(Translation)

Legislative Council Panel on
Information Technology and Broadcasting

Questions on the topic of Information Security
Raised by Hon. SIN Chung-kai on 17 March 2006

Q1. Have government departments carried out risk assessment of information security? What standards on information security are adopted when conducting security audits of IT systems?

A1. As stipulated in the Government IT security policy, procedures and guidelines, all government departments have to conduct security risk assessment and auditing every two years to ensure the security level of their critical systems. In the latest survey conducted by the Office of the Government Chief Information Officer (OGCIO) in March 2006, 74 bureaux and departments (B/Ds) confirmed that they had conducted the security risk assessment exercise as required. Ten (10) B/Ds reported that they had scheduled to do the assessment in 2006/07.

In conducting security audits of IT systems, B/Ds have all adopted the Government's internal standards which were developed with reference to a list of international standards and best practices as shown in the Annex. Our standards are reviewed from time to time to reflect changes in technology and security threats known to us from different sources in the industry.

Q2. What protective measures are currently adopted by major public organisations such as Hong Kong Monetary Authority, Hospital Authority, Securities and Futures Commission and Office of the Telecommunications Authority should information security threat strike? Has the Administration taken any regulatory measures to ensure the IT security of these organisations is maintained at a satisfactory level?

A2. OGCIO has conducted a survey on B/Ds regarding the protective measures implemented by major public organisations under their purview for handling information security threat. The relevant B/Ds have reported that the organisations[1] cited in the question have adopted various measures to protect themselves against information security threats. These include setting up the security management framework, implementing technical measures, establishing incident management procedures and devising business continuity arrangements. For other public organisations not cited in the question, B/Ds have reported that they had adopted these measures in varying combinations.

According to the survey, B/Ds have also reported that different measures had been taken to ensure the IT security of the major public organisations under their purview was maintained at a satisfactory level. These include participating in the management boards/committees, receiving management/operation reports, or promulgating related guidelines on information security. In some cases, B/Ds got their assurance by way of the obligation under or compliance with applicable legislation frameworks, established code of practice, rules and regulations, or other industry/professional standards.

[1] The public organisations cited in the question include Hong Kong Monetary Authority, Hospital Authority, Securities and Futures Commission and Office of the Telecommunications Authority.

Annex

List of international standards and best practices referenced when drawing up Government's information security standards

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