# Report of the
# Task Force on the Computer Theft Incident
# of the Registration and Electoral Office

**June 2017**

# Content

# EXECUTIVE SUMMARY

The Secretary for Constitutional and Mainland Affairs announced on 11 April 2017 that a task force led by a deputy secretary of the Constitutional and Mainland Affairs Bureau and consisted of members from Security Bureau, Office of the Government Chief Information Officer (OGCIO) and Registration and Electoral Office (REO) would be established to review the reasons leading to the computer theft incident of the REO that happened in the fallback venue for the 2017 Chief Executive election (CEE) in AsiaWorld Expo (AWE), and to make recommendations regarding the handling of personal data, information technology (IT) security, the security arrangement for election venues as well as internal supervision and review system of the REO. The Task Force shall submit a report in two months' time.

## THE INCIDENT

2. The Task Force formed an interviewing panel which interviewed 30 staff members of the REO, encompassing the senior management, staff in two relevant election divisions, and the Information Technology Management Unit (ITMU). The Task Force found that based on past practice, two notebook computers loaded with the Polling and Counting Access Control System (PCACS) and the Electors Information Enquiry System (EES) were brought to the AWE for access control and batch replacement purposes in the event the fallback venue needed to be activated. The PCACS contained only the names of the 1194 EC members which were public information that posed no risk of data leakage. The EES contained the information of about 3.78 million

Geographical Constituencies electors which was to be used in conjunction with the PCACS for identifying EC members for badge replacement purpose. The EES also allowed for on-the-spot checking of registration particulars of non-EC members who were to demand entry. The EES was protected with multiple layers of access control measures. The disk drive containing the database was further protected by AES 256-bit encryption, which was more stringent than the guidelines promulgated by OGCIO.

3. Since the EES had been used in previous CEEs and in Dedicated Polling Stations in past Legislative Council and District Council Elections, its use was regarded as a standard practice and there was no deliberation on whether it was essential for the 2017 CEE. Neither the staff of the user teams requesting the system nor the senior management were aware of the exact data stored in the EES.

4. The two missing computers were stored in Room 107 of the AWE which is a fixed room with a front door and a back door, both of which had an electronic lock. There is a pantry connecting to Room 107 and a door in the pantry provides access the corridor outside Room 107, and this door has a physical lock. The AWE provided the REO with keycards for operating the front and back doors during the presence of REO staff and the locks would be switched back to lock mode upon the notification of REO staff on departure. Additional CCTVs were installed in the halls for surveillance, but there was no dedicated CCTV camera for Room 107. There was an understanding between the AWE and REO that the rooms in the venue would be locked, but the REO had no information on who would be the keyholders. (Factually, a water dispenser was delivered into Room 107 during 25 and 26 March 2017 and

the door for Room 107 was opened for Police security check in the early hours of 26 March 2017.) The staff member of the ITMU responsible for the logistics for the IT equipment considered that Room 107 satisfied the relevant requirement that classified information must be stored in "locked" room. The REO had placed its trust on the AWE as venue management to ensure venue security, including preventing unauthorised access to Room 107 in the absence of REO staff.

5. On 24 March 2017, after testing the two missing computers, one staff member of the ITMU put them inside two computer bags and placed them on top of a carton box in Room 107 before leaving the AWE. Two other staff members of ITMU in Room 107 saw that the two computers were still inside the computer bags at around 5:30 p.m.

6. No REO staff went to Room 107 on 25 and 26 March The two computers were found missing on 27 March 2017 when ITMU staff went to collect the IT equipment in AWE.

## RECOMMENDATIONS BY THE TASK FORCE

7. The Task Force has a number of recommendations on the REO's practice in the handling of personal data, IT security and venue security.

### *A. Handling of personal data*

8. To address the inadequacies identified in the compliance with Data Protection Principle 4 under the Personal Data (Privacy) Ordinance, the Task Force recommends that:

- The REO should develop and regularly review detailed guidelines and provide proper training for staff on the handling of personal data for organisation of public elections.
- The departmental Controlling Officer for Personal Data should be consulted on the transfer of personal data among divisions and preparation of computer systems involving loading of personal data.
- The REO should develop a comprehensive privacy management programme to enhance accountability for personal data protection.

***B. IT Security***

9. The Task Force considers that the relevant IT Security Guidelines about storage of classified information to mobile device has not been strictly followed, and there are inadequacies in the IT security policies and practice. The Task Force recommends that:

- The REO should formulate a complete set of departmental IT security policy, procedures and guidelines that at least meet the security requirements of the IT security policy and related guidelines issued by OGCIO.
- ITMU should ensure that the systems of REO comply with the departmental IT security policy, procedures and guidelines.
- The ITMU should advise the teams which requests the computer systems on the appropriate measures to protect the integrity of data stored in computer systems.
- Approval by divisional head (at Chief Executive Officer level) must be sought before requests for bringing personal data out of the REO are made; measures to be put in place to ensure physical security must be set out in the application for approval.

- The ITMU should play a gatekeeping role in assessing whether a request for storage of personal data mobile devices is commensurate with the operational need.
- The EES should not be used in public elections.

### *C. General Security of election venues*

10. The Task Force noted that the configuration of Room 107 and the act of leaving the two computers on top of carton box after testing could not fully satisfy the requirements under Security Regulation on storage of restricted information and there are shortcomings in venue security planning. The Task Force recommends that:

- The REO should establish formal procedures for endorsing overall venue security plans for public elections and seek comments from the Police, clear the plan with the CEO, and submit to Electoral Affairs Commission for information and comments.
- Security measures should be strengthened for restricted information and/or personal data stored in mobile devices in election venues. Storage of any personal data in fallback sites before actual activation should be avoided.
- Inventory count should be conducted at the end of each day, and venue set-up of main and fallback sites should ideally be taken up by the same division.
- Fresh, proper and comprehensive planning on the use of personal data and security arrangements for major election venues should be carried out for every election.

### *D. The Institutional Aspect*

11. The Task Force considers that there are inadequacies in the observance of the relevant Government guidelines and regulations for the handling of personal data, IT security, and general security, but believes that institutional factors could not be overlooked. Based on the institutional issues identified, the Task Force recommends that:

- The post of the Principal Electoral Officer should be made permanent to assist the Chief Electoral Officer to review the preparation and organisation of public elections after an election cycle to preserve institutional memory.
- Certain core members in the election teams and key ITMU staff should be retained in non-election years to consolidate experience from the previous election cycle and to introduce improvements.
- Civil servants occupying permanent posts in the REO should as far as possible be assigned to take up key planning and supervisory duties.
- Proper and adequate familiarisation programmes should be organised during election cycles for time-limited staff.
- Responsibilities between "users" and coordinating teams must be clearly defined.

# CHAPTER I: THE TASK FORCE

The 2017 Chief Executive Election (CEE) took place on 26 March 2017 at the Hong Kong Convention and Exhibition Centre (HKCEC). As a contingency measure, a fallback election venue which would be activated in the event the main venue at HKCEC was compromised, was set up at AsiaWorld-Expo (AWE). On 27 March 2017, the Registration and Electoral Office (REO) found that two notebook computers stored in a locked room in AWE, i.e. the fallback venue, were missing and suspected to be stolen. Amongst the two missing notebook computers, one contained only the names of Election Committee (EC) members and no other personal data. As the names of EC members had already been promulgated through public platforms, the missing of this computer posed no risk of data leakage. The other missing computer contained information of about 3.78 million Geographical Constituencies (GCs) electors in the 2016 Final Register, including their names, addresses, Hong Kong Identity Card (HKID) numbers, and the constituencies that the electors are registered in.

2. The Constitutional and Mainland Affairs Bureau (CMAB) and the REO attached much importance to the matter. The REO reported the loss of the computers to the Police on 27 March 2017 and the case was classified as "theft". CMAB asked the REO to submit an urgent incident report on the case. The bureau also proactively requested that a special meeting of the Legislative Council (LegCo) Panel on Constitutional Affairs (CA Panel) be convened so that the Administration could address the concern of LegCo on the incident in the first instance. To underline the importance the Government attached to the matter, the Secretary for Constitutional and Mainland Affairs (SCMA) announced at the special

CA Panel meeting on 11 April 2017 that a task force led by a deputy secretary of CMAB and consisted of members from Security Bureau (SB), Office of the Government Chief Information Officer (OGCIO) and REO would be established to review the reasons leading to the incident, and make recommendations regarding the handling of personal data, information technology (IT) security, the security arrangement for election venues as well as internal supervision and review system of the REO having regard to the lessons learnt from the incident. The Task Force shall submit a report to SCMA in two months' time.

3. The Task Force on the Computer Theft Incident of the Registration and Electoral Office (the Task Force) held its first meeting on 21 April 2017. The membership list of the Task Force and its terms of reference are at Annex A.

4. The Task Force has convened a total of four meetings and set up an interviewing panel to conduct interviews with 30 REO staff members who were relevant to the incident. This report is prepared based on the information obtained through interviews with staff members and the documentary materials that the Task Force obtained from the REO.

## CHAPTER II: IMMEDIATE FOLLOW-UP ACTION BY THE REGISTRATION AND ELECTORAL OFFICE AND OTHER PARTIES

5. Immediately after confirming that two notebook computers were missing in the AWE, the REO reported the incident to the Police, the Office of the Privacy Commissioner for Personal Data (PCPD), and the Government Information Security Incident Response Office. The Police classified the case as "theft", and the PCPD commenced an investigation pursuant to section 38(b) of the Personal Data (Privacy) Ordinance (Cap. 486). As of 9 June 2017, investigations by the Police and the PCPD were still ongoing.

6. The REO issued press releases on 27, 28 and 30 March 2017 to inform the public about the suspected theft of the computers. Following the PCPD's guidelines and advice, REO also individually informed all GC electors of the incident via email or by post to increase their awareness and minimise potential damage. About 550 000 electors who have provided email addresses to the REO were informed by email, while others were informed through mail. The letter has also been uploaded onto the REO website (www.reo.gov.hk).

7. Internally, the REO submitted an incident report to SCMA on 11 April 2017 to give an account of the incident and provide the department's initial observations. The REO also wrote to relevant government departments and organisations on various sectors which would likely process or receive personal data, including finance, insurance, telecommunications, retail, estate agents, information

technology, etc., to alert them of the incident and appeal for their assistance in adopting appropriate measures to prevent the relevant information from being used for identity theft in criminal activities, so as to protect the interest of the data subjects and that of their own. The Hong Kong Monetary Authority (HKMA) announced, through issuing a press release on 31 March, that it had immediately contacted major retail banks and understood that customers of retail banks were typically required to use pre-registered login names and passwords / PINs to access online banking services systems. The banks also indicated that they followed rigorous loan vetting and approval procedures, and while initial loan applications may be made online or through telephone calls, a successful loan applicant would need to produce identity proof and sign loan documents in person before the loan was granted. Generally speaking, one could not access online banking services by using just a name and a HKID number alone; and high-risk transactions such as third party transfer were not allowed through telephone banking. The HKMA also reminded retail banks to stay vigilant and continue to monitor relevant developments.

8. The REO also took the initiative to follow up with other relevant organisations on any suspected identity theft incidents. A list of the organisations that the REO has contacted is at Annex B. As of 9 June 2017, no irregularities have been reported.

9. On the voter registration front, REO staff has been paying special attention to any unusual or suspicious voter registration and change of particulars applications. For incomplete or suspicious cases, REO staff would clarify with the applicants and ask for written supplementary information, if necessary. If an applicant fails to provide supplementary

information, the REO would typically not process the application further. No irregularities have so far been detected.

10. In addition, CMAB sought the support of the LegCo CA Panel on 19 April 2017 on a proposal to require address proof for change of registered address applications under the Voter Registration system. The Electoral Affairs Commission (EAC) will amend the relevant subsidiary legislations. After the introduction of address proof requirement in relation to change of registered particulars, the possibility of a third party successfully impersonates a voter to submit application for change of registration particulars would be significantly reduced.

11. Regarding the possibility of lawbreakers making use of stolen personal data to produce forged HKID cards, the existing smart identity card has a number of anti-forgery features, such as optical variable ink, multiple laser image, kineprint with colour-changing images when viewed at different angles, and high-quality laser engraved photograph on the polycarbonate card body, all of which make it very difficult to successfully alter or produce counterfeits of the HKID card. Members of the public who have doubts about the authenticity of identity cards may refer to the Immigration Department's website for further information.

# CHAPTER III: BACKGROUND OF THE INCIDENT

12. The Task Force is tasked to identify the reasons that caused the computer theft incident, so that feasible remedial measures could be recommended to prevent similar incidents from happening in the future. To find out the background and facts of the incident, the Task Force formed an interviewing panel which consisted of the Task Force Leader, representatives of CMAB, OGCIO and SB. A total of 30 staff members of the REO including the senior management, officers from the two relevant election divisions, as well as relevant officers from the Information Technology Management Unit (ITMU), were interviewed.

***Preparation for public elections***

13. The REO has on its permanent establishment the Operations Division, Committee and Research Division, Media Relation Unit and the ITMU to handle regular duties including voter registration, secretariat support for the Electoral Affairs Commission, the planning and implementation of information systems used in the REO, as well as ad hoc duties such as organisation of by-elections. The REO typically creates a substantial, yet time-limited Election Division (E Division) during an election cycle to handle the preparation and organisation of territory-wide elections, including District Council Election (DCE), Legislative Council Election (LCE), Election Committee Subsector Elections (ECSSE) and CEE. The current E Division is responsible for the election cycle starting with the 2015 DCE, followed by the 2016 LCE, 2016 ECSSE and the 2017 CEE. A Principal Electoral Officer (PEO) post is also created during the election cycle on a time-limited basis to take charge of the preparation and organisation of these public elections.

An organisation chart of REO is at Annex C.

14. During election cycles, the Chief Electoral Officer (CEO) and PEO typically meet with colleagues at two regular meetings chaired by the CEO. Firstly, there is a weekly meeting which involved all the division and unit heads. The respective teams will report progress of their tasks at hand at this meeting. Secondly, there is an Election Division meeting (E Division meeting) which is held on a bi-weekly basis. All Deputy Chief Electoral Officers (DCEOs), Senior Executive Officers (SEOs) and Executive Officers (EOs) of the four election divisions as well as the Head of ITMU (H, ITMU) will attend. More detailed discussion about the preparation work for elections will normally take place at E Division meetings, with checklists prepared to keep track of the progress of different aspects of the preparation of the elections.

***The planning of the venue set up for AWE***

15. The entire E Division was fully engaged in the preparation and organisation of the 2016 LCE until early September 2016. As such, the bulk of the preparatory work for the 2017 CEE only started around September 2016. Venue set-up of the Central Counting Station and Media Centre for the main site of the 2017 CEE at HKCEE and the fallback site at AWE was originally planned to be taken up by a team under E4 division in REO, namely E4(Central Counting) (commonly known in the department as E4CC).

16. At the initial planning stage, E4CC made reference to past practices (such as 2016 LCE), and assigned Room 107of the AWE as an office for ITMU in the preliminary layout plan, noting that it was a fixed

room instead of a room temporarily erected with partitions. E4CC drew up a preliminary list of equipment needed for the AWE. Notebook computers to be installed with EES and PCACS for use at the counter for issuing replacement badges for EC members were included on this list.

17. Subsequent to the completion of the ECSS election on 11 December 2016, it was noted that the E3 division (specifically the E3(Central Counting) (E3CC team)) had some spare capacity while E4CC was overloaded with the preparatory for the 2017 CEE for both the main site at HKCEC and fallback site at the AWE. It was therefore agreed that the venue set-up work for AWE should be transferred from E4CC to E3CC. The DCEOs of E3 and E4 divisions and PEO who oversaw both divisions agreed to this arrangement. In early January 2017, E4CC and E3CC had a handover meeting, and the reference note included a preliminary lay-out plan and list of equipment for AWE passed from E4CC to E3CC.

18. The scale of the set up in AWE was discussed among PEO, DCEO(3) and DCEO(4) during the preparation stage. Having regard to the fact that the fallback site in 2012 CEE involved only minimal set-up which might affect the operability of the fallback site if activated, it was decided that while the scale of the fallback site for 2017 CEE should be kept to the minimum in order to minimize waste, the fallback site should still have an adequate set-up so that it would be operable within a reasonable amount of time after a decision was made to switch sites. The planning of the AWE proceeded on this understanding and the configuration of the venue at the AWE largely mirrored the main site at HKCEC.

***The data systems in the two missing computers***

19. For the purpose of verifying the identity of EC members for admission to the venue and for checking of their voting eligibility, two notebook computers were installed with two data systems, i.e., the Polling and Counting Access Control System (PCACS) and the Electors Information Enquiry System (EES) respectively.

*PCACS*

20. To facilitate crowd management on the polling day, different access control points were set up at the main venue of the 2017 CEE, i.e., the HKCEC. EC members, who were authorised to enter the main polling station and the "EC Members area" of the media centre, were identified by badges issued to them before the polling day. PCACS was designed to identify and record EC members' entrance, and to facilitate badge replacement or re-issuing of badges to EC members on the spot.

21. The system operated through handheld devices which performed as badge scanners and information display. The handheld devices were connected to the database stored in the server (i.e. the missing computer which contained the names of all EC members) through end-to-end encrypted Wi-Fi network. Upon scanning an EC member's badge, the system would verify the validity of the badges. The data file was protected by an 8-character password, and the plan was to erase the data on the spot at the end of the election.

*EES*

22. The EES was first developed in the late 1990s as a system installed in District Offices to facilitate public checking of electoral particulars. After entering his/her identity card number, an elector would be able to see his name and his designated polling station. This function has been taken over by the Online Voter Information Enquiry System (OVIES) launched in September 2014, but the EES continued to be used in different recent elections, especially in Dedicated Polling Stations in police stations set up for DCE and LCE. As detainee electors at police stations on the polling day may come from any constituency, the EES, which contained information of all registered electors, was deployed for identifying electors and retrieving their electoral particulars at DPSs in police stations.

23. The EES was protected with multiple layers of access control measures. To access the system and retrieve information from the database, a user has to first login to the Windows operating system, then login to the encryption software which protected the database and the EES programme, and finally login to the EES programme itself. All three layers were password protected. The disk drive containing the database and the EES programme was further protected by AES 256-bit encryption, which was more stringent than the guidelines promulgated by the OGCIO. In addition, the HKID numbers were encrypted using AES 256-bit encryption and the whole database (including the encrypted HKID numbers) was further encrypted using AES 128-bit encryption. The decryption would need to be done through the EES programme. Therefore, particulars of a specific elector could only be retrieved upon entering an elector's HKID number using the EES programme. Reverse

enquiry (e.g., retrieving a person's HKID number through inputting his/her name) was not allowed. The key to decrypt the database was unrelated to the three passwords mentioned above. In other words, even if a person holds the three passwords, he/she would still not be able to decrypt the entire database using the passwords.

24. In the 2017 CEE, the EES was set up at the election venue to be used in conjunction with the PCACS for identifying EC members for badge replacement purpose, since the PCACS contained only the names of EC members and no particulars such as HKID numbers. In addition, the EES also allowed on-the-spot checking of registration particulars of any non-EC members who were to demand entry at the entrance of the election venue. The EES system was installed in notebook computers set up at different admission points of the election venue and the main polling station. One of these computers is found missing on 27 March 2017.

***Preparation of IT equipment***

25. When the ITMU called for requests for IT equipment for use at the 2017 CEE in early January 2017, E3CC requested two notebook computers be loaded with PCACS and EES respectively for the AWE. E4CC also requested computers loaded with PCACS and EES for the main site at HKCEC. Officers in both teams told the Task Force that they had no knowledge of the exact type or volume of data stored in the EES.

26. The requests were made by the two teams to ITMU separately without cross-referencing each other. In the REO, requests for IT equipment to ITMU are made by frontline officers at EO level and copied

to the relevant section head at the rank of SEO or equivalent. Upon receiving the requests from the "users", ITMU staff would make available the required IT equipment (including data systems) accordingly without the need to seek senior level approval.

***Personal data used in EES***

27. The Task Force noted that technical staff in the ITMU responsible for the development of the EES and H, ITMU were aware of the type and amount of data stored in the EES. However, since the EES was used in previous CE elections and in Dedicated Polling Stations in past LCEs and DCEs, its use was regarded as a standard practice and there was no deliberation on whether it was essential for the 2017 CEE, either at the working level, the E Division meetings or the weekly meetings. The Operations Division which was responsible for the administration of voter registration was not consulted on the transferring of data to the EES or of their loading onto notebook computers either. There were several demonstrations of the access control and batch replacement system before the CEE, but the use of EES was not a focal point catching the attention of the senior level of the REO. The CEO told the Task Force that he was not informed of the deployment of the EES or the type and volume of data stored therein. The PEO was aware of the deployment of EES in previous elections and knew that it contained data of all GC electors. Nevertheless, she told the Task Force that she had no idea of the exact volume of data stored in the EES for the 2017 CEE. As regards the PCACS, it was on the checklist for the weekly meeting as it was a newly developed system based on the admission control system used in the previous CEE, and the progress of its development was reported at the meetings.

28. E4CC was the main user for the PCACS and EES for the 2017 CEE. However, staff of E4CC told the Task Force that they were not aware that the EES would contain data beyond that of the 1194 EC members until mid-March 2017. Upon enquiry by staff member of E4CC, ITMU staff advised that isolating the data of EC members under the current configuration of the EES was not practicable, and the observation was not followed up further.

***Security arrangement regarding Room 107***

29. As regards venue security, E3CC was responsible for coordinating the requests from user teams on the security requirements in the AWE and liaised with AWE management accordingly. Specifically with regard to Room 107 which was assigned to the ITMU for setting up server computers and storage of IT equipment, E3CC expected the ITMU to set out the security and other requirements for the room. However, the staff member of the ITMU responsible for logistics arrangement for the IT equipment considered that Room 107 satisfied the relevant requirement (i.e., classified information must be stored in "locked" room) and it did not occur to the officer's mind that there was a need for additional security measures.

30. Room 107 is a fixed room with a front door and a back door, both of which had an electronic lock. There is a pantry connecting to Room 107 and there is no lock for the door between the pantry and Room 107. The pantry opens into a plant room which has no other door. There is another door in the pantry which could access the corridor outside Room 107, and its door has a physical lock operated by key from

the outside and by a thumbturn from the inside. (A layout plan of Room 107 is at Annex D)

31. The AWE provided the REO with two keycards for operating the front door and back door of Room 107. Upon notification by REO staff on arrival, the locks on the front and back doors would be switched to card mode and they could be unlocked by the keycard. The locks would be switched back to lock mode when the REO staff notify the control room to deactivate the keycard before departure. REO staff told the Task Force that there was an understanding between the AWE and REO that the rooms, including Room 107 would be locked, but the REO had no information on who held the keys to the locks in relation to the rooms.

32. In the licence agreement for the venue between the REO and AWE, there was a clause which provided that the AWE had access to the venue licensed to REO. E3CC raised concern over this provision as the room for storing ballot paper (Room 105) must not be accessible to any unauthorized person. In the end, E3CC and the AWE management agreed that no AWE personnel should enter Room 105, but no such agreement was made in respect of other parts of the venue, including Room 107.

33. A working group consisting of the representatives of AWE, Police, and relevant teams of the REO on venue set-up for the AWE discussed in detail at one of its meeting the security of Room 105 (which is identical in terms of layout with Room 107) which would be used to store ballot papers and agreed on a series of additional security measures for that room. The security arrangement of Room 107 was however not discussed. Immediately before this meeting, members of the working

group conducted a site visit at AWE. PEO visited Room 105 but not Room 107. DCEO(3) visited both Room 105 and Room 107 but raised no security concern about Room 107.

34. The security plan for the fallback site in the AWE was made having regard to the arrangement in the main site in HKCEC and discussion with the AWE management. E4CC shared with E3CC the latest development in the arrangement, including the latest layout plans, for the main site at HKCEC so that E3CC could set up the fallback site correspondingly. However, the Task Force noted that not all details were relayed despite such a liaison channel. For example, bar-locked cabinets were ordered for the store room in HKCEC to store the computers loaded with EES and PCACS among other things, but this was not communicated to E3CC.

35. Regarding extra security measures in the AWE, additional CCTVs were installed in the halls for surveillance, but there was no dedicated CCTV for Room 107 and the closest CCTV camera was outside the entrance of Hall 7, which was a few meters away from the corridor leading to the front door of Room 107. Security guards were deployed to station at the foyer area outside different halls (which were meters away from the corridor leading to the front and back door of Room 107) during the licensed hours of the venue as specified in the licence agreement[1] and throughout the day on 26 March 2017. The security plan was sent to Support Wing of the Police Headquarter and Police Tactical Unit of the New Territories South District of Police for comments before it was finalised.

[1] 8:00 am to 11:59 pm on 22 – 25 March 2017, 7:00 am – 5:59 pm on 26 March 2017, 7:00 am - 5:59 pm on 27 March 2017 and 8:00 am – 11:59 pm on 28 March.

***Storage of IT equipment in Room 107***

36. After preparing the IT equipment pursuant to user requests, the ITMU would normally deliver the IT equipment to the venue and conduct functionality tests with the user teams. After testing on site, the IT equipment would be handed over to the user teams, which would then be responsible for the safekeeping of the equipment. However, such procedures were not followed on this occasion, and there was no clear understanding between the ITMU, E3CC (fallback venue coordinator) and E4CC (coordinator of access control and batch replacement systems) on the ownership of the two notebook computers in the fallback site.

***Moving-in of IT equipment into AWE***

37. On 22 March 2017, the ITMU oversaw the moving of all necessary IT equipment (a total of 50 desktop computers and 26 notebook computers, alongside other equipment and accessories for use in different parts of the venue) to the AWE. Most of the equipment was for general purpose like sending email or web-browsing and not loaded with data. The two missing notebook computers were among the computers delivered to the AWE on that day.

38. An officer of the ITMU was in charge of the moving-in of the IT equipment. In the afternoon of 22 March, ITMU staff delivered the IT equipment to the various designated locations within the fallback site. The two missing notebook computers were put in computer bags and placed inside a carton box in Room 107. ITMU staff left the AWE for the day at around 6:00 pm and asked the AWE security to switch the lock for the doors of Room 107 to lock mode.

39. In the afternoon of 23 March 2017, the two notebook computers were brought to the entrance of Hall 5 (where they would be used on polling day in case the fallback site was to be activated). However, as network connection for the area was not yet ready, testing could not be conducted and the notebook computers were taken back to Room 107. When ITMU staff left Room for the day, they informed the AWE control room to change the locks to lock mode.

40. On 24 March 2017, one staff member of the ITMU took the two notebook computers to the entrance of Hall 5 to test the functionality of the LAN network. He did not possess the password for the two systems and the operation of the PCACS and EES were not tested. After the testing, at around 11:30 a.m., he put the two notebook computers inside two computer bags and placed them on top of a carton box in Room 107 before leaving the AWE for HKCEC. Two other staff members of ITMU stayed in Room 107. At around 5:30 p.m., in response to a telephone request from the staff member who tested the computers to locate a handheld device, the two remaining ITMU staff members searched Room 107 and saw the two notebook computers in the computer bags on top of the carton box during the search. The two remaining staff member made sure both the front and back doors of Room 107 were changed to lock mode and could not be opened by keycard before they left at around 6:00 p.m.

41. No REO staff went to Room 107 on 25 and 26 March 2017, and the security of the entire fallback site, including Room 107 was entrusted to the AWE as venue owner and management. The Task Force was told during the interviews that the AWE delivered a water dispenser into

Room 107 during those two days as REO staff found a water dispenser in the room on 27 March. The REO was not notified when the delivery was arranged. The door for Room 107 was also known to be opened for the police security check conducted in the early hours of 26 March 2017.

42. On 27 March 2017, ITMU staff went to the AWE to collect the IT equipment. The ITMU staff member who did the testing on 24 March discovered that the two computer bags for the notebook computers were left empty on the chairs in Room 107. REO staff then searched for the two computers first in Room 107 and then the entire venue but to no avail. Later in the day the REO concluded that the two notebook computers had gone missing and reported to the police the suspected theft of the two computers at 4:30 p.m.

# CHAPTER IV: OBSERVATIONS AND RECOMMENDATIONS BY THE TASK FORCE

43. Taking into account the information obtained during the staff interviews and a review of relevant REO internal documents, the Task Force wishes to set out a number of observations on the current practice of the REO in the handling of personal data, IT security and venue security. In the light of these observations, the Task Force recommends a series of measure to address the inadequacies identified. A summary of the recommendations of the Task Force is at Annex E.

## *A. Handling of personal data*

44. All government bureaux/ departments need to comply with the Personal Data (Privacy) Ordinance (PDPO). The PDPO requires data users to comply with six Data Protection Principles (DPPs). DPP4 on data security states that a data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use. The Task Force was aware that the PCPD had commenced an investigation on the REO's compliance with the PDPO in relation to the computer theft incident. In the course of its work, the Task Force also observed a few issues in relation to the compliance of DPP4 in the REO:

(a) the REO has drawn up a circular memorandum on compliance with the PDPO, which sets out the general principles on the handling of personal data. On top of this, the REO has issued a circular on "Guidelines on Handling Personal Data of Electors and Measures of Data Protection in the Operations Division" which is only

circulated among staff in the Operations Division. There is however no detailed guidelines or training on the handling of personal data during public elections and the knowledge of E Division staff on compliance with the PDPO could be in question.

(b) The DCEO of the Operations Division is the Controlling Officer for personal data in the REO, but he was not consulted on requests for deploying the EES on notebook computers for public elections. There is in fact no established mechanism for seeking the advice or approval from the Controlling Officer for the internal transfer of personal data among divisions or the preparation of databases involving personal data. Data transmission for use at public elections has been driven solely by the request of a user team without the need for clear justification and formal approval by a competent authority within the department. Close monitoring on the compliance with the relevant DPP was therefore not possible.

45. To address the above issues related to handling of personal data, ***the Task Force recommends that:***

(a) the REO should develop, and regularly review, detailed guidelines that are directly relevant to the work of its staff especially with regard to the organisation of public elections on the proper handling of personal data. Apart from general promulgation and periodic circulation of these guidelines to all staff, in view of the high turnover of REO staff in between election cycles, proper training should be provided to all staff for every election cycle at the minimum.

(b) The departmental Controlling Officer for personal data should play a more pro-active and functional role in the handling of personal data requests in the REO, and should be consulted on the transfer of personal data among divisions and preparation of computer systems involving the loading and keeping of personal data.

(c) on top of (a) above, in the longer run the REO should develop a comprehensive privacy management programme (PMP), which involves a detailed plan for specific actions to be taken by designated officers involved in different aspects of personal data handling in the REO. The PMP should be drawn up in the light of an in-depth examination of all operations involving personal data (including scenarios which may require the ad hoc use of personal data) and the associated privacy risks. By clearly delineating the roles of teams and individual officers in implementing data protection measures, the timetables for specific steps to be completed and documented, and a mechanism for the relevant procedures to be reviewed, the PMP will serve to enhance accountability for personal data protection.

### *B. IT Security*

46. Paragraph 10.3 of the IT Security Guidelines issued by OGCIO states that storage of classified information to mobile devices should be avoided. Staff should justify the need to store classified information in these devices and proper authorisation should be sought before storing minimum required classified data to the mobile device. In the opinion of the Task Force, this Guideline was not strictly adhered to in this case.

47. The Task Force also noted that one circular, REO Administrative Circular (REOAC) No. 4/2008, provides policies and guidelines on the proper use of computer and other IT facilities and services in the REO, and sets out the control procedures, good practices and precautionary measures in using computers and IT facilities and services for all staff's information and compliance. However, the topics covered by REOAC No. 4/2008 are only a subset of the Baseline IT Security Policy (S17) and IT Security Guidelines (G3) issued by the OGCIO, which also cover, among others, departmental IT security organisation and responsibilities of different roles, core security principles, physical and environment security, outsourcing security and business continuity management. The level of details set out in REOAC No. 4/2008 is also lower than that set out in S17 and G3. The Task Force observed that REOAC No. 4/2008 does not comply with S17 and G3, which outlines the mandatory minimum security requirements for bureaux/departments to formulate their own departmental IT policies, procedures and guidelines (see Sections 2.3.2 and 2.3.3 of S17). The Task Force further observed that REOAC No. 4/2008 was published in 2008. Since then, there have been three major revisions of S17 and G3. In the information security audit for REO conducted by OGCIO in 2015, OGCIO recommended that the departmental IT security policies, standards, procedures and guidelines shall be reviewed regularly and updated to comply with the latest security requirements in S17 and related guidelines, and that the records of review or approval of department IT security policies, standards, guidelines and procedures should be maintained. The REO has not revised its relevant policies and guidelines since 2008 to keep them up-to-date.

48. Regarding the three layers of password protection for the EES, the Task Force observed that the stated password policy for the EES did

not entirely comply with the IT Security Guidelines (Section 11.4). However, the Task Force noted that the password policy for EES at two of the layers effectively required even stronger passwords to be used. Furthermore, recognising the multiple layers of access controls and the putting in place of a mechanism of delayed login process after each unsuccessful login attempt, the Task Force considered that the overall protection of the data therein would still be sufficiently strong to guard against unauthorised access.

49. The Task Force noted that REO staff primarily followed past practices for the use of personal data and the arrangement for venue security in previous elections, without critical assessment of the changing circumstances and possible loopholes. For example, given that the EES was used in past CE elections and other elections, it was used in the 2017 CEE without regard to actual need, nor the risk that might arise from bringing such a large volume of personal data out of REO office premises. The ITMU had also not acted as a watchdog to point out the potential security risks.

50. In this connection, the Task Force observed that the PCACS was developed to facilitate the administration of admission control and the EES was primarily used to assist in the verifying of the identity of EC members for badge replacement. As admission control was an important area in the CE Election, the PCACS and the EES should both be key data systems to be used in the election. However, the senior management of the REO did not have thorough knowledge about the operation of the systems and how they could achieve the intended purpose. The decision of requesting these two systems be made available at the fallback site was made by staff at Executive Officer I

level without much supervision of senior level staff. The fact that the EES was loaded with data of all GC electors was also not known beforehand by the senior management. As a result, there was no senior level review of the appropriateness of the decision specifically and of the compliance of the IT Security regulations generally.

51. To address the above issues identified and to further enhance the IT security, ***the Task Force recommends that:***

(a) As a general improvement and compliance measure, the REO should formulate as soon as possible a complete set of departmental IT security policy, procedures and guidelines that at least meet the security requirements of the Baseline IT Security Policy (S17) and related guidelines as advised in Section 2.3.3 of the Baseline IT Security Policy. The departmental IT security policy, procedures and guidelines should also be reviewed regularly and kept up-to-date with the latest requirements of S17 and related guidelines.

(b) ITMU should ensure that the systems of REO comply with the departmental IT security policy, procedures and guidelines.

(c) ITMU, as the advisor on IT security in the REO, should advise the team which requests computer systems on the appropriate measures to protect the integrity of the data stored in the computer systems, especially those that are brought out of office, taking into account the nature of the data and the physical and IT environment for the operation concerned. For example, the system should be designed in such a way that allows truncation of data according to actual

need. In the case of data stored on networked computers, there should be remote wipe / automatic wipe of data after a number of unsuccessful log-in attempts. For locations where secured network connection is possible, remote access to the database stored on the central computer may be a better option than off-line storage given the better log-in trail and avoidance of risk of data loss owing to theft of equipment.

(d) Operationally, proper approval at an appropriately senior level must be sought for the storage of personal data in mobile device and brought out of REO office premises. As a general rule, approval by divisional head (at Chief Executive Officer level) must be sought before requests for personal data to be brought outside of the REO could be sent to ITMU and, in complex cases the approval of the PEO should be sought. The need for storing such data on mobile devices, whether alternative measures have been explored, and also the measures in place to ensure physical security, must be set out in the application for approval.

(e) Apart from ensuring the security of data stored in computer systems, the ITMU should also play a gatekeeping role in assessing whether a request for storing personal data in mobile devices is commensurate with the operational need having regard to computer systems prepared in other similar cases, and advise the team which requests computer systems on the appropriate precaution and security measures in relation to the usage and storage of such systems. Every such case should be cleared with the H, ITMU personally.

(f) The EES was used in past elections in the Dedicated Polling Stations in police stations to verify the identity of the detainee voters. It was also used in the 2012 CEE to verify the identity of the entrants. Upon closer examination, it is apparent that such a large database is non-essential in the election venues. In fact, in the general elections of District Council and LegCo, more than 500 general polling stations would be set up across the territory and polling staff in all such stations would rely on a hotline administered by REO headquarters to verify the identity or eligibility of the electors in cases of doubt. The Task Force believes that the same practice could be followed for other public elections.

***C. General Security of election venues***

52. Regulation 197 of the Security Regulation states that restricted documents must be kept either (i) in a locked steel filing cabinet; or (ii) in an office which is locked up after office hours and to which members of the public do not have access. Separately, Regulation 366 of the Security Regulation states that restricted information stored on removable devices must be kept in compliance with Regulation 197, i.e. that when not attended to or not in use such information on mobile devices must be kept in a locked room or cabinet. The Task Force noted that Room 107 has electronic locks for front door and back door which could be controlled by AWE security control room under lock mode, and that the door leading to Room 107 from the pantry to the corridor could also be accessed by AWE personnel who kept the keys. Without additional security measures Room 107 could not fully satisfy the requirement for storing restricted document under Regulation 197. Moreover, the two

notebook computers were left on top of a carton box in the Room 107 after testing on 24 March 2017. If Room 107 were not able to fully comply with the requirement for a "locked room", then Regulation 366 might not have been complied with as well. That being said, the Task Force must point out that REO staff had placed their trust on the AWE as venue owner and management to ensure venue security, including prevention of unauthorised access to Room 107, especially during the time when REO staff had all left the site. In hindsight, the Task Force considers it neither desirable nor fair to place the responsibility solely on the AWE. In this sense, it would be advisable for the REO to take the initiative to request additional security measures be put in place by the venue management in future public elections.

53. On venue security planning, the Task Force also have the following observations:

(a) The transfer of responsibility for the venue set-up for the fallback site at AWE from E4CC to E3CC in mid-December 2016 aimed to even out the workload among various divisions in the REO. This has however given rise to coordination problems. In addition, while E3CC drew up the venue security plan on the basis of requests from different user teams and the advice from venue management and the Police, there was no formal endorsement process for the overall venue security plans. It was doubtful whether the REO senior management could have a holistic view on the adequacy of the security measures for different aspects of the venues and give instructions on the compliance with security requirements in a timely manner.

(b) In terms of records keeping and equipment tracking, the incident revealed that while there is an inventory list for IT equipment taken out of office, there is no inventory count for such equipment at the beginning and close of a working day in the fallback venue. Visitors who might have entered Room 107 after the departure of REO staff was not logged which could give rise to security loopholes.

54. To address the above issues, ***the Task Force has the following recommendations:***

(a) Given the importance of the security arrangements, the REO should establish formal procedures for endorsing overall venue security plans for public elections, and seek advices from relevant Police formations according to different purposes and scope of expertise. The overall security plan should be endorsed by CEO personally and submitted to the EAC for information and comments, if any.

(b) In cases where it is unavoidable for restricted information and/or personal data be stored in mobile devices and be stored in election venues, the relevant security measures should be strengthened as far as possible given the fact that such venues are mostly hired on a temporary basis and under the relevant licence agreements it could be impossible for the REO to have exclusive access control for certain parts of the venues. Locked cabinets that satisfy the relevant government regulation, CCTVs installed in the rooms for round-the-clock surveillance, or arrangement of designated security guards to impose access control, introduction of a visitor access

record are examples of possible additional security measures. This would minimize the risk of loss even if unknown parties were to gain access to the storage rooms. For fallback sites, with the objective of cost control and minimising wastage in mind, only minimal manpower would be deployed to manage the site and the storage of any personal data before actual activation of the site should be avoided.

(c) For better inventory management, REO staff should conduct inventory count at the end of each day before departure and a material log. To ensure consistency of venue security measures for the main and fallback sites, venue set-up of both sites should ideally be taken up by the same division (under one DCEO).

(d) There should be proper and comprehensive planning on the use of personal data and security arrangements for major election venues (including fallback sites) for every election. While the practice of past elections could be of reference, they must not be taken as assurance or guarantee that the arrangements adopted therein for handling of personal data or venue security would necessarily be flawless. A fresh examination should be conducted for every election and a plan for use of personal data and venue security should be endorsed at PEO level or above to make sure proper supervisory oversight and timely guidance and instructions be given. A thorough walk-through security assessment should be conducted for the entire site with focus on, among others, peripheral security (such as doors and locks, windows, partitioning), surveillance (such as guards and CCTV), as well as access control (access log, key management, authorization for entry). The Task

Force strongly advises that the REO should enhance communication with the venue management and come to a clear understanding on the venue security arrangements. It should also take into account the track record of individual venues in drawing up the security plan for public elections and put in place additional security measures as and when a need arises.

### *D. The Institutional Aspect*

55. The Task Force is of the view that there are inadequacies in the observance of the relevant guidelines and regulations stipulated by the Government for the handling of personal data, IT security, and general security. Notwithstanding this, the Task Force believes that there are several factors from the institutional aspect which could not be overlooked in identifying the causes of the present incident and in recommending measures to prevent future occurrence of similar incidents.

#### *(i) Organisational Structure and systemic reviews*

56. At present, the REO maintains only a skeleton establishment during non-election years and the staff establishment will be increased significantly during the election cycle through posting of civil servants and recruitment of NCSC and contract staff. To illustrate this, the PEO plays an overarching role in overseeing the preparation and organisation of all public elections in an election cycle. The post holder is expected to lead all teams under the E Division and to ensure that guidance and instructions are given in a timely manner and that the CEO as the head of the department is consulted on matters of significant importance.

However, the PEO post is a supernumerary one. The current post-holder joined REO in June 2014, while the four election divisions were only gradually staffed and strengthened in the run-up to the 2015 DCE and 2016 LCE. Considering the lead time required for much of the preparatory work such as the tendering for election materials, there was not much capacity for the staff in election divisions to familiarise themselves, with and critically review, past practices before they make plans for coming elections. This inevitably undermined the officers' ability to spot potential inadequacies in previous practices.

57. Relating to this is the fact there is no systemic review on whether the REO's work procedures could keep up with the prevailing versions of the relevant guidelines. The Task Force noted that the process for the storing of the EES, which contains personal data of all GC electors, in notebook computers has not been reviewed in recent years despite the amendment to the IT security guidelines in 2012 which provides that the storing of classified information to mobile device should be avoided and where this is indeed considered necessary the need must be justified and the request must be properly authorised. As a result, the teams concerned simply followed practices from previous elections and user requests for data was handled without any requirement for submitting additional justifications.

58. The Task Force further notes that largely owing to its specific organisation structure and the irregular posting cycles for the bulk of its election staff, the REO does not have a comprehensive system of knowledge management to transfer past experiences, post-event review, best practices, etc., for new post-holders to draw reference. The skeleton staff members that remain in the department between election cycles do

not have the necessary expertise and spare capacity to conduct holistic reviews on the organisation of different public elections, and this seriously undermines the REO's ability to introduce improvements and rectifications to the prevailing practices.

59. In view of the above observations, ***the Task Force has the following recommendations***:

(a) The post of the PEO should be made permanent, so that a proper hierarchy within the REO could be maintained at all times and the PEO could assist the CEO to review the preparation and organisation of public elections after an election cycle. Having a permanent "second-in-charge" post in the department would also allow the posting periods of the CEO and PEO to stagger, thereby helps preserving institutional memory in between different election cycles.

(b) The Task Force also considers it imperative that some core members in the election teams should be retained in non-election years to consolidate the experience in the previous election cycle, to distil lessons learnt, and to critically examine what improvements (systemic and detailed) could be introduced. The same team could also review if the current operating procedures are up-to-date in view of the past experience and latest government regulations and guidelines. Similarly, the ITMU only has two permanent civil servant staff on the technical side during non-election years, which significantly limit their capacity to review the IT security measures and related procedures and

guidelines. Possibility for enhancing the permanent establishment for the ITMU should be explored.

(c) Given the large number of NCSC staff in the REO especially at the peak of election cycle, civil servants occupying permanent posts in the REO should be assigned as far as practicable to take up key planning and supervisory duties. Taking into account the large number of time-limited posts (for both NCSC staffs and civil servants) during the election cycle, familiarisation programmes are essential for them to comprehend the procedures in organising elections and to alert them of any potential risks, such as maintenance of personal data in mobile devices.

*(ii) Accountability not clearly delineated amongst divisions*

60. It is observed that the "user" concept is widely used in the REO in the handling of personal data and coordination of venue security. For example, the ITMU would handle requests from "user" to prepare for the relevant IT equipment including the applications and systems to be installed in the computers, and the team coordinating venue security would rely on the requirement of different "users" in devising the overall venue security plan.

61. While the "user" concept enables the coordinating teams or the ITMU to understand better the need of different teams and make the necessary arrangement accordingly, it gives rise to a potential problem of lack of clearly delineated accountability. For example, the "user" who makes request for data systems may not be the best to determine the most appropriate system for their purpose. The ITMU in acceding to a

request from a user team would not assess the need for such a large amount of data as it assumes that the user making the request should know best. Indeed, upon a closer look at the request, it is apparent that a centralized hotline would suffice for verifying the identity of the entrants, and there was no need for the deployment of the EES in the election venue for CEE at all.

62. In devising the venue security plan, the "user" concept could also give rise to possible loopholes as the "user" and the coordinating team may have different understanding about their roles in ensuring relevant security. For example, for Room 107, the coordinating team, i.e. E3CC, did not receive from the ITMU any request for additional security measures and did not take the initiative to check what exactly was stored inside the room. On the other hand, ITMU did not give extra consideration or examination to the security setup of Room 107, believing that the room already met their requirement for a "locked" room and should have been inspected by E3CC.

63. To address this, ***the Task Force recommends that:***

a) the roles of "users" and coordinating teams must be clearly defined to make sure that the respective teams are aware of their responsibilities. In devising venue security plans, the "user" should have ultimate responsibility for the security of the rooms and ensure that additional security measures would be put in place as necessary. All equipment or materials brought to election venues should be clearly assigned to a specific user team to ensure accountability. Similarly, for requests for computer systems storing electors' data, the user teams should bear the responsibility

for specifying and justifying their need for data and be ultimately responsible for handling the data properly. The ITMU as gatekeeper should verify if proper approval has been sought, and ensure that the features and functions of the data systems are documented and communicated to the user teams.

## CONCLUDING REMARKS

64. Organising public elections is a hugely complex task which involves a lot of preparation, the bulk of which is minute and operational. The REO has over the years been conducting public elections in an open, fair and honest manner under the supervision of the EAC. While noting a number of inadequacies in the handling of personal data and arrangement for IT and venue security on the part of the REO in this incident, the Task Force fully recognizes that members of the REO staff have been working under immense pressure in the preparation of the various elections during the current election cycle. In around six months preceding the 2017 CEE, the REO had to organise the 2016 LCE in September 2016 and 2016 ECSSS in December 2016. Apart from the large amount of work in the organisation of elections which creates immense pressure, public elections have also been increasingly politicised in recent years and have received increasingly strong public and media attention. The Task Force appreciates the hard work of REO staff in organising the various public elections in the current election cycle, and recognises that the elections, including the 2017 CEE, were by and large conducted in a smooth manner.

65. The Task Force recognises that it is not tasked to conduct investigation under the civil service disciplinary procedures. Some of the factual narratives and observations in this report could reflect inadequacies in compliance with government regulations and guidelines. The Task Force would suggest that considerations be given as to whether relevant performance appraisal or disciplinary action procedures would be initiated in respect of the relevant officers and their supervisors.

66. This incident is an unfortunate event as it has caused distress among the general public and raised much concern about the handling of personal data by the REO. Looking positively, the incident serves as a reminder to REO of the importance to ever upgrading its capability to live up to the public's high expectation for the conduct of public elections. The Task Force expects the REO to implement the recommendations in full and continue to strive to provide high quality service to the public. In this connection, the REO should formulate a detailed plan to implement the various recommendations in this report the soonest possible. Some of the recommendations proposed by the Task Force, such as making the PEO post permanent, retaining core staff of E Division in non-election years, assigning dedicated staff to take charge of the updating of guidelines and manuals, and enhancing of training for staff, will require the provision of additional resources for the REO. CMAB will work with relevant bureaux to secure the resources required for implementing such recommendations.

**Annex A**

# Task Force on the Computer Theft Incident of the Registration and Electoral Office

**Membership:**

| | | |
|---|---|---|
| Leader: | | |
| Miss Rosanna Law | Deputy Secretary for Constitutional and Mainland Affairs 1 | Constitutional and Mainland Affairs Bureau |
| Members: | | |
| Mr Ryan Chiu | Principal Assistant Secretary for Constitutional and Mainland Affairs 3 | Constitutional and Mainland Affairs Bureau |
| Ms Phidias Tam | Principal Assistant Secretary for Constitutional and Mainland Affairs 4 | Constitutional and Mainland Affairs Bureau |
| Mr George Lee | Government Security Officer | Security Bureau |
| Mr Jason Pun | Assistant Government Chief Information Officer (Cyber Security and Standards) | Office of the Government Chief Information Officer |
| Mr S M Wong | Chief Electoral Officer | Registration and Electoral Office |

Note 1: The Chairman of the Electoral Affairs Commission attended all Task Force meetings as observer.

Note 2: Although a member of the Task Force, the Chief Electoral Officer was not involved in the drafting of this report or the interviewing of REO staff.

**Terms of Reference:**

1. To identify the reasons leading to the theft of two notebook computers in the back-up venue for the 2017 Chief Executive (CE) Election (AsiaWorld-Expo).

2. Taking into account the reasons identified in (1) above, to examine and review the current system of the Registration and Electoral Office (REO) on personal data handling, information technology security, implementation of Government Security Regulations, with a view to recommending measures to enhance REO staff's implementation of and adherence to the relevant regulations and guidelines generally and in respect of the planning and conducting of major elections (i.e. District Council, Legislative Council, Election Committee Subsector and CE Elections) specifically.

3. To examine and review REO's internal supervision and review system especially with regard to conducting major elections, with a view to recommending measures to strengthen REO's internal supervision and review.

**Annex B**

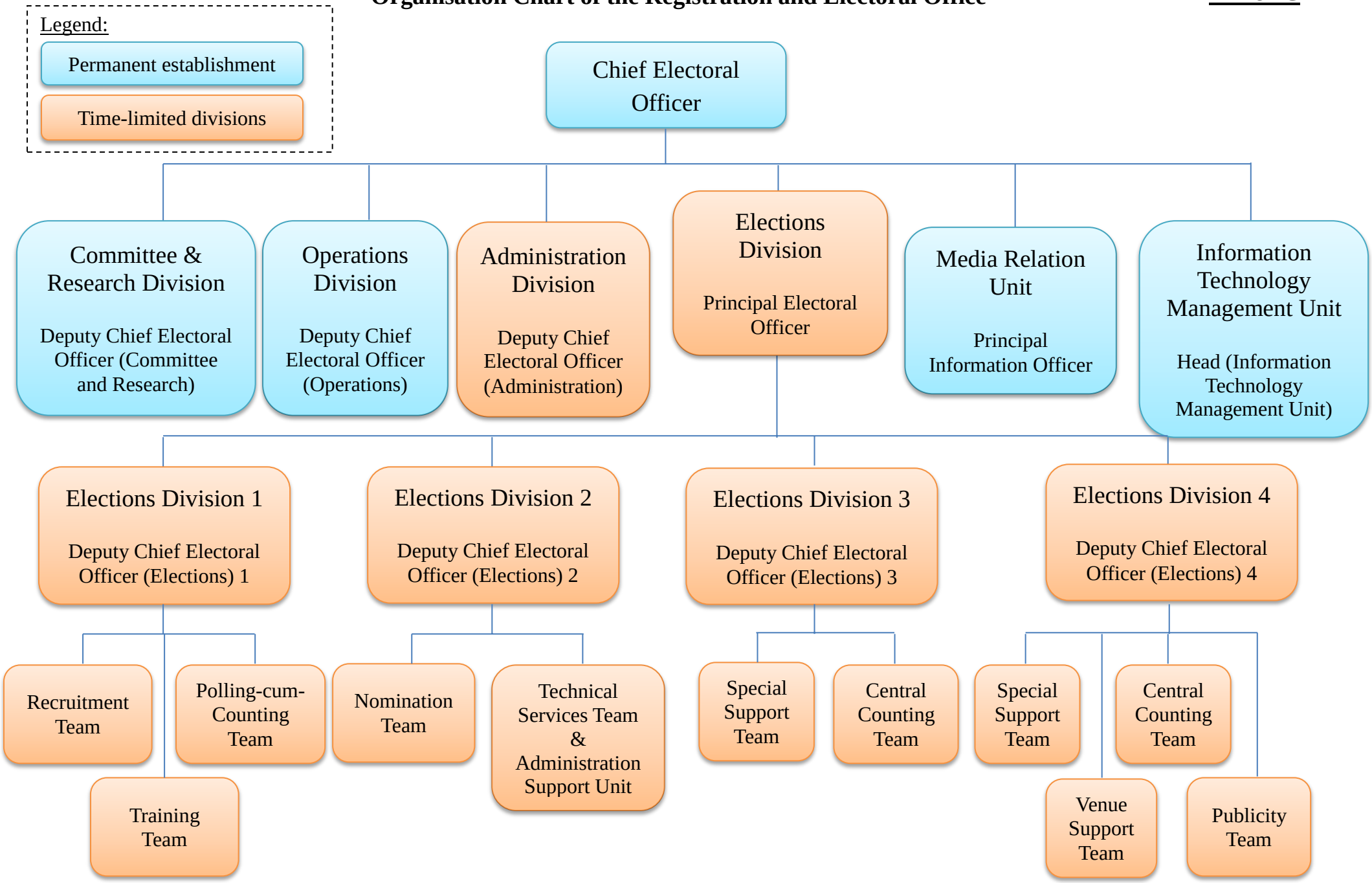
## List of Organisations Contacted by the Registration and Electoral Office after the Computer Theft Incident

Hong Kong Monetary Authority
The Hong Kong Association of Banks
The Hong Kong S.A.R. Licensed Money Lenders Association
Hong Kong General Chamber of Property Finance
The Hong Kong Federation of Insurers
Estate Agents Authority
The Hong Kong Mortgage Corporation Limited
Hong Kong Retail Management Association
The Chinese General Chamber of Commerce
Federation of Hong Kong Industries
The Chinese Manufacturers' Association of Hong Kong
Hong Kong General Chamber of Commence
The Chinese Gold & Silver Exchange Society
Hong Kong Futures Exchange Limited
The Stock Exchange of Hong Kong Limited
Hospital Authority
Hong Kong Computer Society
Hong Kong Information Technology Federation Limited
Communications Association of Hong Kong Limited
Hong Kong Wireless Technology Industry Association Limited
Hong Kong Software Industry Association Limited
Hong Kong Information Technology Joint Council Limited
Information Technology Division of The HK Institution of Engineers
Association for Computing Machinery, Hong Kong Chapter
Institute of Electrical and Electronics Engineers, Inc., Hong Kong Section, Computer Chapter
Institute of Electrical and Electronics Engineers, Inc., HK Section, HK Joint Chapter on Circuits & Systems/Communications
The Institution of Engineering and Technology Hong Kong
The British Computer Society (Hong Kong Section) Limited
The Hong Kong Association for Computer Education
Hong Kong Society of Medical Informatics Limited
Hong Kong Internet Service Providers Association Limited
Hong Kong Radio Paging Association Ltd.
Information and Software Industry Association Limited

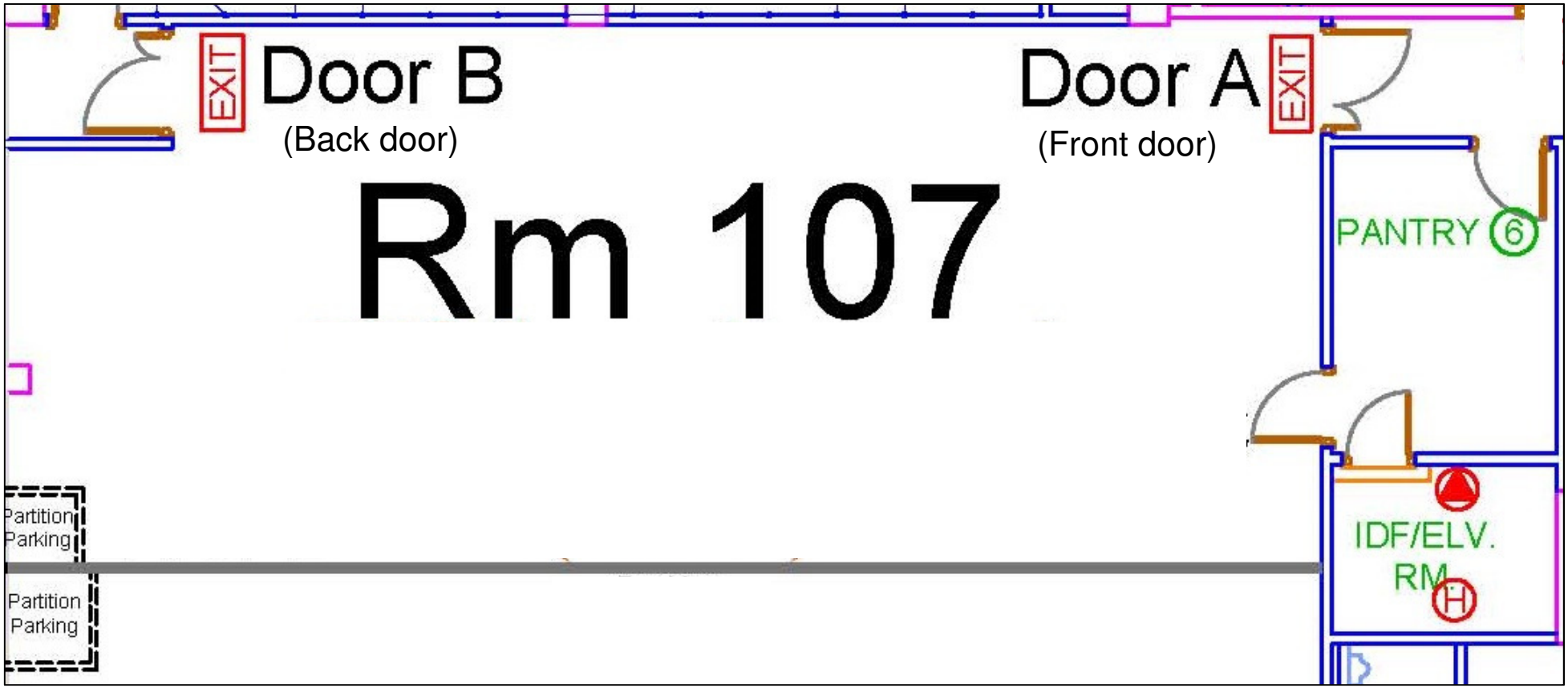
Internet Professional Association Limited
Professional Information Security Association
Information Systems Audit and Control Association China Hong Kong Chapter Limited
The Society of Hong Kong Services-Based Operators
Information Security and Forensics Society

**Annex C**

# Organisation Chart of the Registration and Electoral Office



**Annex D**




Doors A & B - Card and lock access mode.

Tenants assigned with card keys for access to the room in "card" mode.

**Annex E**

## Summary of Recommendations of the Task Force

| | |
|---|---|
| ***A. Handling of personal data*** | |
| 1. | REO should develop detailed guidelines and provide proper training to staff on the handling of personal data for organisation of public elections |
| 2. | The departmental Controlling Officer for Personal Data should be consulted on the transfer of personal data among divisions and preparation of computer systems involving loading of personal data |
| 3. | REO should develop a comprehensive privacy management programme (PMP) to enhance accountability for personal data protection |
| ***B. IT security*** | |
| 4. | REO should formulate as soon as possible a complete set of department IT security policy, procedures and guidelines which should also be reviewed regularly and kept up-to-date |
| 5. | ITMU should ensure that the systems of REO comply with the departmental IT security policy, procedures and guidelines |
| 6. | ITMU should advise the team which requests computer systems on the appropriate measures to protect the integrity of the data stored in computer systems |
| 7. | Approval by divisional head (at Chief Executive Officer level) must be sought before requests for personal data to be brought outside of the REO are made; measures to be put in place to ensure physical security must be set out in the application for approval |
| 8. | ITMU should play a gatekeeping role in assessing whether a request for storage of personal data mobile devices is commensurate with the operational need |
| 9. | The EES should not be used in public elections for the purpose of verifying the identity of voters |
| ***C. General security of election venues*** | |
| 10. | REO should establish formal procedures for endorsing overall venue security plans for public elections and seek comments from the Police, clear the plan with the CEO, and submit to EAC for information and comments |

| | |
|---|---|
| 11. | Security measures should be strengthened for restricted information and/or personal data stored in mobile devices and stored in election venues. Storage of any personal data in fallback sites before actual activation should be avoided |
| 12. | REO staff should conduct inventory count at the end of each day, and venue set-up of main site and fallback sites should ideally be taken up by the same division |
| 13. | A fresh, proper and comprehensive planning on the use of personal data and security arrangements for major election venues should be carried out for every election |
| ***D. Institutional aspects*** | |
| 14. | The post of the PEO should be made permanent to assist the CEO to review the preparation and organisation of public elections after an election cycle to preserve institutional memory |
| 15. | Certain core members in the election teams and key ITMU staff should be retained in non-election years to consolidate the experience in the previous election cycle and to introduce improvement measures |
| 16. | Civil servants occupying permanent posts in the REO should as far as possible be assigned to take up key planning and supervisory duties |
| 17. | Familiarisation programmes should be organised during election cycles for time-limited staff |
| 18. | Responsibilities between "users" and coordinating teams must be clearly defined |