理由陳述

網絡安全法

（法案）

一、制定本法案的必要性

隨着互聯網及通訊技術高速發展和廣泛應用，澳門特別行政區如同其他的國家或地區一樣，正朝智慧城市的方向發展，“工業 4.0”引領澳門進入人工智能及大數據的網絡時代，資訊化與社會各領域的活動和各階層市民的日常生活密切相關。電腦、資訊網絡及互聯網成為各行各業及廣大市民日常生活的必要工具。

誠然，資訊化及人工智能為人們、企業及機構帶來莫大裨益與方便，但正因為其異常重要，面對全球網絡安全威脅，公私領域的網絡和資訊安全面臨網絡入侵及襲擊的嚴峻挑戰，為確保主要資訊網絡運作暢順及無間斷，以及為保障電腦數據資料的保密性和完整性，有必要制定適當的防護機制。

澳門特別行政區政府曾在《二零一六年財政年度施政報告》保安範疇強調“由於技術的缺陷和防範意識的不足，資訊系統的高危漏洞必然有增無減，公私領域的網絡和資訊安全正面臨嚴峻的挑戰；各種形式的網絡犯罪及網絡安全事故，正以前所未有的規模、嚴重性和複雜程度出現”。

送立法會第一文本

基於此，本法案旨在從法律上構建上述的防護機制，清楚制訂網絡安全方面的義務和責任，透過強化公共和私人機構營運的關鍵基礎設施的網絡安全，維護公共安全、公共秩序及社會穩定等重大公共利益，以及保障澳門居民的利益。在本法案的公開諮詢過程中，相關業界與公眾的意見普遍認同立法的必要性。為確保澳門居民的正當權利，澳門特別行政區政府在草擬《網絡安全法》法案的過程中，一直遵守《個人資料保護法》的規定，並且在法律生效後，亦會對法律的成效持續作出必要的檢討。

本法案的直接保護標的是公共部門和營運關鍵業務的私人實體的資訊網絡及資訊系統，包括運輸、電訊、銀行和保險、醫療衛生、水電供應等本法案第四條（適用的主體範圍）盡數列舉的業務。本法案稱此等公共部門及私人實體為關鍵基礎設施營運者。

本法案選取上述領域及實體的理由是，一旦有關的資訊網絡及系統受到襲擊，將造成極大的衝擊，直接危害公共安全及秩序，以及廣大市民的福祉，無可避免地將對社會帶來嚴重後果。

二、法案的內容

1. 法案的編排與結構

本法案共五章，分別為一般規定、組織規定、網絡安全義務、處罰制度、過渡及最後規定。

送立法會第一文本

2. 一般規定

本法案第一章確立（法案的標的）構建網絡安全的框架性體系。為此，對若干重要的表述作出明確定義，例如資訊網絡、關鍵基礎設施、未經許可的行為、網絡安全事故等，本法案亦訂明網絡安全所涉及的活動（第三條），以及規定本法案的適用主體範圍（第四條）。就一些不適合納入適用範圍的實體，第五條對適用主體劃定不適用的範圍。

網絡安全體系是具行政性質的體系，其主要性質為防範資訊網絡的威脅。

本法案不規範網絡安全的具體措施（例如“防火牆”、鑑證、存取控制、電子簽名、入侵檢測系統、加密系統等），原因是此類措施極具多變性，且含高度技術成分。該等措施應透過監察實體的指示及傳閱文件所制訂的純規範性條文規範（參見第三條（二）項）。本法案建議的制度與金融體系法律制度所採用的技術監察及規管模式相似。

3. 組織規定

本法案第二章規範整個網絡安全體系的架構（或組織）。該體系將有關的實體分成兩大類別：

- 總體性的實體：屬頂層機關的“網絡安全常設委員會”，其職權主要是訂定實現網絡安全目標的一般性及策略性的方向及目的；以及主要負責管理及執行緊急事故應對措施的“網絡安全事故預警及應急中心”；

- 各領域的實體：對包括公共部門、機關及實體在內的關鍵基礎設施營運者在其業務領域內遵守網絡安全義務的情況作出長期常規性監測的實體。

本法案細列了上述實體較重要的職責；關於職權及運作的事宜，建議以補充性行政法規規範。

4. 網絡安全義務

為使網絡安全達至應有的水平，本法案第三章規定關鍵基礎設施營運者須履行的義務。

為條文清晰起見，有關的義務按照其性質於四條條文內訂定：

- 組織性義務；
- 程序性、預防性及應變性義務；
- 自行評估及報告義務；
- 合作義務。

第十條至第十三條訂定關鍵基礎設施的私人營運者的網絡安全義務的標準，第十四條則按關鍵基礎設施的公共營運者的特質訂定其義務。

該章內容包含本法案的核心規定。關鍵基礎設施營運者以標準化及監察模式有效地推行網絡安全的義務，確保達至這項全新法律制度的下列主要目標：確保關鍵基礎設施營運者所使用的資訊網絡及電腦系統的可操作性、完整性及可用性，以及電腦數據資料的保密性，以防止該等資訊網絡、電腦系統及數據資料遭受未經許可的行為所損害或任何形式的影響。

設立“網絡安全主要負責人”的職位，旨在於組織內引入較大的個人責任機制。該建議要求有關人員須具備適當資格及專業經驗，並訂定某些強制規定，確保其在澳門特別行政區切實聽候安排，以便與當局合作，尤其是在緊急情況下。

由於本法案第十一條所指的網絡安全的技術操作義務（“防火牆”、認證、存取控制、電子簽名、入侵檢測系統、加密系統等）極具多變性及含高度技術成分，因此，以規章性文件規範。

第十二條所指的自行評估及報告義務有兩個目的：強制要求關鍵基礎設施營運者定期自行評估，同時，讓公共當局知悉真正及具體的情況，藉此建議調整及改善有關的法律或法規制度，以提升澳門特別行政區網絡安全的水平。

最後，合作義務是為確保在網絡襲擊的緊急情況下能作出適當且有效的介入。然而，網絡安全事故預警及應急中心的代表僅在為查核防護機制義務的遵守情況下，方可進入營運者的關鍵基礎設施，該等防護機制包括“防火牆”、認證、存取控制、電子簽名、入侵檢測系統、加密系統等。面對網絡襲擊時的介入是根本性的工作，其目的在於防止營運者的網絡及電腦系統因網絡安全威脅擴散而受病毒感染。

為使網絡安全體系運作靈活，關鍵基礎設施營運者可“授權”第三人為其推行及確保網絡安全，但下列者除外：

- 公共營運者方面：僅在經行政長官預先許可的情況下，方可“授權”網絡安全私人服務提供者，但不免除有關的公共實體適切“監

督”及監察私人服務提供者的工作表現，並在必要時及私人服務提供者因過錯或不作為而須負責任時予以取代（本法案第十四條第一款（三）項）；

- 私人營運者方面：保留“授權不免除私人營運者的行政違法行為責任”。因此，即使可將不遵守網絡安全義務的責任歸咎於網絡安全私人服務提供者，但私人營運者仍可被處罰；換言之，可能出現的情況是，該等私人營運者其後可向網絡安全私人服務提供者追究民事責任（本法案第十五條第三款）。

5. 行政處罰制度

本法案第四章涉及處罰性條文。

違反網絡安全義務，如情況嚴重，科澳門幣十五萬元至五百 萬元罰款；如情況較輕微，科澳門幣五萬元至十五萬元罰款。

然而，在一些特殊情況下（如有關情況對網絡安全不構成實質危險，且非屬累犯），監察實體可勸誡違法者在指定期間補正不合規範的情況。相反，對較嚴重的違法行為，可單獨或合併科處下列附加處罰：

- 剝奪參與公共部門、機關及實體購置物品或取得服務的公開招標的權利；
- 剝奪獲公共部門、機關及實體發給津貼或利益的權利。

送立法會第一文本

由於某些違法行為可能同時違反其他規範（例如違反《個人資料保護法》），本法案專門設立一條規定以規範該情況。此外，本法案亦規範了累犯、立案權及處罰權的內容。

儘管如此，有關章節篇幅不大，而精簡條文的原因是考慮到本法律制度適用對象的特質，基本上均是具有穩定性的大、中規模企業。

關於關鍵基礎設施的公共營運者，如其負責人故意或過失地不履行有關義務，須負起紀律責任，甚至在嚴重的情況下，以撤職論處。

6. 過渡及最後規定

本法案最後一章的內容涉及兩個實質問題，該等問題雖不直接涉及網絡安全，但與網絡安全息息相關，因為都是為了更好地保護資訊網絡及其廣大用戶。

首個問題涉及“實名制”：網絡經營者與用戶簽訂合約、確認向用戶提供互聯網接入服務、域名註冊服務、固定或流動公用電信服務時，網絡經營者應要求用戶提供真實身份資料。該制度乃參照國際上採用的方式，是一種對付利用流動電話終端的“用戶身份模塊卡”（下稱“SIM 卡”）作犯罪用途的震懾機制。

第二十三條以過渡規定的形式處理在法律生效前購買的無須預先提供身份資料的預付式 SIM 卡的情況。

第二個問題涉及“保存及提供私人網絡地址轉換成公共網絡地址*(network address translation)*的紀錄”：網絡經營者向用戶提供互聯網接入服務時，應將用戶私人內聯網地址與互聯網公共網絡地址（IP）的轉換紀錄保存一年。由於這問題涉及作倘有的刑事調查用途的數據保存，有關的內容透過在第 11/2009 號法律《打擊電腦犯罪法》內增加一條條文的方式和諧地引入該法律。而警察當局獲取該等數據時，須遵守司法機關的監管制度，因此，並不存在保護隱私的問題。

除上述兩個問題外，最後一章訂定了適用的補充法律、補充規範及生效日期的慣用規定。

在適用的補充法律方面，第二十六條的條文是以簡化本法案的方式作出。

由於准用十月四日第 52/99/M 號法令《行政上之違法行為之一般制度及程序》，因此，無須在本法案另行規定罰款的歸屬和繳付期間等問題。

另外，由於准用刑法及刑事訴訟的一般原則，因此，無須在本法案規範處罰的酌科等事宜（這方面的事宜經必要配合後適用《刑法典》第六十五條所載的原則）。

在補充規範方面，本法案以一般性條文的方式規定，行政長官具權限發出為妥善執行《網絡安全法》所需的補充規範。儘管如此，本法案對下列內容作出明確規定：

- 規範網絡安全常設委員會、網絡安全事故預警及應急中心的組成、職權和運作方式；

- 透過准用第 2/1999 號法律《政府組織綱要法》及第 6/1999 號行政法規《政府部門及實體的組織、職權與運作》的規定，指定負責監察關鍵基礎設施的私人營運者的公共實體，以及列明指定該等監察實體所持的邏輯。

至於生效方面，本法案規定其自公佈後一百八十日起生效，但將私人內聯網地址轉換成互聯網公共網絡地址（IP）的紀錄保存一年的特定義務除外（網絡經營者僅須在較後的日期開始履行有關義務，以便其能為履行義務作出必要的實際準備工作）。