**Bills Committee on Legislation Publication Bill (the "Bill")**

**Response to request for information by members on the Bill**

At the meeting on 7 January 2011, the Bills Committee asked the Administration to provide further information to address the concerns raised by members on the Bill.

## Protection of the integrity of the Database

2. We will follow the standards and guidelines issued by the Office of Government Chief Information Officer on IT Security to design and implement safeguards to protect the Database's integrity. A highlight of the preventive measures against hacking and fake web site is described as follows.

*Architecture of the system*

3. The Database's system architecture will contain multiple tiers, separating the external facing web server(s) and the internal server(s) which contain legislation data as shown in the diagram below. With such a tier-based architecture, even if an attacker compromises/hacks the external facing web server(s) from outside, the attacker still has to find ways to attack the internal network.

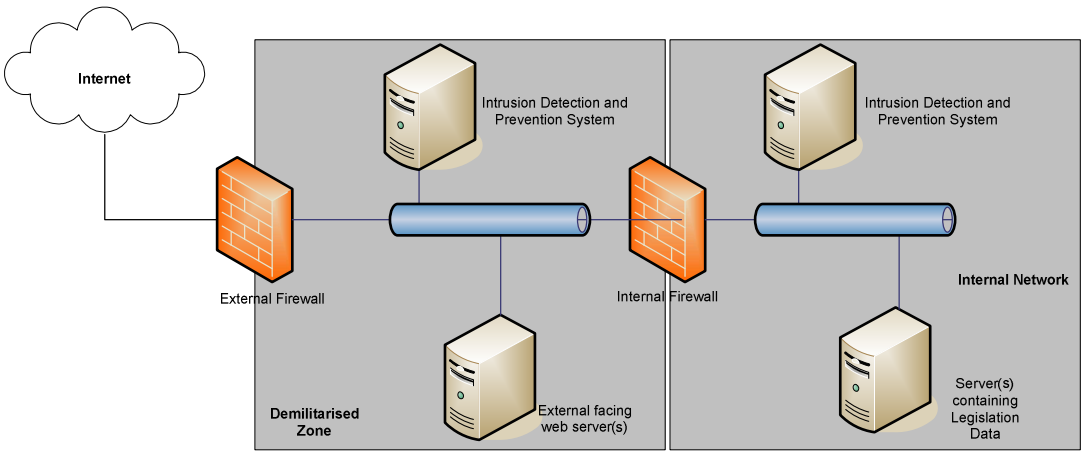


*Figure 2.1 High level illustration of the Database's system architecture*

4. The external facing web server(s) will be confined within a demilitarised zone (DMZ). The DMZ is a special network segment added between an internal network and an external network, such as internet, in order to provide an additional layer of security protection.

5. Both the external facing web server(s) and the internal server(s) will be protected by firewalls. Firewall is the sole means of entry and exit for all the data transmitting between Internet and the Database. All the data flow across firewalls will be inspected, data will be blocked if it does not meet the security criteria of the system. The internal and external firewalls will be from different vendors and will adopt different technologies in order to further enhance the security protection effectiveness of the firewalls.

*Intrusion detection and prevention mechanism*

6. We will install intrusion detection and prevention system (IDS/IPS) to detect and prevent attacks in the system. An IDS/IPS monitors the network as well as the servers of the system, it will keep track of changes on program, data and configuration of the Database and if it detects any potential hacking activity, sends alerts and reports to corresponding support staff for immediate follow-up actions. We will ensure most up-to-date intrusion and attack pattern information are in place so that, if applicable, IDS/IPS will be capable to stop these activities automatically and record them for subsequent analysis.

7. We will put in place anti-virus and malicious code detection software in all the servers, in order to prevent computer virus and malicious code from affecting the operation of the Database and the data thereof.

*Data communication and identity of the external facing web site*

8. All data transmission between the system and public will be protected by Secure Socket Layer (SSL). SSL encrypts the data being transmitted between the external facing web site and the public to ensure it will not be eavesdropped by third parties. At the same time, SSL also adopts the Public Key Infrastructure (PKI) technology to provide the proof of the identity of the external facing web site. Members of the public can validate the identity of the web site by checking SSL certificate information in their web browser software. The PKI technology has been widely adopted in web sites which require high level of security such as internet banking.

*Special security measures*

9. We will put in place automatic functions to periodically compare the legislation data of the external server(s) and internal server(s). In case

of discrepancy, alerts will be sent to corresponding support staff for immediate follow-up actions. For permanent record purpose, we will also have archiving devices to store legislation data to permanent, non-rewritable and removable media whenever legislation data are to be published or uploaded to the website of the system.

10. With a view to minimising the business and operational impact due to natural disasters and trespassing, the external facing web server(s) and the internal server(s) will be installed in different locations (i.e. in data centre(s) of a third party hosting company and in the Department of Justice's premises respectively) and disaster recovery environments will be provided.

*Fulfilment of security measures*

11. We will include the aforesaid security requirements in the tender document which when entered into will mandate the Database service provider to fulfil. Under the contract, the Database service provider must conduct security planning and implement appropriate security measures and controls for the Database.

*Security Risk Assessment and Audit*

12. To ensure that the security measures for the Database will comply with the standards adopted by the Government, independent consultants will be engaged to conduct security risk assessment and audit before the full roll-out of each phase, as well as periodically after the Database is launched.

*Manpower and overseas experience*

13. Sufficient manpower would be reserved to verify the data in the Database against the hardcopy legislation. Also, all contractual staff would be closely monitored and supervised by internal professional staff to ensure efficiency and accuracy.

14. We have consulted our counterparts in the UK and the Commonwealth, NSW and ACT in Australia on measures against possible security threats such as hacking. The security measures adopted are commensurate with their assessment of the risk of hacking. According to their implementation experience, the chance for their legislation database being hacked is on the low side and there is no incidence of hacking so far.

## Safeguard measures

15. The establishment of the new Database is to facilitate public access to updated and consolidated HK legislation. The Database only provides copies of legislation which are presumed, unless the contrary is proved, to correctly state the legislation. Any user can verify the copies in the Database with the hardcopy Gazette which is deemed to be an "authentic copy" of Ordinances under section 98(1) of the Interpretation and General Clauses Ordinance (Cap. 1). Also, we would endeavour to ensure the integrity of the Database by putting in place adequate security measures as described in paragraphs 2 to 12 above to prevent any unauthorized interference to the Database.

16. Under the adversarial system in HK, it is natural that different parties involved in a matter would access the Database at different times and consult different sources. The chance of a user relying on altered legislation is rather slim. Moreover, we have made it clear in the Bill that any unauthorised amendment made to the copies of Ordinances published in the Database, whether with malicious intent or not, does not have any legal effect and does not change the text of the Ordinances.

17. While we are eager to provide accurate information on the Database and tackle any possible hacking or false websites, we do not think it advisable to provide for statutory redress for reliance on inaccuracies in materials in an official version of the laws. Also, we are not aware of any major common law jurisdictions providing this kind of redress.

## Commencement of the BLIS

18. The Bilingual Laws Information System (BLIS) was made available to the public in November 1997, and 1 July 1997 was adopted as the benchmark date. The system contains legislation in force in Hong Kong on or after that date, and legislation in force immediately before that date (i.e. on 30 June 1997).

## Estimated cost for back capturing before the benchmark date

19. The following is an assessment of the manpower and costs involved in preparing the past versions of laws from the first issue of the Loose-leaf edition.

20. We would need to involve colleagues of different grades in the exercise, including typists to type out the text of legislation and subsequent amendments; assistant clerical officer, law clerks and senior law clerks to incorporate the amendments and check the accuracy of each and every consolidated version; as well as counsel to monitor the whole project and handle special cases. We also have to ensure that all contractual staff would be supervised by internal professional staff.

21. We are unable to provide very detailed estimates at this stage. [1] However, given the huge amount of time and manpower involved, our preliminary rough estimate is around $44,544,000 for the whole exercise.

22. The staff costs to be saved from the retirement of the Loose-leaf Edition will be deployed to help ensure that laws are compiled in a meticulous manner that is commensurate with the legal status of the new Database. The saved staff effort would also be used to provide more information and services under the new Database such as records of amendment and email alert service.

**Arrangements for retiring the Loose-leaf**

23. We would consult the AJLS Panel, the Hong Kong Bar Association and the Law Society of Hong Kong and other stakeholders before we seek to commence Clauses 21 and 26 of the Bill. Views expressed would be duly considered and we would not table the commencement notice until we are satisfied that the arrangement is practicable.

24. In light of the above, we are of the view that negative vetting procedure would be sufficient and there is no need to emphasize in the Bill that the commencement date for Clauses 21 and 26 are different from that for other provisions. This is also in line with the prevailing drafting practice.

**Department of Justice**
**January 2011**

[1] The rough estimate has not included the costs required for conducting a feasibility study before it can be decided whether to take up the project.