards, password aging as well as the responsibilities of users and system administrators in relation to compliance and monitoring of the policy. Additionally, no user password should be set to “never expire” and all users should be forced by the system to change their passwords periodically.
- 5.14** Subsequent checks revealed that the Commission has started a review of its password policy in keeping with our recommendations. Additionally, only one account remained set to “never expire” at the time of this report and we were advised that steps will be taken to update this account.

Inadequate Controls over Administrator Accounts/Activities

- 5.15** The accounts of administrators and other privileged users should normally be closely monitored because these accounts/users usually have extensive access to an organization’s information technology systems. There should be a limited number of such accounts and for accountability, the administrator password should be known only by one individual. Best practice also requires that the password be changed periodically to avoid mis-use.
- 5.16** We identified 21 accounts that had administrator privileges on the ECJ’s network, with the core “Administrators” account consisting of at least four users. There was no evidence to suggest that the passwords associated with these accounts were changed periodically. This reduced the level of accountability within the ECJ’s IT environment and increased the risk of unauthorized changes to the Commission’s information resources such as sensitive elector information.
- 5.17** Furthermore, the ECJ did not have a system in place to monitor the activities of privileged users and administrators to ensure that they were not abusing or misusing their access rights.
- 5.18** Other activities such as network monitoring, firewall activity review and review of user accounts were not conducted in accordance with a specified schedule but were performed on an ad hoc basis and the results of the reviews were not normally documented. Additionally, the Commission did not have a mechanism in place to log all the activities conducted on its various servers.
- 5.19** The ECJ’s failure to effectively monitor and review all network and firewall activities could result in irregularities going undetected which could compromise its systems.
- 5.20** The Commission should move urgently to implement appropriate systems and procedures to ensure that the activities of all users, especially privileged users such as system administrators and all network/systems/database activities including firewall activities are monitored and reviewed on a timely basis. Additionally, all activities on the Commission’s servers should be logged and an independent officer should regularly review the logs.

Inadequate Documentation of System Procedures

- 5.21** The procedures to be followed for the activation and de-activation of system user accounts were not adequately documented to include, for example, the designated officials responsible for authorizing additions and removals from the ECJ's network. We also found that the relevant records containing authorization for adding or removing network users were either inadequate or not maintained.
- 5.22** The Commission should document the procedures to be followed for the activation and de-activation of all user accounts. These procedures should also include completed authorization forms (hard copy or electronic) from managers and human resource personnel that define the access rights of each user.

Excessive User Privileges

- 5.23** We found that an officer in the Information Systems Department was able to add or remove/disable users from the system as well as perform other administrator functions that were outside his established job scope. This officer also had unrestricted physical access to all departments within the ECJ. This increases the risk of unauthorized activities and irregularities going undetected and consequently undermines the Commission's information systems internal control mechanism.
- 5.24** The Commission reported that the officer in question is usually assigned the duties of another senior employee whenever that employee is absent from work. We, however, observed that even on occasions when the senior officer was at work the other employee maintained privileged access to the ECJ's systems.
- 5.25** Going forward the Commission should ensure that all user access rights are consistent with each employee's established job scope. Temporary assignments should be carefully monitored and access restricted as soon as those assignments are completed.

Former Employees with Logon Activities & Active Accounts

- 5.26** We found that the user accounts of three former employees had logon activities on the ECJ's network subsequent to their date of departure. Two of these persons were employed to the Commission's Information Systems (IS) Department while the other employee's user account was still active at the time of our audit. We were subsequently advised that one employee was still employed to the Commission at the time listed as the date of separation, another employee was given access to complete an outstanding assignment while the third employee's account was accessed by a manager from the IS Department to retrieve work related items.
- 5.27** We also identified four former employees whose user accounts in the Elector Registration System (ERS) were still active at the time of our review. The ECJ's failure to de-activate the user accounts of former employees in a timely manner increases the risk of unauthorized access to its systems and data, including confidential and sensitive elector information. The four accounts have since been de-activated.

Unaccounted for Active ERS User Accounts

- 5.28** Our review of the ERS Election Officer User Information Table revealed that there were 77 active ERS user accounts. We compared the table with the ECJ's most recent staff list and identified 18 user accounts that did not directly relate to any member of staff listed on the staff list. We also compared the table with a list of persons who left the ECJ since 2008 but we were still unable to account for these 18 user accounts.
- 5.29** We brought the matter to the attention of the Commission, who subsequently advised us that 13 of the 18 accounts belonged to persons who were either temporarily employed to the IS Department or employed as Election Day Workers (EDW) between 2005 and 2010. These 13 accounts have since been de-activated.
- 5.30** The remaining five accounts were not assigned to individual employees but more than one person could access them. Three of the five accounts remained active at the time of this report.
- 5.31** Going forward, the Commission should strengthen its systems to ensure that the accounts of former employees are de-activated in a timely manner to reduce the risk of unauthorized access or sabotage.

Multi-User Network Accounts

- 5.32** We reviewed a list of all network user accounts and found that the ECJ's practice of creating accounts that were used by multiple persons reduced the system accountability that was necessary for effective access control. There were 189 user accounts on the ECJ's network that could be accessed by multiple users. This could result in unauthorized access, system abuse and eventual compromise of the Commission's information systems. The likelihood of these breaches occurring is even higher, given the fact that these accounts were not regularly monitored and reviewed.
- 5.33** The Commission should discontinue the practice of creating multi-user accounts as well as the sharing of passwords for certain system accounts such as the administrator account. Furthermore, all current multi-user accounts should be reviewed with a view to being disabled. Each user should be assigned an individual account with appropriate privileges to ensure a greater degree of system accountability.

Deleted User Accounts

- 5.34** The practice of the ECJ is to disable the user accounts of former employees. However, instead of de-activating their user accounts, we found that the accounts of two former employees were removed from the ECJ's network contrary to its practice. The manner of removal was also contrary to standard information system security best practice, which recommends that account related data should be archived prior to the removal of an account if the removal of the account is deemed necessary.

- 5.35** One of the accounts belonged to a former senior employee of the Commission who, at the time of employment, would likely have had unrestricted access to the ECJ's information resources. The absence of systems and related audit logs meant that we were unable to determine which officer was responsible for removing these accounts. This also prevented us from reviewing the network/system activities related to these accounts.
- 5.36** The ECJ reported that the decision to remove the account of the former senior employee was taken against the background of concerns raised about the possibility of the officer accessing the Commission's systems.
- 5.37** The Commission further advised that going forward it will ensure that the accounts of former employees are de-activated in accordance with its established practice.

Inadequate Controls over Access Card System

- 5.38** Physical access to the Commission's corporate offices was regulated by an access control system that required the use of an access card. Additionally, to gain access to certain restricted areas, the card was used along with an access code or a fingerprint. Each member of staff was assigned an access card granting them access to specific areas according to their assigned group. A review of the controls relating to the Commission's physical access control system revealed the following areas of concern:

No Documented Policy

- 5.39** The Commission did not have a documented policy that outlined the procedures to be followed for the issue, return, activation and de-activation of its access cards. The cards were activated and de-activated by a member of the ECJ's Technical Support Unit on the advice of a member of the Human Resources (HR) Department or other user Departments. However, these records were not routinely maintained for review, monitoring and control.
- 5.40** Additionally, the card accounts of former employees were usually deleted from the card system as opposed to being disabled. This removed all user activities associated with those former employees thus preventing management's review of those activities.
- 5.41** We recommended that a policy relating to the activation, de-activation and management of the Commission's access cards be formalized. The ECJ subsequently reported that it will immediately undertake a review of its access control system and produce a documented policy.

Inadequate Review of Access Rights

- 5.42** There was no system in place to regularly review the access rights assigned to users to ensure that user credentials were consistent with their job functions and that they complied with the instructions from HR. This increased the risk that employees may be assigned inappropriate credentials and gain unauthorized access to restricted areas.

- 5.43 We recommend that the Commission implement an appropriate system of review to ensure that users' credentials are consistent with their job functions.

Unencrypted Access Codes

- 5.44 We found that 30 employees were assigned cards that granted them access to the ECJ's server room, which housed the Commission's critical servers. As an added security feature, access to the server room required the use of an access code in addition to the card. However, the codes for these 30 employees were stored in plain text and could be viewed by anyone with access to the system.
- 5.45 We recommended that the ECJ conduct an immediate review of all persons who currently have access to its server room with a view to limiting access to only those persons who need access to perform their duties. The Commission should also review its access card system with a view to encrypting employees' codes to reduce the risk of abuse.
- 5.46 The Commission subsequently reported that access to the server room has now been restricted to 12 persons and their access codes have also been encrypted.

Re-assignment of Access Cards

- 5.47 The ECJ's access card system did not permit the *card issue date* to be updated where an access card was re-assigned to another employee. Where a card was re-assigned, the system did not record the date of the re-assignment, only the date of the original assignment. The card system also did not record the date a card's status changed from "active" to "suspended" or vice-versa. This restricts management's ability to effectively track card usage and activities.
- 5.48 We found that three employees of the Information Systems Department were assigned two access cards each, contrary to the ECJ's policy. We were initially advised that the original cards were lost and not de-activated and the officers re-assigned new cards. Subsequently, however, the Commission reported that the initial cards issued to these employees were either defective or destroyed and new cards were issued without the de-activation of the previous cards. Further checks revealed that the initial cards have now been de-activated. The ECJ should strengthen its controls in this area to prevent the abuse of its access cards.

Employees Not On the Card Credential List

- 5.49 We identified ten individuals from the Information Systems Department who appeared on the "EOJ Staff with Access Card" list but who were not on the "Card Credential" list. The "Card Credential" list records certain critical card account information that may be used to monitor and review the activities of cardholders. These include the cardholder's name, card status, card and access code, issue date, the last door accessed along with the date and time of access.
- 5.50 Consequently, management was not able to adequately monitor and review the activities of those users. This appears to be a system weakness because both lists were generated

from the system at the same time and should therefore contain the same names. This further increases the risk of system manipulation due to management's reduced ability to track cardholders' activities.

- 5.51** The ECJ has promised to review this issue with a view to identifying and correcting the cause of this discrepancy.
- 5.52** The concerns noted above, if not addressed, could lead to a compromise of the Commissions operations especially if unauthorized individuals were to gain access to restricted areas such as the server room. We recommend that the ECJ take the necessary steps to address the weaknesses identified in its access card system and to improve its monitoring and review of cardholder activities and credentials.

Inadequate Maintenance of Computer and Related Equipment

- 5.53** The ECJ did not have a computer and related equipment maintenance policy to guide its maintenance activities. Equipment such as PCs, servers, UPSs and back-up generators, AC units, cameras, alarm systems, and fire extinguishers need to be serviced regularly because they operate under potentially unstable environmental conditions. A regularly scheduled maintenance program helps to reduce the risk of loss, downtime and business interruptions resulting from breakdown or damage to computer and related equipment.
- 5.54** The Commission's computer and related equipment were serviced on an ad hoc basis as opposed to a planned periodic maintenance schedule. This increased the risk of unplanned business interruptions due to prolonged use and inadequate maintenance. For example, during the audit, we observed that a DVR that controlled 16 of the Commission's security cameras was not functional and the responsible officer could not confirm the length of time that the DVR was out of operation. The DVR has, however, since been repaired but during the period it was out of service, certain activities that would normally have been recorded by the respective cameras were not recorded and any breach that may have occurred would not have been captured.
- 5.55** In order to protect its computer and related equipment and avoid unplanned business interruptions, the ECJ should develop a comprehensive asset maintenance policy that identifies maintenance requirements, priorities and resources. The policy should also mandate the development of a scheduled maintenance plan for all types of assets especially those that are critical to operations.
- 5.56** The Commission has accepted our recommendations.

Inadequate Testing of Business Continuity & Disaster Recovery Procedures

- 6.1** The need for providing continuous IT services requires developing, maintaining and testing IT/business continuity plans, utilising offsite backup storage and providing periodic continuity plan training⁹. By their nature, contingency plans are needed infrequently and at a time when the organisation is under stress. There is a risk that they will become outdated or be unavailable when an emergency arises. Therefore, best practice requires that contingency plans be reviewed and tested at regular intervals¹⁰.
- 6.2** The ECJ developed an *Information Systems Disaster Recovery Plan* to guide its management of unplanned disruptions resulting from certain natural disasters or systems failure. The plan documented the Commission's systems configuration as well as outlined the basic procedures relating to power failures, back-up and systems recovery.
- 6.3** The plan, however, did not provide any guidance on dealing with the occurrence and impact of an unauthorized system penetration (hacking). The Commission claims to have adequate safeguards in place to prevent unauthorized system penetration, however, there were no documented procedures in place to guide staff in the event of a successful attack on the Commission's systems.
- 6.4** The Disaster Recovery Plan (DRP) also highlighted the need to establish a fully equipped test environment to evaluate the DRP procedures, however, no such facility existed and there was no formal system in place to conduct periodic testing of the Commission's DRP to ensure that the procedures remain relevant and effective in the event of a disaster.
- 6.5** There was also no formal procedure in place to ensure that the back-up tapes for the ERS and other systems were regularly tested to determine the integrity and completeness of the back-up files. Furthermore, back-ups were not frequently done for the systems located at the Commission's constituency offices island-wide because the Commission claimed that the information on these systems were frequently sent to head office. The DRP also did not establish the procedures to be followed in transporting the back-up tapes to the off-site location for storage.
- 6.6** The Commission contends "*periodic testing of the Disaster Recovery Plan and Procedures is undertaken from time to time even though not explicitly outlined in the plan*". However, we found no documentary proof of such tests during the audit.
- 6.7** If the Commission fails to periodically test its disaster recovery plans and procedures this may lead to complications and delays in the event of an unplanned system disruption especially if back-up tapes are corrupted or other circumstances have changed subsequent to the last review of the plan.

⁹ COBIT 4.1-DS4: Ensure Continuous Service

¹⁰ ISSAI 5310: Information System Security Review Methodology

- 6.8** Additionally, an unauthorized system penetration could corrupt the ECJ's databases or cause sensitive elector information to be exposed, resulting in a compromise of the Commission's entire operations.
- 6.9** We therefore recommend that steps be taken to develop a more comprehensive information systems disaster recovery plan that takes into account the risk of unauthorized system penetration, regular testing of recovery procedures and back-up media, regular back-up of critical systems located at fixed centres as well as security procedures relating to the transporting of back-up tapes to off-site locations.
- 6.10** The Commission should test and document the test results of back-up tapes and disaster recovery plans on a regular basis to ensure that all systems can be effectively recovered and shortcomings adequately addressed prior to a disaster occurring.

Inadequate Change Management Controls

- 6.11** All changes relating to hardware, software and telecommunications infrastructure within an information technology environment should be formally managed and controlled. Changes especially relating to procedures, processes, systems and service parameters should be logged, assessed and authorized prior to implementation and reviewed against planned outcomes following implementation. This helps reduce the risk of instability within the IT environment.
- 6.12** The change management process begins with authorizing changes to occur using a system for prioritizing and approving all change requests. For acquired systems or off the shelf programmes, the vendor may distribute periodic updates, patches or new release levels of the software. The Commission's management should review these changes and determine whether they are appropriate for the ECJ's existing systems.
- 6.13** We found that the ECJ did not have a documented change management policy to control the authorization, testing and implementation of changes to its information technology infrastructure and applications. Furthermore, there was no evidence that all critical software updates were tested by the ECJ prior to their implementation. This increased the risk of errors or irregularities due to incomplete or inadequate specifications, systems documents, programme testing and reviews. Unauthorized changes may also go undetected resulting in a compromise of the Commission's systems.
- 6.14** We therefore recommend that the ECJ develop and implement a formal change management policy to provide guidance for changes relating to both internally developed and acquired software, hardware, network equipment and related procedures. The policy should ensure that before changes are implemented an analysis is done to determine the precise reason(s) for the proposed change as well as the financial and non-financial cost and expected benefits of the change.
- 6.15** The ECJ advised us, *"The recommendation for the development and implementation of a formal change management policy will be reviewed"*.

PART SEVEN IT Governance

- 7.1** Corporate governance is the general system by which organizations are directed and controlled. This includes developing relevant policies and procedures to enable an organization to achieve its objectives and safeguard its assets.
- 7.2** Information Technology (IT) governance is a critical component of corporate governance, it establishes the framework for managing IT within an organization by way of systems, policies and related procedures. IT governance deals with the management of IT resources in such a manner that enables IT to deliver value to the organization while at the same time IT risks are appropriately managed.
- 7.3** The use of technology in essential aspects of the ECJ's operations has created a critical dependency on information technology to initiate, record, process and manage most aspects of the ECJ's operations. Consequently, there is an urgent need to implement an appropriate IT governance framework to ensure that IT investments are safeguarded.
- 7.4** The ECJ's corporate governance structure is guided by the Electoral Commission (Interim) Act, the Public Bodies Management and Accountability Act (PBMA) and relevant guidelines issued by the Ministry of Finance. We reviewed the Commission's policies, procedures and practices to determine whether they were consistent with the various regulatory requirements or with generally accepted principles of good corporate and IT governance.

ECJ Did Not Establish an IT Governance Framework

- 7.5** An IT Governance Framework is a system by which the current and future use of information technology is directed and controlled. It consists of a model that integrates a set of guidelines, policies and methods that represent the organizational approach to the management of information technology. The aim of adopting such a framework is to ensure that the organization's information technology resources sustains and extends its strategies and objectives. Most IT Governance Frameworks comprise activities at three different levels within an organization, these include:
- **Strategic Level** – Board of Directors or equivalent group evaluate, direct and monitor the performance of information technology against plans, internal policies, external obligations, standards and strategic objectives.
 - **Tactical Level** – Management plan, supervise, review and take steps to leverage IT resources and drive continuous improvement by way of a system that includes policies, plans, organizational structures, processes and governance mechanisms.
 - **Operational Level** – Activities are performed, controlled and reviewed to ensure alignment with business objectives.

- 7.6** Our review revealed that there was no structured IT governance framework or mechanism within the ECJ to ensure that its information technology resources delivered value to the organization while at the same time ensuring that IT risks were effectively managed. IT governance is the responsibility of the Commissioners and senior management. However, the governance of information technology did not receive the necessary attention from these strategic decision makers to address issues such as IT strategic alignment, IT performance measurement, risk and resource management and value delivery.
- 7.7** Traditionally, organizations that place a heavy reliance on information technology to achieve their mandate have executive level committees to deal with IT issues that are relevant to the entity. The ECJ, however, did not have any IT committees that provided insight and advice to the Commission on areas such as the alignment of IT with the ECJ's business direction, the achievement of the ECJ's strategic IT objectives and the availability of suitable IT resources, skills and infrastructure to meet the strategic objectives.
- 7.8** Additionally, the ECJ did not formally adopt any international IT/IS standards to guide its management and use of its information technology resources. References were made to standards issued by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), however, those standards were not formally adopted by the ECJ and there was no mechanism in place to monitor compliance.
- 7.9** The absence of an effective IT governance framework increased the ECJ's exposure to IT risks, including compliance risks. Information security may be compromised without adequate policies, systems, procedures and monitoring mechanisms that are comparable with industry standards. Inadequate governance may also lead to a weak control environment as well as low returns on IT investments and expenditure.
- 7.10** Information technology governance and the effective application of an IT governance framework are the responsibilities of the ECJ senior management and Commissioners. An IT governance framework, such as the ***Control Objectives for Information and related Technology (COBIT)*** or ***ISO/IEC 38500:2008 Corporate Governance of Information Technology*** can be a critical element in ensuring proper control and governance over information and related systems within the ECJ. We therefore, urge the Electoral Commission of Jamaica to identify and implement an appropriate IT governance framework in order to reduce its exposure to IT risks and improve its management of all information technology resources.
- 7.11** The Commission reported that it is currently in the *"process of reviewing the necessary requirements in order to be ISO certified"*.

ECJ Has No Internal IT Audit Capacity

- 7.12** Information Technology is now central and pervasive within the Electoral Commission of Jamaica and is no longer seen as a separate function isolated from the rest of the entity. How IT is applied and managed will have a significant effect on whether the ECJ attains its mission, vision or strategic goals. Consequently, it needs to evaluate its IT control environment and general IT governance as part of its overall corporate governance review.

- 7.13** Internal IT audit should play a significant role in the successful implementation of IT governance within the ECJ. The Internal Audit Function should be well positioned to provide independent advice to the ECJ Commissioners and senior managers to help improve the quality and effectiveness of any IT governance initiatives implemented.
- 7.14** The ECJ's Internal Audit Function did not conduct any form of information technology/information systems audits. In fact, we found no evidence that the ECJ's internal auditors have ever undertaken these types of audits. The ECJ has four established internal audit posts: a Chief Internal Auditor, one Auditor and two Audit Clerks. The ECJ confirms that this structure was established over 20 years ago and it does not reflect the changes that have taken place within the Commission over-time especially as it relates to the use of technology in its operations. Their job descriptions did not require them to perform any information systems review and none of the four has received any formal training or exposure to IT/IS auditing.
- 7.15** Consequently, the most significant aspects of the ECJ's operations were not subjected to regular, independent reviews to ensure that management was aware of critical risks associated with its information technology systems. In addition, the ECJ has failed to invest in building the capacity of its Internal Audit Function to enable its internal auditors to continually monitor, analyse and evaluate its information technology and related systems, which are necessary for the efficient and effective operations of the Commission.
- 7.16** Our review also revealed that the ECJ did not have an Audit Committee as required by section 8(1) of the Public Bodies Management and Accountability (PBMA) Act neither did it have an updated approved Internal Audit Charter defining the Internal Audit Function's purpose, authority and responsibility. The existence of these gaps have weakened the ECJ's overall corporate governance mechanism because the Audit Function should help to ensure compliance with corporate and IT governance initiatives that have been implemented within the Commission.
- 7.17** Reviewing and reporting on IT governance involve monitoring at all levels within the Commission. The Commission must ensure that its Internal Audit Function is adequately supported by staffing the unit with individuals who possess the requisite IT/IS auditing skills, qualifications and experience. The Commission should also establish an Audit Committee in accordance with the provisions of the PBMA Act and ensure that an updated Internal Audit Charter is prepared, reviewed and approved. This Charter should outline the role of internal audit in the ECJ's overall IT governance framework.
- 7.18** The Commission has since advised us that steps will be taken to increase its internal IT audit capacity.

ECJ Has Multiple Outstanding Audited Financial Statements

- 8.1** Section 13 of the Electoral Commission (Interim) Act (ECIA) specifies that *“the funds and resources of the Commission shall consist of such sums as may, from time to time, be placed at its disposal by Parliament and all other sums and other property which may, in any manner, become payable to or vested in the Commission in respect of any matter incidental to its functions.”* The revenues of the Commission shall be applied for the purposes authorized by the ECIA or any other law in relation to its functions.
- 8.2** Section 16 of the ECIA requires that *“the Commission shall keep proper accounts and other records in relation to its business and shall prepare annually a statement of accounts in accordance with directions issued or regulations made under section 24A of the Financial Administration and Audit Act.”* Furthermore, *“the accounts of the Commission shall be audited by an auditor or auditors appointed annually by the Commission and approved by the Auditor General.”*
- 8.3** We found that since the ECJ commenced operations on December 1, 2006 it has not produced a set of audited financial statements in accordance with the provisions of the ECIA. There was no evidence to suggest that urgent steps were being taken by the Commission to address these breaches and bring their financial records up to date.
- 8.4** The absence of these statements prevented the Parliament from reviewing the Commission’s financial performance to determine whether the ECJ’s resources were applied for the purposes authorized by the ECIA or other relevant laws. The Commission’s approved estimates of expenditure for the year ended March 31, 2012 was \$2.9B (2011: \$761.7M) as shown in **Table 5**.

Table 5: ECJ Approved Estimates of Expenditure

Expense Classification	F/Y 2012	F/Y 2011
General Administration	367,104,000.00	351,114,000.00
Registration of Voters	368,258,200.00	399,484,000.00
Holding of Elections	2,248,207,000.00	11,200,000.00
	2,983,569,200.00	761,798,000.00

Source: GOJ Estimates of Expenditure

- 8.5** The Commission should take the necessary steps to comply with section 16 of the ECIA and ensure that its financial statements are audited annually in accordance with the Act.
- 8.6** The ECJ has since advised us that steps will be taken to submit their financial statements for the period 2006 to 2010 for audit.

No Oath of Secrecy was Signed by ECJ Staff

- 8.7** Section 9 of the Electoral Commission (Interim) Act states, *“Every person appointed to the staff of the Commission shall, before he performs any function assigned to him under or by virtue of this Act, take and subscribe an oath to be administered by the Commission, in the form set out in the Second schedule.”*
- 8.8** Our review revealed that it was not the practice of the ECJ to require all members of staff to sign the oath of secrecy in accordance with the ECIA. We examined a sample of 30 employees and found initially that none had signed the oath. However, since then we confirmed that 27 of the 30 employees have signed the oath while three remain outstanding at the time of this report.
- 8.9** We also observed that the ECJ staff was not required to sign the Official Secrets Act Declaration that is applicable to Public Officers. This document is the basic standard confidentiality agreement throughout the public sector.
- 8.10** The sensitive nature of the information collected by the ECJ requires that all members of staff adhere to the highest levels of confidentiality. The Commission should therefore strengthen its existing mechanisms to ensure that all employees complete the oath of secrecy and the Official Secrets Act Declaration in accordance with the relevant statutes. This is necessary to preserve the confidentiality and integrity of certain aspects of the Commission’s operations.
- 8.11** The Commission advised us that going forward they will ensure that all members of staff complete the oath of secrecy. However, the ECJ has not addressed the issue of the Official Secrets Act Declaration.

Unapproved Emoluments

- 9.1** Section 7 (2) of the Electoral Commission (Interim) Act states, *“the Director shall receive such emoluments and be subject to such other terms and conditions of service as may from time to time be prescribed by or under any law or by affirmative resolution of the House of Representatives.”* Section 8 (1) of the ECIA empowers the Commission to appoint and employ at such remuneration and subject to such terms and conditions as may be approved by the Minister responsible for electoral matters, such officers, agents and employees as it thinks necessary to assist the Director in the discharge of his duties. However, no salary in excess of the prescribed rate per annum shall be assigned to any post without the prior approval of the Minister.
- 9.2** We found that the ECJ “bench-marked” the salaries of the Director and the Deputy Director of Elections against the posts of the Director General and the Deputy Director General of the Office of Utilities Regulation (OUR) without any approval from Parliament or the Minister responsible for electoral matters. The Ministry of Finance’s approval was also not obtained in accordance with section 20 of the Public Bodies Management and Accountability (PBMA) Act. We found no substantial reasons for the bench-marking to the OUR posts especially since the OUR is a self-financing entity and the ECJ receives most of its income from the Consolidated Fund.
- 9.3** The ECJ reported that the decision to bench-mark the Director’s salary to that of the OUR Director General was arrived at after consultations with a former Cabinet Secretary because the previous post to which the Director was bench-marked no longer existed in the government service. We were not provided with copies of the related correspondences between the former Cabinet Secretary and the ECJ Chairman.
- 9.4** The Commission further reported that *“following the sudden resignation of the former Director of Elections in 2008, the ECJ found that there was nothing in place to facilitate continuity in the management of the EOJ. The ECJ, therefore, took the decision to appoint a Deputy Director of Elections and wrote to the Ministry of Finance advising of the decision. Taking into account the fact that the post of Director of Elections was benchmarked to that of the Director General of Utilities Regulations, the ECJ appointed the Deputy Director of Elections and benchmarked the position to that of the Deputy Director of Utilities Regulations”*.
- 9.5** When the matter was initially submitted to the Ministry of Finance, the Ministry did not approve the creation of the post of Deputy Director. The post was eventually approved and classified within a specific established civil service grade.
- 9.6** However, the Commission disregarded the Ministry’s directive and instead paid the officer at a higher rate that was bench-marked to the salary of the Deputy Director General of the OUR. The Commission reasoned that *“the salary package of the Deputy Director was*

arrived at with perfect logic and after taking all matters into consideration the Deputy Director should continue to be paid in accordance with the salary package of the Deputy Director of the OUR while the Commission should continue to pursue the matter with the Ministry of Finance”.

- 9.7** This resulted in an excess payment of \$4.66M for the period September 2010 to March 2012¹¹.
- 9.8** The Commission should take urgent steps to have these matters regularized, including recovering all excess payments and ensure that future payments are made in accordance with the relevant guidelines. Failure to recover the excess amounts could lead to a possible surcharge action against the responsible officials.

ECJ in Breach of MOFP Security Allowance Guidelines

- 9.9** The Ministry of Finance and Planning (MOFP) by way of *Circular No. 9, ref no. 12548, dated May 31, 1995* established guidelines governing the provision of personal security for certain public officers in relation to the performance of their duties. Officials who qualify for this benefit have the option of either installing a security system at their residence with the Government bearing 80% of the installation cost or receive a taxable monthly security allowance.
- 9.10** We observed that a senior employee of the Commission who was in receipt of this benefit did not pay the requisite tax as required by the Ministry of Finance’s guidelines.
- 9.11** We recommend that the Commission take the necessary steps to ensure that the appropriate tax is deducted from the employee in accordance with the guidelines. Additionally, unless approved otherwise, all financial arrangements for personal security should be consistent with the established guidelines issued by the Ministry of Finance.

ECJ in Breach of MOFP Guidelines on Qualification Increments

- 9.12** The Ministry of Finance and Planning Circular No. 25, Ref. No. 59/40, dated September 15, 2005 outlines the Government’s policy on increments payable for attaining additional qualifications while employed in the service. Paragraph *vi* states, “Where an officer is promoted upon attaining the additional qualification, qualification increment is not to be paid.”
- 9.13** We observed that one officer within the Information Systems Department was promoted shortly after attaining an additional qualification. He was subsequently awarded two qualification increments with effect from the date of his promotion contrary to the MOFP guidelines. He was also erroneously paid a seniority allowance with effect from April 1, 2010. Consequently, the officer was overpaid \$162,805.39 for the period September 2009 to April 2012.

¹¹ Maximum of the recommended salary grade was used in the computation.

- 9.14** The Commission should take the necessary steps to recover the amounts overpaid and ensure that this type of breach does not recur. Failure to recover the overpaid amounts could lead to a possible surcharge action against the responsible officials.