立法會

資訊科技及廣播事務委員會

單仲偕議員於二零零六年三月十七日

就資訊保安有關課題作出的提問

問一　各部門有否進行資訊保安危機評估? 在進行資訊系統審計(Security Audits)的過程中, 他們採用何種資訊保安標準?

答一　政府的資訊保安政策、程序及指引訂明，各政府部門須每隔兩年進行一次資訊保安風險評估及審計，以確保其重要資訊系統符合保安水平。在政府資訊科技總監辦公室於本年三月進行的最近一次調查中，有 74 個決策局及部門確認已完成指定的保安風險評估,另 10 個部門亦已預訂於 2006-07 年度內進行評估。

各局及部門就資訊系統進行保安審計，一律採用政府的內部標準。這套標準是參考附件所列的國際標準及良好作業模式而制訂，當局並會不時加以檢討，以確保標準能反映科技發展及從業界得悉的保安威脅。

問二　各主要公營機構例如金融管理局、醫管局、證監會、電訊管理局等目前採取什麼措施去保障一旦出現的資訊危機? 當局有何監管措施以確保這些公營機構的資訊保安管治水平?

答二　爲了解主要公營機構處理資訊保安威脅所採取的防範措施，政府資訊科技總監辦公室已就負責這些機構的決策局及部門進行調查。據有關決策局及部門表示，提問引述的機構[1]已採取各種措施，以防範資訊保安威脅。這些措施包括建立保安管理架構、推行技術方案、設立事故管理程序及策劃業務持續運作安排。至於在調查內的其他公營機構，亦各自按不同組合採用此等措施。

調查又顯示，有關決策局及部門經已採取不同措施，以確保轄下各主要公營機構的資訊保安達至穩當水平。這些措施包括參與有關機構的董事局／管理委員會、要求提交管理／營運報告、公布資訊保安指引等。在某些情況下，公營機構規定須在適用的法例架構、既定的作業守則，或其他業界／專業標準的規範下運作，亦給予有關決策局及部門作出了這方面的保證。

[1]提問引述的公營機構包括金融管理局、醫管局、證監會及電訊管理局。

附件

制訂政府資訊保安標準所參考的
國際標準及良好作業模式列表

1. ISO17799:2005, Information Technology - Security Techniques - Code of Practice for Information Security Management

2. IS Standards, Guidelines and Procedures for Auditing and Control Professionals, Information Systems Audit and Control Association

3. National Institute of Standards and Technology, "Security for Telecommuting and Broadband Communications"

4. National Institute of Standards and Technology, "Wireless Network Security"

5. The Internet Engineering Task Force (IETF) RFC 2350 Expectations for Computer Security Incident Response

6. The Internet Engineering Task Force (IETF) RFC 2196 Site Security Handbook

7. Federal Information System Controls Audit Manual (Volume I - Financial Statement Audits), USA General Accounting Office

8. ISO/IEC 9798-3, "Information Technology - Security Techniques - Entity Authentication Mechanisms - Part 3: Entity Authentication Using a Public Key Algorithm"

9. ISO/IEC 9796, "Information Technology - Security Techniques - Digital Signature Scheme Giving Message Recovery"

10. ISO/IEC 9798-1, "Information Technology - Security Techniques - Entity Authentication Mechanisms - Part 1: General Model"

11. Malik, Gartner Group, "Enterprisewide Security"

12. ISO7498-2, "Information Processing System - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture"

13. Guide to Security Risk Management from Communications Security Establishment, Government of Canada