澳門特別行政區

《網絡安全法》

諮詢文本

公開諮詢期：二零一七年十二月十一日至二零一八年一月二十四日

澳門特別行政區政府

二零一七年

目錄

序言

資訊科技與澳門特別行政區各行各業及市民的生活已經分不開，電腦、手機等資訊設備及互聯網成為日常生活不可或缺的工具，“移動互聯網”、“互聯網+”、“雲服務”、“物聯網”和“人工智能”等新興技術迅速發展且廣泛應用，網絡已成為訊息傳播的新渠道、生產生活的新空間、經濟發展的新引擎、文化傳承的新載體、社會治理的新工具、交流合作的新平台及國家主權的新疆域。

然而，當今國際形勢複雜多變，恐怖主義瀰漫全球，各種犯罪亦乘勢衝破地域限制，利用資訊系統的高危漏洞，實現跨境化及全球化，網絡攻擊及網絡入侵的種類亦層出不窮，網絡安全涉及國家安全及個人安全，成為了世界先進國家及地區政府的關注焦點，紛紛就網絡安全專門立法規範。在這方面，澳門也不能獨善其身，有必要配合全球趨勢，為促進澳門社會的網絡系統良好運作，以及確保網絡數據完整及得到充分保障進行立法，從而為社會的關鍵基礎設施構建一個良好的防範管理體系，以更好地配合國家“一帶一路”的發展倡議，以及《澳門特別行政區五年發展規劃（2016－2020）》有關建設智慧城市、推動產業與互聯網融合的發展目標。

為此，行政長官於 2015 年指示成立跨部門網絡安全工作小組，由

保安司司長統籌協調各相關部門開展澳門特別行政區網絡安全立法及部門構建等工作。小組在 2016 年訂定了網絡安全工作計劃和網絡安全總體框架後，隨即啟動網絡安全框架法律的立法工作，並遵從下列三大原則構思網絡安全法：

1. 保障市民安全，尊重個人隱私；

2. 適度立法（尤其在立法對象方面和技術措施方面）；

3. 架構設置精簡有效。

建立網絡安全法律制度有賴社會各界人士，包括與廣大市民的日常生活息息相關的各關鍵基礎設施營運者的積極參與，為此，澳門特別行政區政府冀以盡量透明的方式，讓大眾了解我們的立法目的及原意，從而廣泛聽取社會各界的意見，優化有關制度的制定工作。

在此，我們誠意邀請各界人士（包括市民、企業及機構）在以下期間透過下列方式，就本諮詢文本的內容提出書面建議或意見：

1. 公開諮詢期：

二零一七年十二月十一日至二零一八年一月二十四日

2. 遞交建議或意見的方式：

（1）信函方式：郵寄或直接遞交予澳門特別行政區兵營斜巷保安司司長辦公室或水坑尾街 162 號公共行政大樓 27 樓行政公職局。

（2）電子方式：透過澳門特別行政區政府入口網站（www.gov.mo）或保安司司長辦公室網站進入專頁（www.gss.gov.mo/ch/ciberseg）發表意見。

3. 建議或意見的封面：有關文件的封面或開首處，請註明“關於《網絡安全法》的立法意見和建議”。

4. 提出建議或意見及保密聲明：請參考本諮詢文本附件“關於《網絡安全法》的立法建議和意見欄”，提出建議及意見。如希望將所提出的意見或建議保密，祈請在相關欄目內清楚指明。

本諮詢文本可在保安司司長辦公室網頁下載，網址：www.gss.gov.mo/ch/ciberseg。

1. 建立網絡安全防護體系

關於資訊及網絡方面的法律制度，現時只有第 11/2009 號法律《打擊電腦犯罪法》規範網絡犯罪及其刑責，卻沒有專門規範網絡安全行政管理的法律或法規。

網絡與國家安全及民生密切相關，預防勝於一切。然而，預防工作不可能單靠政府，而是需要社會各界的積極參與。只有政府、社會各界和廣大市民上下齊心，彼此配合，方可有效地防護網絡的安全。

有見及此，經參考中國內地及其他國家或地區的相關法律制度，澳門特別行政區政府認為亟需填補制度上的空白，在遵照“保障市民安全、尊重個人隱私”的原則下，設法構建屬於澳門的網絡安全防護體系。同時，有關體系屬於防範性行政管理體系，當中各方在網絡安全方面的義務和責任需清楚訂明。因此，政府擬制定的《網絡安全法》將是一部以“守護”、“防範”及“管理”為主的法律，透過監察關鍵基礎設施營運者是否履行網絡安全義務，以及監察關鍵基礎設施營運者資訊系統與互聯網之間的資訊數據流量以及其數據包特徵等，了解網絡安全狀況，達至防範、偵察及打擊網絡入侵及攻擊，確保關鍵基礎設施網絡安全，保障本澳公共安全、公共利益或公共秩序；應對網絡安全事故，推行網絡安全義務及措施，進一步完善網絡安全防範管理制度；發出預警信息，防止或減少關鍵基礎設施的網絡安全事故；以及開展針對性的宣傳教育活動，提升關鍵基礎設施營運者的網絡安全意識等目的。

至於涉及網絡、資訊、電腦領域的刑事不法行為，仍然由《打擊電腦犯罪法》進行規範。

基於網絡安全的具體防護機制及措施因應不同情勢，需隨時進行更新和調整，強調專業性和技術性，因此我們遵照適度立法的原則，建議《網絡安全法》法案不直接規範維護網絡安全的具體措施，例如防火牆、加密

系統、電子認證和病毒入侵檢測系統的採用標準等技術標準，此類措施將按照政府所訂定的總體方向透過監察實體的指示及傳閱文件作出規範。

2. 關鍵基礎設施和網絡安全的相關定義

社會的正常運作及居民的日常生活，離不開基礎設施的服務供應，例如自來水及能源（電力、天然氣）等供應；陸上、海上及航空運輸；電視及無線電廣播；公共網絡包括互聯網服務；銀行、財務及保險服務；醫療服務；公共服務（政府部門提供之各項服務）等等。如果關鍵基礎設施的資訊網絡及系統一旦受襲擊，其網絡系統遭破壞、數據洩漏或喪失功能，將會造成極大的社會衝擊，甚至令政府和社會的運作陷入癱瘓，直接危害公共安全及公共秩序，以及廣大市民的福祉，無可避免地對社會帶來無法估計的嚴重後果。

考慮到中國內地、歐美發達國家、俄羅斯、新加坡、香港及台灣等國家及地區均先後以法律及其他配套措施重點保護上述的“戰略設施”，我們建議在立法時將上述設施的經營者定義為“關鍵基礎設施營運者”，並規範其網絡安全義務，進一步完善網絡安全防範管理制度。

為清晰與網絡安全有關的表述，我們建議對相關事物作出下列定義：

“關鍵基礎設施”是指對社會利益及社會正常運作具有重要意義的資產、系統和網絡，不論其營運者屬公共性質或私人性質，該等資產、系統和網絡一旦遭到破壞、數據洩漏或喪失功能，可能嚴重危害公共安全、公共利益或公共秩序。

“關鍵基礎設施營運者”是指營運關鍵基礎設施及提供有關服務的公共或私人實體。

“網絡”是指由電腦或其他電腦終端及相關設備互相連接的系統，該系統按照一定的規則及程序對數據進行收集、儲存、交換、傳輸及處理。

“網絡數據”是指通過網絡收集、儲存、傳輸、處理及產生的各種電子數據。

“網絡安全”是指澳門特別行政區所推展的長期且多領域活動，旨在

保護關鍵基礎設施營運者所使用的主要資訊網絡的安全，以保障網絡數據的完整性、保密性及可用性，並防範網絡遭受意外事故和未經許可的行為，尤其私自存取、入侵、使用、控制、干擾、洩漏、破壞、修改或銷毀的影響。

“網絡安全事故”是指任何可能或已經對網絡的運作或其內運行的網絡數據的機密性、完整性或可用性造成損害或影響的事件。

3. 網絡安全防護體系的適用對象

按照上述的定義，“關鍵基礎設施營運者”來自公、私兩大領域，其對一些重要的“關鍵基礎設施”的網絡安全，須負起一定的責任，絕對不容有失。

3.1. 關鍵基礎設施的公共營運者——公共機關、部門及實體

此建議的表述將涵蓋所有的公共機關、部門及實體，尤其包括：

（1）行政長官辦公室、政府主要官員的辦公室及行政輔助部門、立法會輔助部門、終審法院院長辦公室及檢察長辦公室、廉政專員辦公室及審計長辦公室；

（2）以任何形式設立的公務法人及自治基金；

（3）無法律人格但具財產及財政自治權的其他公共部門及機構。

然而，上述公共機關、部門及實體如根據適用的組織法規定或行政長官批示，不使用網絡或使用網絡但由其他公共實體保障其網絡的操作、維護及安全的，則不屬本法律制度的適用對象。

3.2. 關鍵基礎設施的私人營運者

當代社會的多項重要公共服務趨於“私營化”運作，由私人企業或機構提供相關的服務，公共部門和私人機構成為了現代社會的公共服務提供者。

故此，我們建議將下列的私人實體界定為“關鍵基礎設施的私人營運者”：

- 以特許經營方式、准照方式或判給方式開設及營運具重大公共利益的特定業務的私人實體；
- 全公共資本公司；
- 法規定性為行政公益法人的私法人，但其業務適宜被排除者除外。

上述實體是按既有的法律制度規定開設與經營，包括以下實體：

（1） 以特許經營方式、准照方式或向行政當局提供服務的判給方式開設及營運者：水電及天然氣供應及分配、燃油批發、污水處理和垃圾收集及處理、受衛生檢疫及植物檢疫的食品批發、法定屠宰宰殺動物、港口及海上運輸、機場、直升機機場及航空運輸、陸上運輸、視聽廣播（衛星電視及僅限於娛樂節目廣播的營運者除外）、娛樂場幸運博彩；

（2） 以行政准照方式開設及營運者：私人醫院、銀行、財務實體及保險業機構；經營公用固定或流動電信網絡以及提供互聯網接入服務的實體（我們專門稱之為“公共網絡經營者”）以及其他持准照經營上項(1) 所指業務範疇的實體；

（3） 全公共資本公司；

（4） 由法規定性為行政公益法人的私法人，但其宗旨與慈善、救濟、教育、文化及/或娛樂活動有關者除外。

4. 政府的監察實體

《網絡安全法》能否有效地防範遭受攻擊，有賴健全的監察機制。為此，我們遵照“架構設置精簡有效”的原則，建議網絡安全的監察系統為一個三層次的運作架構：

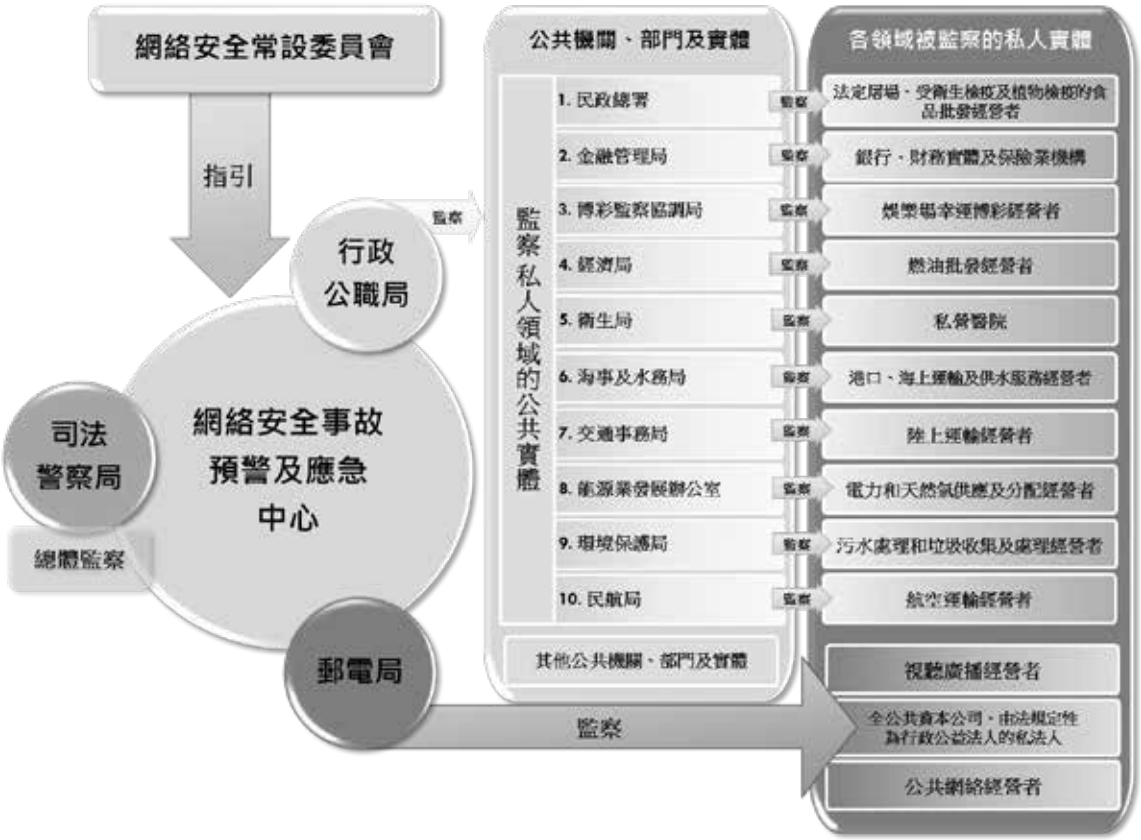
第一層次：“**網絡安全常設委員會**”，屬頂層機關；

第二層次：“**網絡安全事故預警及應急中心**”，屬行動統籌機關；

第三層次：**各領域的監察實體**（參見下圖）。

三層次的監察系統有機運作，策略與執行無縫對接、上下貫通，務求監察到位。

網絡安全管理架構



4.1. “網絡安全常設委員會”

“網絡安全常設委員會”是網絡安全的頂層決策機關，宏觀地監察整個特別行政區的網絡安全情況，主要負責為訂定網絡安全總體方向、目的及策略；關注及評估公共機關及實體和私人實體涉及網絡安全的活動的發展及運作；就澳門特別行政區網絡安全總體報告作出審議及議決；向網絡安全事故預警及應急中心和監察實體發出相關指引。委員會由行政長官擔任主席、保安司司長任副主席，其他委員為各司司長及網絡安全監察實體的領導。

4.2. “網絡安全事故預警及應急中心”

“網絡安全事故預警及應急中心”是落實網絡安全防範工作的核心組織，肩負協調行動、上情下達和下情上達、內外交流的重要任務。由司法警察局、行政公職局及郵電局負責該中心的運作。為有效運作，三部門派人參與網安義務履行情況的監察工作，各司其職，但互相合作及通報。該中心實行二十四小時無間斷運作，並由司法警察局負責統籌。中心根據國際上的普遍做法，監察關鍵基礎設施資訊系統與互聯網之間以機器語言方式傳輸的資訊數據，在必要時實時監察數據流量大小、數據包特徵等，以防範、偵察及打擊網絡入侵及攻擊。

“網絡安全事故預警及應急中心”負責以下職能：

（1）應對網絡安全事故、推行網絡安全義務及措施，以及為此收集網絡安全預警消息，並協調不同參與實體之間的合作及適當行動，與外地同性質的實體合作，以防止或減少網絡安全事故的影響；

（2）按照網絡安全常設委員會訂定的目標和政策，以及國際上的良好實務經驗，訂定事故預警及應急行動的模式、指示和程序，並向網絡安全體系的所有參與者作出宣傳；在必要時，就網絡安全事故發出預警信息；

（3）向網絡安全常設委員會提交網絡安全總體報告以及提供其所需的支援；

（4）向監察實體及被監察實體提供其所需的技術支援，以便其切實履行其責任及義務；

（5）開展網絡安全方面的宣傳教育活動。

4.3. 各領域的監察實體

“關鍵基礎設施”按照定義分為公共及私人兩大領域，所以監察系統的第三層次——**“各領域的監察實體”**亦相應分為兩方面：一方面，由行政公職局負責監察公共機關及實體；另一方面，由十一個公共部門監察私人領域的關鍵基礎領域營運者，詳細分工如下（參見第 11 頁圖）：

（1）民政總署監察法定的動物屠場、衛生檢疫及植物檢疫的食品批發經營者；

（2）金融管理局監察銀行、財務實體及保險業機構；

（3）博彩監察協調局監察娛樂場幸運博彩經營者；

（4）經濟局監察燃油批發經營者；

（5）衛生局監察私營醫院；

（6）海事及水務局監察港口、海上運輸及供水服務經營者；

（7）交通事務局監察陸上運輸經營者；

（8）能源業發展辦公室監察電力及天然氣供應及分配經營者；

（9）環境保護局監察污水處理和垃圾收集及處理經營者；

（10）郵電局監察公共網絡經營者和視聽廣播經營者、全公共資本公司及上文第 3.2.項第(4)分項所指由法規定性為行政公益法人的私法人(但其宗旨與慈善、救濟、教育、文化及/或娛樂活動有關者除外)；

（11）民航局監察航空運輸經營者。

“**各領域的監察實體**”的職權包括：

(1) 按照常設委員會發出的指引，為其監察的營運者釐定網絡安全內部管理制度的範圍，尤其是涉及網絡襲擊和網絡入侵的日常防護機制及工具方面；

(2) 與網絡安全事故預警及應急中心合作，釐定應急程序指引的範圍及在事故發生時推行該等程序；

(3) 收集其監察的營運者網絡安全報告，並抄送其副本予網絡安全事故預警及應急中心；

(4) 根據法律規定監察網絡安全規則的履行情況。

5. 法定義務

網絡安全的防範管理制度需要各相關機構的積極配合，為此，有必要對關鍵基礎設施的私人營運者及公共營運者制定有關的義務。

我們建議關鍵基礎設施營運者的義務按性質分四大類：

（1）組織方面的義務；

（2）程序、預防及應變方面的義務；

（3）自行檢測評估及報告義務；

（4）合作義務。

基於網絡經營者及公共實體的特定性質，以及其業務性質，我們建議對這兩類被監察實體予以特別規定，詳見下文 5.5 及 5.6。

5.1. 組織方面的義務

基於網絡安全的保密性及敏感性，“專人專責”和“信息到位”成為各關鍵基礎設施營運者組織架構必要考慮的因素，故此，我們建議關鍵基礎設施私人營運者在組織方面的義務如下：

（1）設置專責網絡安全管理單位及負責人，負責透過運用人力資源、財政資源、物資及財產資源，落實網絡安全的內部保護措施；

（2）對關鍵基礎設施營運者負責人及其關鍵職位的人員進行適當資格及專業經驗的背景審查，並為此必須向司法警察局徵求意見；

（3）建立涉及網絡安全的投訴和舉報的機制及渠道。

在背景審查方面，如該人被法院因下列任一犯罪，且有關的判決已確定，則視之為不具備擔任網絡安全負責人的職務或職位的適當資格：

（1）第 2/2009 號法律《維護國家安全法》所規定的犯罪；

（2）電腦犯罪或偽造技術註記罪、損壞或取去文件或技術註記罪、侵入私人生活罪、不當利用秘密罪、違反函件或電訊保密罪、或其他形式的違反保密罪；

（3）任何其他可處超逾五年徒刑的犯罪。

倘若處以超逾五年徒刑的犯罪的判決非由澳門特別行政區司法系統所宣示，則僅在有關的行為根據澳門特別行政區法律亦構成犯罪時，方產生上述的背景審查的法律效力。

5.2. 程序、預防及應變方面的義務

網絡安全的關鍵在於日常的資訊及網絡系統有效的管理制度、操作程序，以及預防和應急的措施。為落實此等制度、程序及措施，非得遵守相關義務不可。

所以，我們建議關鍵基礎設施營運者在程序、預防及監控網絡安全事故，以及作出應急方面的義務如下：

（1）制定網絡安全管理制度及內部操作程序；

（2）按照網絡安全管理制度、監察實體發出的傳閱文件及其他指示，落實內部的網絡安全保護、監測、預警及應急措施，尤其：a）防範網絡或該網絡內運行的數據遭受意外事故及未經許可的行為，包括進入、私自存取、增加、使用、修改、控制、入侵、干擾、洩漏、破壞或銷毀；b）監察和記錄網絡運行狀態，尤其按照規定儲存及適時提供該日誌；

（3）當發生網絡安全事故時，向網絡安全事故預警及應急中心作出通報，並告知相關的監察實體有關的事件以及同時展開應急工作。

5.3. 自行檢測評估及報告義務

為掌握網絡安全的落實情況以及檢查各方面的預防工作是否到位，我們建議關鍵基礎設施營運者在自行檢測評估及報告方面的義務如下：

（1）自行或委託專業機構對其網絡的安全性及可能存在的風險進行檢測評估；

（2）每年向其所屬的監察實體提供網絡安全報告，尤須提及網絡安全事

故(如曾發生網絡安全事故)、上項所指的檢測評估結果及已採取的改善措施。

5.4. 合作義務

網絡安全的預防及事故調查，由於網絡訊息瞬間即逝，要搜集有關的資料，須分秒必爭並與各方通力合作，故我們建議關鍵基礎設施營運者，以及其管理層、管理人員或獲授權人的義務如下：

（1）在審查程序性、預防性或應變性義務履行情況的必要範圍內，允許網絡安全事故預警及應急中心及監察實體指派的代表進入其設施，讓該等人員進入其辦公地點，並提供該等人員職務範圍內所要求的資訊；

（2）提供必要的支援及合作，以確保網絡安全的妥善管理。

5.5. 公共網絡經營者的特別義務

公共網絡經營者是具准照經營公用固定或流動電信網絡以及提供互聯網接入服務的實體，在網絡安全擔當非常重要的角色，所以，我們建議公共網絡經營者除了上述各項的義務外，尚須負有以下義務：

（1）“實名制”：公共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、公用固定或流動電訊服務時，須要求用戶提供真實身份資料；

（2）“日誌保存”：為用戶提供互聯網接入服務時，須將其所使用的互聯網地址與內聯網地址的轉換對應關係的日誌保存一年。

5.6 關鍵基礎設施的公共營運者的義務

關鍵基礎設施的公共營運者是指政府機關、部門和實體，其活動必然與公共利益有關，故同樣肩負提供關鍵服務的社會使命。

有鑑於此，關鍵基礎設施的公共營運者與私人營運者有同樣的義務，即須遵守程序、預防及應變方面的義務、自行檢測評估及報告義務以及合

作義務。關於組織方面的義務，基於公共部門須經深思熟慮後方予設立，而且已設有公共的投訴及建議機制，所以，僅需明確規定關鍵基礎設施的公共營運者應在領導層或等同職級的人員中，指定一名擔任網絡安全負責人職務，負責透過運用人力資源、財政資源、物資及財產資源，落實網絡安全內部保護措施。

6. 對不遵守義務的行政處罰和紀律責任

我們在本法律制度內建議不以刑事處罰，而僅以行政處罰追究不遵守網絡安全義務的責任，主要的理由有三方面：

（1）網絡安全制度在性質上屬於防範性行政管理制度；

（2）違反防範性規定的行為通常不以刑事方式處理，即不以犯罪論處；

（3）這種處理方式符合澳門特別行政區法律制度的其中一個總原則—“刑法最小介入原則”。

基於上述考慮，我們建議對於不遵守上述義務的行為，不論屬作為或不作為，在不妨礙其他法律或法規追究刑事責任的情況下，均構成行政違法行為，應科處罰款。輕微者，罰款澳門幣 5 萬元至 15 萬元。嚴重者，罰款澳門幣 15 萬元至 500 萬元。

對嚴重不遵守義務者，即不遵守有關義務可能導致較嚴重的損失或影響時，我們建議可單獨或合併科以附加處罰。附加處罰包括剝奪參與公共機關及實體購置物品或取得服務的公開招標的權利；剝奪取得公共機關及實體的津貼或利益的權利；中止有關許可、准照、批給合同或執照的部分或全部效力。

相反，在某些情節屬輕微的情況(當不遵守義務對網絡安全不構成實質危險，且非屬累犯的情況)，如違法者在當局指定的期間內能夠補正有關的不合規範情況，有關的罰則可減輕至僅對其處以警告。

關鍵基礎設施的私人營運者，原則上須對業務範圍內所犯的行政違法行為承擔機構的法律責任，無論該機構是否認為需要向行政違法行為所牽涉的人員作出追究、所牽涉的人員在機構內擔任何等職級，以及該違法人員與關鍵基礎設施營運機構之間的職務或工作關係為何。

關鍵基礎設施的公共營運者，如營運者負責人因故意或疏忽而不遵守網絡安全義務，須負起紀律責任。如涉及不遵守主要的網絡安全義務(即程

序性、預防性及應變性的義務)，其紀律處分一般不低於(10 日至 240 日的)停職，嚴重者以撤職論處。

7. 對生效日期的特別考慮

基於網絡安全法律制度是一個全新的制度，我們建議按慣常的立法方式，規定較充裕的待生效日期，亦即在法案公佈後三十日起生效。

然而，考慮到《網絡安全法》與現時公共網絡服務存在密切關係，為免對公共網絡經營者造成衝擊，我們建議對網絡經營者的兩項特定義務（“實名制”及“日誌保存”）另訂生效日期。此規定旨在讓經營者在“待生效期”內作出適當準備及適應，以盡量避免對市面正銷售的電話預付卡或網卡造成巨大衝擊，影響經營者的生意及其收益。

8. 細則性規定

基於第 13/2009 號法律《訂定內部規範的法律制度》賦予政府就其組織架構的內容有權以行政法規的形式予以規範，我們將以補充性行政法規規範“網絡安全常設委員會”和“網絡安全事故預警及應急中心”的職權和運作，以及指定負責監察的公共實體。

上述的規範模式亦具實務性，在必要時可對指定監察實體、其職權及運作作出更新及調整。

《網絡安全法》的立法建議和意見欄

發表意見者/建議者基本資料
發表意見者/建議者姓名或機構名稱：
來自關鍵基礎設施所涉及行業或其他行業服務(例如：電力供應)：
保密聲明：如希望將意見或建議保密，請在方格以✓符號標示： ----------☐
提交日期：

意見及建議所針對的諮詢內容章節	意見及建議
1. 建立網絡安全防護體系	
2.關鍵基礎設施和網絡安全的相關定義	
3. 網絡安全防護體系的適用對象	
3.1. 關鍵基礎設施的公共營運者	
3.2. 關鍵基礎設施的私人營運者	
4. 政府的監察實體	
4.1. “網絡安全常設委員會”	
4.2. “網絡安全事故預警及應急中心”	
4.3. 各領域的監察實體	
5. 法定義務	

5.1. 組織方面的義務	
5.2. 程序、預防及應變方面的義務	
5.3. 自行檢測評估及報告義務	
5.4. 合作義務	
5.5. 網絡經營者的特別義務	
5.6. 關鍵基礎設施的公共營運者的義務	
6. 對不遵守義務的行政處罰和紀律責任	
7. 對生效日期的特別考慮	
8. 細則性規定	
9. 非本諮詢文本所提及的其他網絡安全事宜	

注意：

- 為方便分析和整理，以上表格僅供提出意見及建議時參考之用。
- 如填寫空間不足，敬請按章節題目順序另行以補充頁填寫，並標示所屬章節及頁數。
- 敬請盡可能採用直接的表述方式，內容扼要。