《網絡安全法》

公開諮詢總結報告

澳門特別行政區政府

2018 年

意見來源

1. **業界**

按照諮詢文本定義，“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；“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

(1) **關鍵基礎設施的公共營運者**：包括公共機關、部門及實體

(2) **關鍵基礎設施的私人營運者**：包括法定屠場、受衛生檢疫及植物檢疫的食品批發經營者、銀行、財務實體及保險業機構、娛樂場幸運博彩經營者、燃油批發經營者、私營醫院、港口、海上運輸及供水服務經營者、陸上運輸經營者、電力和天然氣供應及分配經營者、污水處理和垃圾收集及處理經營者、航空運輸經營者、視聽廣播經營者、全公共資本公司、由法規定性為行政公益法人的私法人、公共網絡經營者

2. **公眾**

意見摘要及意見立場的歸納標準

1. **“意見摘要”**是根據收集所得的各條議題意見，歸納出關注熱點或具重要性的意見

2. **“贊成”**是指在意見原文中，就諮詢文本相應章節或子章節的內容明確地表示贊成，例如出現“贊成”、“贊同”、“認同”、“同意”等字句，或者綜合意見原文內容，可以歸納出意見者就諮詢文本相應章節或子章節的內容屬於贊成

3. **“不贊成”**是指在意見原文中，就相應章節或子章節的內容明確地表示不贊成，例如出現“不贊成”、“反對”、“不同意”、“不應該這樣做”等字句，或者綜合意見原文內容，可以歸納出意見者就諮詢文本相應章節或子章節的內容屬於不贊成

4. **“其他”**是指就諮詢文本相應章節或子章節的內容，意見原文提出了其他意見或建議，但對諮詢文本的內容卻沒有表示任何贊成或不贊成立場

5. **“無效”**是指就諮詢文本相應章節或子章節的內容為侮辱性字句及不雅用語，或不能被理解(例如僅表述為符號、亂碼字符、不相關的文詩詞等等)

各章節小結及總結部分中，關於對議題之**“立場”**，僅透過計算“贊成”及“不贊成”比例得出意見者是否**普遍贊成**或**普遍不贊成**

《網絡安全法》公開諮詢總結報告

目錄

前言

《網絡安全法》是構建本澳網絡安全體系的法律依據，明確本澳“關鍵基礎設施”的營運者和社會各相關方面就網絡安全應該負有的義務和責任，並在行政管理層面上落實各項網絡安全工作，包括風險評估、預警、防範、監管以及其他應對工作等等，從而構建一個有效的網絡安全防範管理體系，提升澳門防範和應對網絡安全的能力，更好地維護澳門以至國家的安全。

澳門特別行政區政府就制訂《網絡安全法》，於 2017 年 12 月 11 日至 2018 年 1 月 24 日展開為期 45 日的公開諮詢，期間社會各界就進一步完善相關法律草案、共同籌劃既符合市民意願、又符合澳門現實發展需要的網絡安全體系，進行了廣泛的討論，旨在凝聚社會共識，為建立澳門的網絡安全體系奠定穩固的法制基礎。

是次公開諮詢由保安司司長辦公室負責統籌，並與行政公職局、經濟局、海事及水務局、交通事務局、能源業發展辦公室、環境保護局、民航局、金融管理局、博彩監察協調局、民政總署、衛生局、郵電局及司法警察局共 13 個公共部門、機關及實體攜手推展，亦得到了個人資料保護辦公室積極提供意見及參與公開諮詢的講解會。法律改革諮詢委員會及法務局在法案草擬過程中先後就法案政策性問題及法律問題等進行了討論及提供了意見。

諮詢活動結束後，上述 14 個公共部門、機關及實體隨即全面整理諮詢期間從不同渠道收集所得的意見和建議，並編撰成本諮詢總結報告。

總結報告共分為四部分：第一部分是諮詢工作的總體情況；第二部分是諮詢文本反饋意見的摘要、分析與小結；第三部分是諮詢文本內容以外的意見和建議；第四部分是總結。

第一部分

諮詢工作的總體情況

在諮詢期內，澳門特別行政區政府透過新聞發佈、業界及公眾諮詢會、專題網頁、媒體廣告、社交網絡平台、諮詢文本及小冊子等多種宣傳方式，向社會各界介紹《網絡安全法》的立法內容，積極收集業界及廣大市民的意見，並根據諮詢期間所收集的意見，對有關內容進行分析，集思廣益，藉此完善法案內容。

1. 派發諮詢文本

《網絡安全法》諮詢期間共派發了 2,400 份諮詢文本及 2,700 份小冊子，派發地點分別有保安司司長辦公室、行政公職局、法務局、司法警察局、政府資訊中心、政府綜合服務大樓、中區市民服務中心及離島市民服務中心。諮詢文本亦上載至保安司司長辦公室專題網頁（www.gss.gov.mo/ch/ciberseg），方便市民查閱。

2. 通過媒體宣傳

為使社會各界清楚瞭解《網絡安全法》的立法目的及立法內容，是次諮詢除設有專題網頁外，亦製作了宣傳短片、聲音廣告及簡明易懂的圖文包，涉及是次公開諮詢內容的簡介、“網絡安全法－社會安全的保障”、網絡安全管理、網絡安全的義務及責任四個方面，透過電視台、電台、巴士車廂內播放以作廣泛宣傳，並充分利用 Facebook、Wechat 等新媒體平台向社會發放諮詢活動的訊息。

諮詢期內，保安司司長辦公室共發放了七份新聞稿，讓公眾及時知悉有關諮詢動態。同時，相關政府部門亦密切留意各類媒體，包括傳統媒體、網絡平台及社交媒體關於《網絡安全法》諮詢的報導和評論，留意輿情動態。

政府代表亦出席不同媒體的時事評論節目，就《網絡安全法》與市民作直接交流，包括於 2017 年 12 月 15 日出席蓮花衛視“澳門開講”、12 月 19 日出席澳廣視“澳門論壇”以及於 2018 年 1 月 17 日出席澳門電台“澳門講場”。

3. 舉辦多場諮詢會

公開諮詢期間共舉行了八場諮詢會，當中五場面向公共部門及經營關鍵基礎設施的業界代表，三場面向全澳市民。諮詢會獲得各界的踴躍參與，合共約 600 人出席，同時收到不少市民及相關業界的寶貴意見，對優化法案的內容具有積極意義。

諮詢會	日期	對象
業界諮詢專場	2017 年 12 月 11 日	公共部門、機關及實體
	2017 年 12 月 13 日	燃油批發經營者，港口、海上運輸及供水服務經營者，陸上運輸經營者，航空運輸經營者，電力和天然氣供應及分配經營者，污水處理和垃圾收集及處理經營者
	2017 年 12 月 14 日	銀行、財務實體及保險業機構
	2017 年 12 月 15 日	娛樂場幸運博彩經營者
	2018 年 1 月 3 日	法定屠場、受衛生檢疫及植物檢疫的食品批發經營者，私營醫院，視聽廣播經營者，公共網絡經營者，全公共資本公司、由法規定性為行政公益法人的私法人
公眾諮詢專場	2018 年 1 月 5 日	公眾、傳媒
	2018 年 1 月 13 日	公眾、傳媒
	2018 年 1 月 15 日	公眾、傳媒

4. 推出常見問題集

為使社會各界準確地掌握《網絡安全法》的立法意向，保安司司長辦公室根據諮詢會參與者的提問內容，以及社會輿論就《網絡安全法》所提出的疑問或意見，在諮詢期間推出常見問題集，並不斷更新及進行補充。問題集除上載到專題網頁外，亦透過微信平台“網安知多啲”欄目向市民推送有關資訊，以釋除公眾疑慮。

5. 意見收集工作

公開諮詢期間，按諮詢文本第 13 頁“網絡安全管理架構”所列的監察實體邀請了相關的關鍵基礎設施營運者就諮詢文本內容以書面形式發表意見。諮詢期內，共收到 144 份由公共部門及被監察實體—關鍵基礎設施的私人營運者正式提交的書面意見；另於五場業界諮詢專場中，共有 43 人次發表意見。

另外，諮詢期間亦收到公眾以書面形式發表或直接透過專題網頁所設的意見欄填寫的 31 份書面意見以及 449 份電子意見，並有 49 人次於 3 場公眾諮詢會中發表了意見。

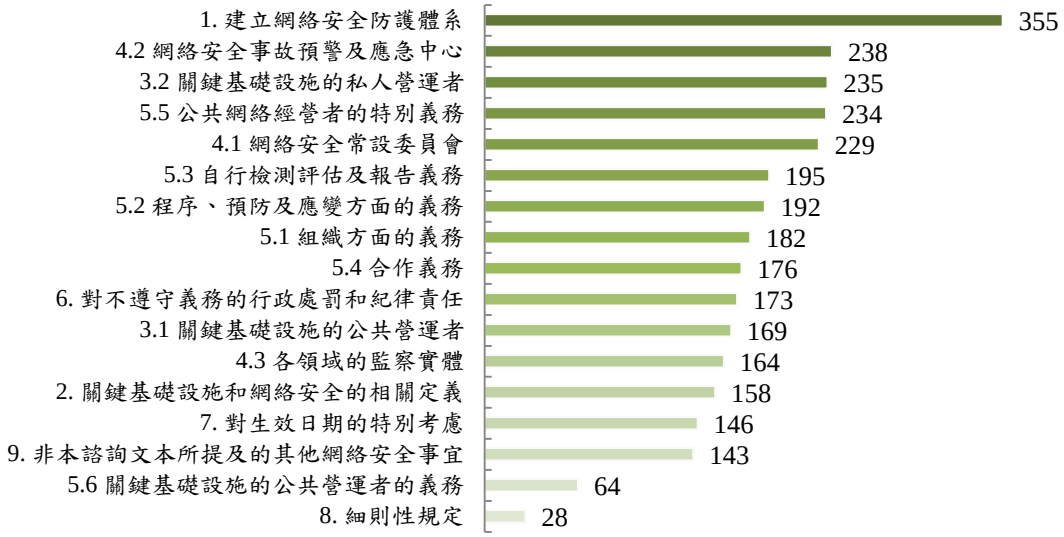
<table>
<tr><th colspan="2">意見來源</th><th>收集渠道</th><th colspan="3">意見數量(份數)</th><th>總數</th></tr>
<tr><td rowspan="4">業界</td><td rowspan="2">公共部門</td><td>書面報告</td><td>36</td><td rowspan="2">38</td><td rowspan="4">187</td><td rowspan="7">716</td></tr>
<tr><td>諮詢會</td><td>2</td></tr>
<tr><td rowspan="2">被監察實體—關鍵基礎設施的私人營運者</td><td>書面報告</td><td>108</td><td rowspan="2">149</td></tr>
<tr><td>諮詢會</td><td>41</td></tr>
<tr><td colspan="2" rowspan="3">公眾</td><td>書面報告</td><td>31</td><td colspan="2" rowspan="3">529</td></tr>
<tr><td>專題網頁</td><td>449</td></tr>
<tr><td>諮詢會</td><td>49</td></tr>
</table>

從不同渠道收集所得的 716 份[1]意見中，按具體討論章節可以整理出 3,081 條議題意見，關注的議題主要包括建立網絡安全防護體系（立法取向）、網絡安全防護體系的適用對象（尤其是關鍵基礎設施的私人營運者的定義範圍）、“網絡安全常設委員會”和“網絡安全事故預警及應急中心”的組成與職能，以及公共網絡經營者的特別義務（包括實名制及日誌保存義務）等內容。

[1] 按意見立場的歸納標準，716 份意見中有一份公眾意見屬於“無效”。

關注的議題分佈

各章節議題	意見數量	各渠道收集所得的意見數量		
		書面報告	專題網頁	諮詢會
1. 建立網絡安全防護體系	355	65	259	31
2. 關鍵基礎設施和網絡安全的相關定義	158	48	104	6
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	169	34	134	1
3.2 關鍵基礎設施的私人營運者	235	51	179	5
4. 政府的監察實體	---	---	---	---
4.1 “網絡安全常設委員會”	229	36	185	8
4.2 “網絡安全事故預警及應急中心”	238	56	175	7
4.3 各領域的監察實體	164	40	114	10
5. 法定義務	---	---	---	---
5.1 組織方面的義務	182	103	66	13
5.2 程序、預防及應變方面的義務	192	74	108	10
5.3 自行檢測評估及報告義務	195	87	98	10
5.4 合作義務	176	57	113	6
5.5 公共網絡經營者的特別義務	234	70	140	24
5.6 關鍵基礎設施的公共營運者的義務	64	31	30	3
6. 對不遵守義務的行政處罰和紀律責任	173	66	106	1
7. 對生效日期的特別考慮	146	60	85	1
8. 細則性規定	28	20	8	0
9. 非本諮詢文本所提及的其他網絡安全事宜	143	32	96	15
議題意見總數：	3,081	930	2,000	151

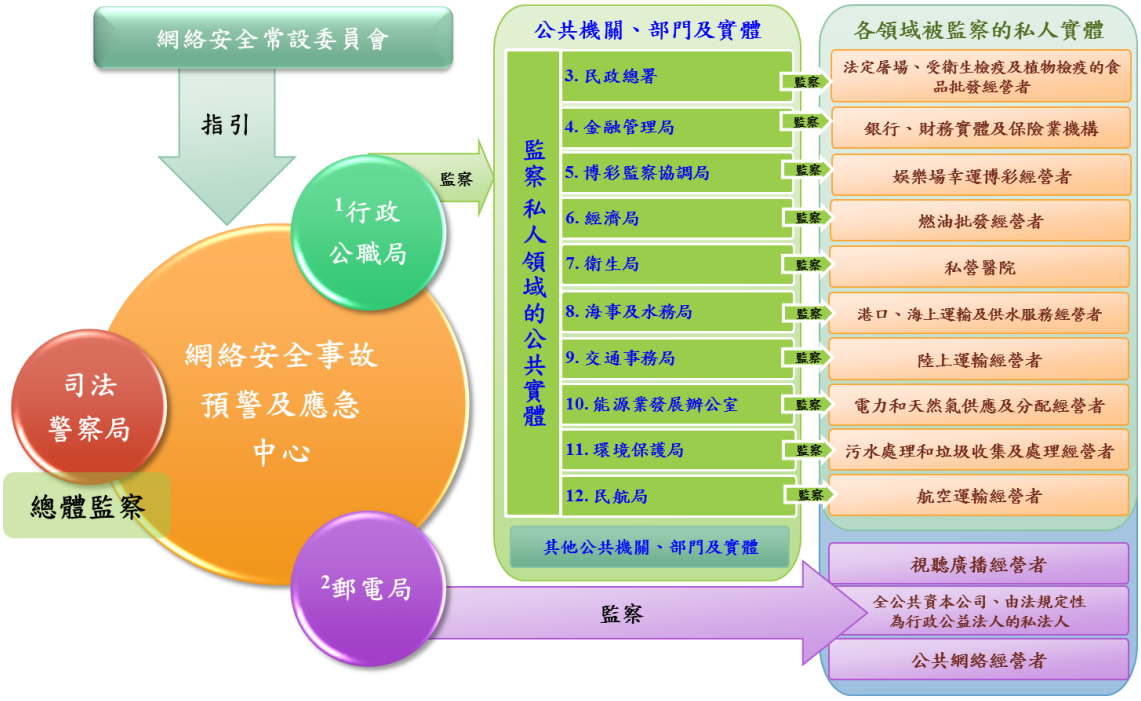


第二部分

諮詢文本反饋意見的摘要、分析與小結

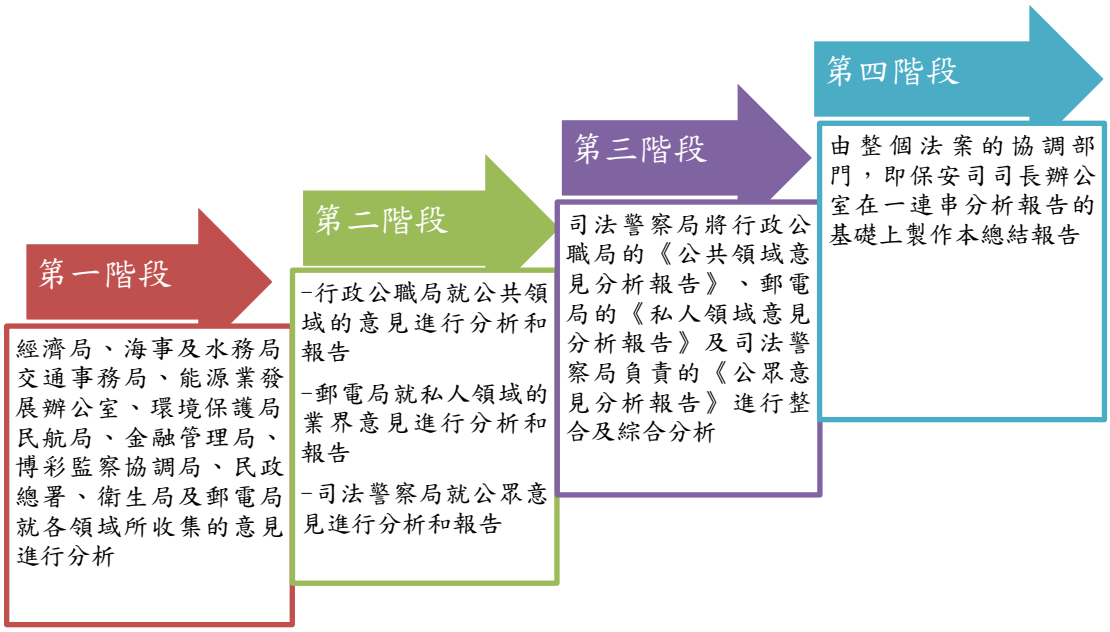
基於《網絡安全法》的社會覆蓋面廣泛，涉及 12 個關鍵基礎設施的業務領域及相關的監察實體，為求意見分析到位和適切考慮各領域業務的實際情況，按公開諮詢的推展計劃及安排，意見分析的工作分四個階段進行，詳見以下示意圖。

網絡安全管理架構



（參閱諮詢文本第 13 頁“網絡安全管理架構”）

意見分析的工作流程

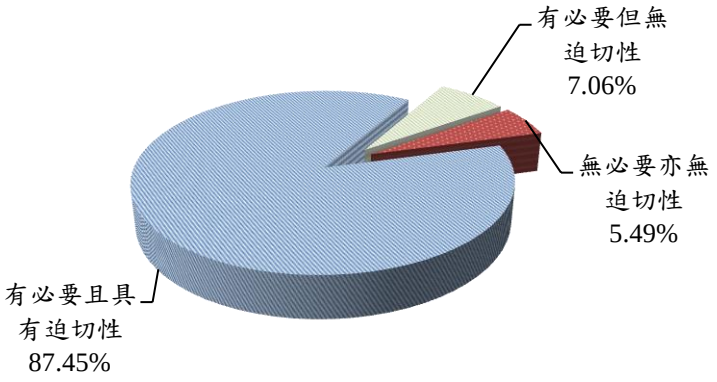


1. 建立網絡安全防護體系

諮詢文本指出，澳門特別行政區需要構建網絡安全防護性行政管理體系，訂明關鍵基礎設施營運者的義務和責任，《網絡安全法》是一部以“守護”、“防範”及“管理”為主的法律。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。

對此有 241 份意見認為有必要建立網絡安全防護體系，有 14 份意見認為並無必要建立網絡安全防護體系；亦有 100 份來自業界及公眾的意見，就日後本澳建立網絡安全體系及制定相關規範指引提出多項建議。

意見	有必要且具有迫切性		有必要但無迫切性		無必要亦無迫切性	
	業界	公眾	業界	公眾	業界	公眾
數量	21	202	7	11	0	14
百分比	87.45%		7.06%		5.49%	



■ **意見摘要**

業界代表普遍認為網絡安全對業界資訊系統安全和正常運作非常重要，社會各階層使用資訊科技的普及程度日益提高，網絡攻擊於全球時有發生，建立網絡安全防護體系有助本澳防範及應對網絡安全事故，保障市民的合法權益。

市民普遍贊成本澳建立網絡安全防護體系，其中有意見認為隨着本澳發展成為智慧城市、普及電子支付，建立網絡安全防護體系有助本澳防範因受到網絡攻擊而影響社會的運作，贊同政府儘快完善相關法律保障市民，尤其是對個人信息容易外洩等問題必須正視。

少部分不贊成設立網絡安全防護體系的意見（共 14 份）均來源於公眾，認為本澳目前已有《打擊電腦犯罪法》對抗黑客攻擊，擔心政府會藉着《網絡安全法》立法使網絡監控合法化，侵害市民的言論自由、通訊保密等權利。

分析與回應

《網絡安全法》的立法原意旨在遵照“保障市民安全、尊重個人隱私”的原則下，為澳門社會的關鍵基礎設施構建一個良好的防範管理體系，防範及減少網絡攻擊對本澳社會的影響。

《網絡安全法》的內容屬於事前預防措施，針對關鍵基礎設施的網絡安全作出防範性管理，並非侵害市民言論自由、個人隱私或干預新聞自由等個人基本權利，而現行《打擊電腦犯罪法》是針對電腦及網絡犯罪行為的刑事法律，屬於事後的刑事偵查措施，所有介入通訊內容的刑事偵查措施，須嚴格按照《澳門基本法》第三十二條及《刑事訴訟法典》第一百六十四條等規定執行。

■ **意見摘要**

有市民建議政府在構建本澳的網絡安全防護體系時，可以參考其他先進國家及地區的相關制度及立法經驗。

分析與回應

在制訂諮詢文本中所建議的網絡安全總體框架過程中，相關部門已作出比較法的研究及充分參考了中國內地以及其他國家或地區的相關法律度，並對實際情況作考量。將來在法律生效後，政府會保持關注世界各地網絡安全防護工作的最新發展情況，並適時作出檢討及更新，以適應資訊科技的高速發展及網絡安全環境的急劇變化。

小結

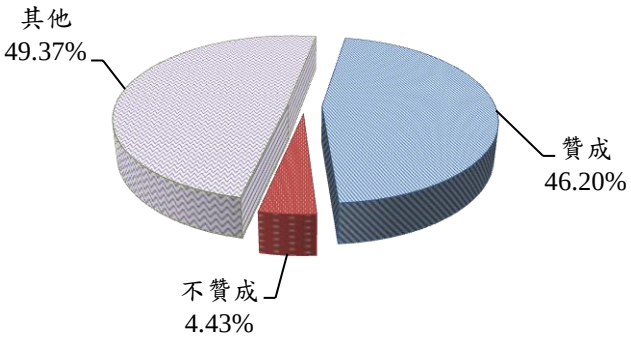
超過87%的意見認為建立網絡安全防護體系屬有必要且具有迫切性，業界與公眾均指出網絡安全是公共安全及個人安全的前提及保障，為確保網絡運作良好、網絡數據保密及完整，澳門特別行政區有必要透過立法，構建良好的防範性管理體系。

2. 關鍵基礎設施和網絡安全的相關定義

諮詢文本建議對《網絡安全法》所涉及的重要概念作出定義，包括“關鍵基礎設施”、“關鍵基礎設施營運者”、“網絡”、“網絡數據”、“網絡安全”及“網絡安全事故”。

對此贊成意見為73份，不贊成意見為7份；有78份意見就諮詢文本中未被定義的內容提出相關具體建議。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	27	46	0	7	78
百分比	46.2%		4.43%		49.37%



■ **意見摘要**

有業界及公眾建議細化各項定義，並透過清晰定義以確立出《網絡安全法》的監管範圍。

分析與回應

經分析所收集的意見，政府將對諮詢文本內部分定義作出調整與修改，包括對“網絡安全”、“網絡安全事故”重新定義，並加入“未經許可的行為”，從而有助釐定“網絡安全”的範圍。

■ **意見摘要**

對於諮詢文本內未被定義的內容（如電子錢幣），業界及公眾建議進行定義及監管。

分析與回應

對於諮詢文本內未被定義的內容，倘屬現行其他法律有相關規定的情況，則無需要及不適宜於《網絡安全法》中重複有關規定。值得指出的是，由於《網絡安全法》為一部涵蓋多個領域的行政管理法律，應具備廣泛的適用性，因此並不適宜於法律條文中分別對某一個別項目內容進行定義及監管。

小結

業界及公眾普遍對“關鍵基礎設施和網絡安全的相關定義”表示贊成，其他意見約佔 50%，主要是建議政府就其他內容再作定義。

經分析有關意見後，政府將適當地修改及調整諮詢文本內部分定義，使其更為清晰明確，以釋除業界及市民的疑惑，亦對將來法案執行提供更穩健的基石。

3. 網絡安全防護體系的適用對象（關鍵基礎設施營運者）

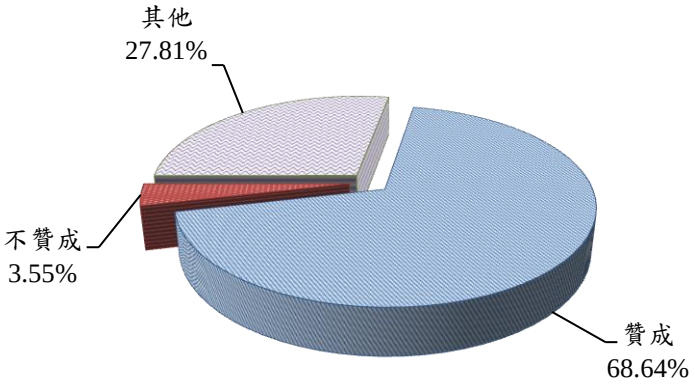
網絡安全防護體系的適用對象為“關鍵基礎設施營運者”，分為公、私兩大領域。“關鍵基礎設施營運者”對“關鍵基礎設施”的網絡安全須負起一定責任，其角色尤其重要。

3.1 關鍵基礎設施的公共營運者—公共機關、部門及實體

諮詢文本建議關鍵基礎設施的公共營運者涵蓋所有公共機關、部門及實體。

就“關鍵基礎設施的公共營運者”的適用範圍，贊成意見為 116 份，不贊成意見為 6 份；有 47 份意見對此部分適用範圍的納入標準進行討論及提出其他建議。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	20	96	0	6	47
百分比	68.64%		3.55%		27.81%



■ **意見摘要**

有公共領域代表建議應就其他部門或機關負責本部門網絡系統及網絡安全的情況作出規範或提供指引。

分析與回應

由於《網絡安全法》規範網絡系統管理者，因此當某一公共部門或機關的網絡系統由另一公共部門或機關提供、支援及維護保養，則系統管理的責任以及網絡安全的管理義務實際上由後者所承擔及履行。為清晰有關的規定，建議在法案明確以上情況會排除於《網絡安全法》的適用範圍。

■ **意見摘要**

有公眾意見建議將適用範圍擴展至全部受特區政府資助的機構。

分析與回應

《網絡安全法》的適用對象是關鍵基礎設施營運者。根據有關納入標準，由於該等受政府資助的機構的業務不一定涉及關鍵基礎設施的運作，故並不適宜將適用範圍擴展至全部受特區政府資助的機構。

小結

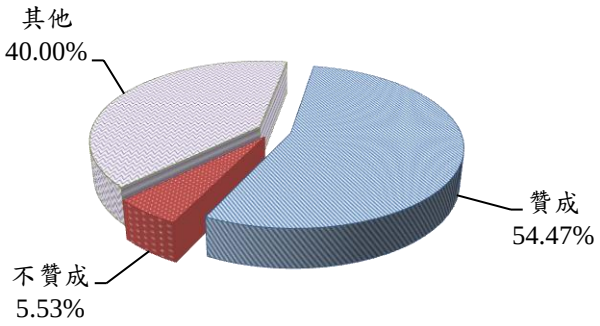
絕大部分意見對關於“關鍵基礎設施的公共營運者”的適用範圍表示贊成。政府經分析有關意見後，將明晰不適用及豁免適用《網絡安全法》的相關規定，以回應業界及公眾的疑慮。

3.2 關鍵基礎設施的私人營運者

現時很多重要的公共服務趨於“私營化”運作，私人機構與公共部門同為現代社會公共服務的提供者，故諮詢文本建議將一系列與關鍵基礎設施業務有密切聯繫的 11 個領域的私人實體定為“關鍵基礎設施的私人營運者”。

就“關鍵基礎設施的私人營運者”的適用範圍，贊成意見為 128 份，不贊成意見為 13 份；有 94 份意見對有關適用範圍的標準提出不同理解，亦有部分意見對於特定行業是否被納入關鍵基礎設施私人營運者的適用範圍提出討論。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	27	101	1	12	94
百分比	54.47%		5.53%		40%



■ **意見摘要**

對於關鍵基礎設施的私人營運者的範圍，有業界代表建議擴展至各行業、民間社團，並修改文本中“全公共資本公司”為“政府機關直接或間接持有 50%以上之法人”；有公眾意見提出應將收集及保存大量個人資料的中小企(如石油氣公司)、學校、私家診所等納入該適用範圍。

分析與回應

考慮到即使各行業、民間社團、醫療診所、高等院校、中小學或“政府機關直接或間接持有 50%以上之法人”等機構遭受網絡攻擊，亦未必對本澳整體社會的運作產生災難性的衝擊，同時，大部分機構亦未必具備足夠資源能夠完全滿足《網絡安全法》中所規定的義務要求，雖然該等機構可能保存大量個人資料，但現行的《個人資料保護法》已經相應作出規範，故不建議將上述機構納入被監察實體。另外，《網絡安全法》生效後，政府將適時對有關適用範圍進行檢討。

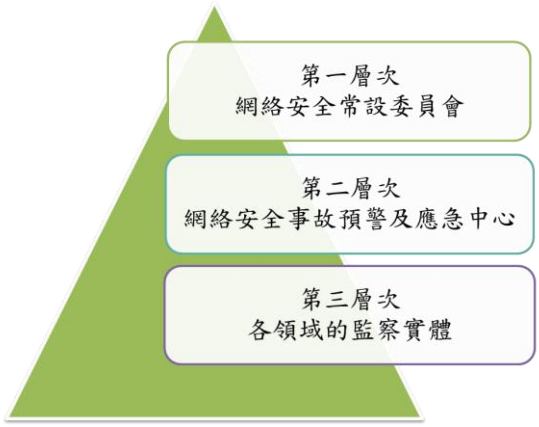
小結

業界和公眾意見對“關於基礎設施的私人營運者”的適用範圍普遍表示贊成，對此部分持不贊成立場意見共有 13 份，主要來自於公眾，他們憂慮監管網絡安全活動會影響個人隱私及言論自由，或者直接不贊成本澳就網絡安全防護體系進行立法。

為此，政府在法律生效後將加強普法宣傳，讓市民明白《網絡安全法》的實施並不會影響個人隱私或言論自由。

4. 政府的監察實體

諮詢文本中建議有關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”。

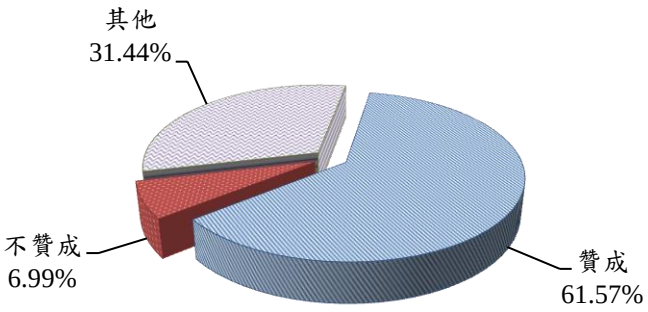


4.1 “網絡安全常設委員會”

諮詢文本中建議設立“網絡安全常設委員會”作為網絡安全的頂層決策機關，負責監察整個特區的網絡安全，並制定網絡安全總體方向、目的及策略。

就“網絡安全常設委員會”的設立及組成，贊成意見為 141 份，不贊成意見為 16 份；有 72 份意見對常設委員會的性質及其成員身份提出建議。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	17	124	0	16	72
百分比	61.57%		6.99%		31.44%



■ **意見摘要**

業界及公眾均建議加入不同領域的代表及專家作為“網絡安全常設委員會”成員，包括網絡安全範疇的專家、資訊業界的立法會議員、相關學術機構代表、法律人士、民間團體代表等。

分析與回應

在規範“網絡安全常設委員會”的補充性行政法規內將規定常設委員會主席可邀請其他公共及私人實體，或對工作有利的其他人士參與委員會的會議或工作，以便常設委員會在履行商討網絡安全政策及法規等職責時，可聽取更多專業及技術性意見。

小結

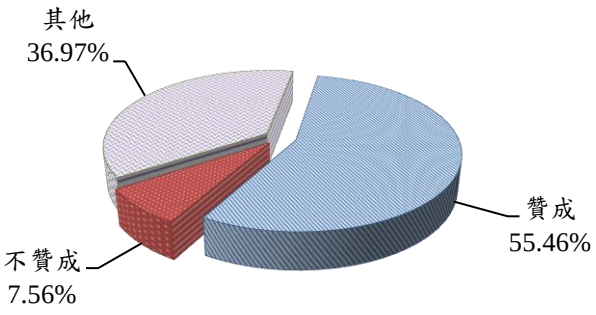
業界和公眾意見對“網絡安全常設委員會”的設立及組成普遍表示贊成，有16 份公眾意見表示不贊成，主要是由於意見者對委員會的組成存有不同理解，或不贊成為構建本澳網絡安全防護體系進行立法，故此不贊成進行相關的規定。

4.2 “網絡安全事故預警及應急中心”

諮詢文本建議設立“網絡安全事故預警及應急中心”作為落實網絡安全防範工作的核心組織，負責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，並於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。

就“網絡安全事故預警及應急中心”的設立及組成，贊成意見為 132 份，不贊成意見為 18 份；有 88 份意見對“中心”的具體運作及其職能，以及“中心”、監察實體和被監察實體之間的義務關係提出建議。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	22	110	0	18	88
百分比	55.46%		7.56%		36.97%



■ **意見摘要**

業界意見集中於關注“網絡安全事故預警及應急中心”進行網絡數據監察（包括作出監察的標準、進行監察時的具體方式、層面與程度），以及“中心”與被監察實體的合作方面的內容，並提出多項具體建議，亦指出應予明確指引規定。

分析與回應

“網絡安全事故預警及應急中心”只會對網絡數據的流量大小及特徵碼進行監察，其目的僅限於協助發現可能與網絡攻擊有關的惡意數據。而《網絡安全法》正式公佈後，政府將與業界合作共同制定有關規範的指引，並適時提供技術指引及適當培訓。

■ **意見摘要**

業界及公眾對網安事故通報機制、發佈和接收網安資訊的渠道、網安培訓及宣傳方面提出多項具體建議，例如建議與外地建立網絡安全通報合作機制、增設 24 小時熱線、舉辦網絡安全事故應急演習等。

分析與回應

“網絡安全事故預警及應急中心”成立後，政府將會依據法定職責與外地建立網絡安全的通報合作機制，並透過不同渠道發放及接收與網絡安全相關的重要資訊，以整體提高社會對網絡安全防護的意識及能力。此外，政府計劃透過多方面渠道，如網上表格、電子郵件等方式，接收網絡安全方面的查詢、舉報及投訴等，並作出適當跟進。另外，“中心”將定期進行網絡安全事故通報及應急演習，加強各參與者對網絡安全事故的應變協調能力。

■ **意見摘要**

部分公眾就“網絡安全事故預警及應急中心”對有關網絡數據流量及特徵碼進行監察方面持不贊成意見，認為會損害個人隱私、言論自由、出版自由或商業機密。

分析與回應

“網絡安全事故預警及應急中心”進行相關監察時只是流水式檢測數據流量及數據包特徵，不會對經檢測的數據流量作任何保留，亦不會記錄任

何資料，更不會對網絡內容或言論進行解碼。故此，監察實體人員不能直接或透過還原數據包技術獲取到個人資料、行業資訊或通訊內容，否則監察人員須承擔第 8/2005 號法律《個人資料保護法》、第 11/2009 號《打擊電腦犯罪法》及《刑法典》的刑事責任及行政違法的責任，並同時須承擔公職法律制度對公務人員所規定的紀律責任，以及在符合《民法典》規定的情況下，須承擔該法典所規定的民事責任。

另外，現行法律制度已訂明相關的行政及司法申訴途徑以確保行政當局行政活動的合法性，與此同時，《網絡安全法》的諮詢文本內容亦設置了不同層級的監察機制，旨在保證網絡安全的各項監察活動不損害個人資料，以及不侵犯言論自由及新聞自由。

小結

業界和公眾意見對關於“網絡安全事故預警及應急中心”的設立及組成普遍表示贊成，表示不贊成立場的意見全部來自公眾，主要原因是他們擔憂“中心”的監察活動對個人隱私、言論自由等權利造成損害。

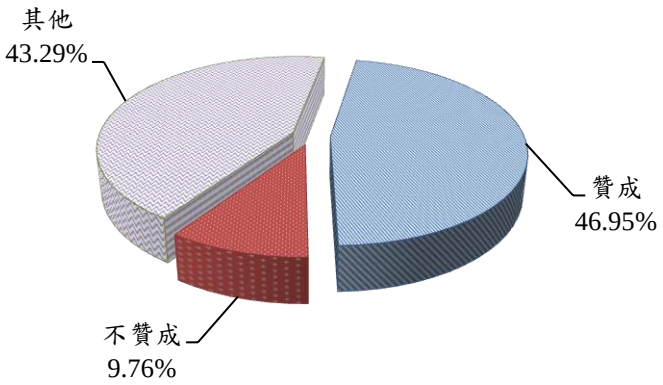
故此，政府會加強有關宣傳工作，讓社會各界瞭解“網絡安全事故預警及應急中心”的運作模式，其監察活動並不會影響個人隱私或言論自由。

4.3 各領域的監察實體

根據諮詢文本，建議監察系統的第三層次—**“各領域的監察實體”**分為兩個方面：由行政公職局負責監察公共機關及實體，以及由 11 個公共部門分工負責監察相應私人領域的關鍵基礎領域營運者。

就“各領域的監察實體”的組成，贊成意見為 77 份，不贊成意見為 16 份；有 71 份意見包括對“各領域的監察實體”的適用對象、監管關係的釐定等進行討論及提出其他建議。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	20	57	0	16	71
百分比	46.95%		9.76%		43.29%



■ **意見摘要**

業界及公眾均認為應由單一組織作為主要監察實體以提高監察效率，並建議統一制定網絡安全管理標準。

分析與回應

《網絡安全法》的立法目的是構建一個完整的網絡安全防護體系，由全社會和所有公共部門來共同維護網絡安全，故此，網絡安全必須依靠全社會、所有公共部門和關鍵基礎設施的共同推動和執行，而且每類關鍵基礎設施均有其獨特性，透過該領域的專責部門進行監察較為合適。

■ **意見摘要**

有意見擔憂各領域的監察實體沒有足夠技術能力對被監察實體的網絡安全情況進行監察。

分析與回應

“網絡安全事故預警及應急中心”將協調各參與實體之間的合作及適當行動，並且向各個監察實體提供其所需的技術指引，以協助其應對技術上問題、確保其能夠切實履行職務。

■ **意見摘要**

有意見質疑監察實體會以審查被監察實體的義務履行情況為由，要求被監察實體交出涉密資料，甚至損害言論或新聞自由。

分析與回應

監察實體人員僅在關鍵基礎設施營運機構的網絡遭受諸如入侵或襲擊時，方可前往該等機構的設施了解實情。即使在檢視過程中，監察實體人員要求取得數據，亦不得藉此提取關鍵基礎設施營運者的業務營運數據、客戶個人資料等涉密資訊，因個人資料及通訊內容不屬監察人員有權查閱及提取的數據範圍，僅在被監察實體明示同意或法官基於刑事偵查程序的需要而根據《刑事訴訟法典》規定允許下，方可被查閱或提取，否則監察人員須承擔第 8/2005 號法律《個人資料保護法》、第 11/2009 號《打擊電腦犯罪法》及《刑法典》的刑事責任及行政違法的責任，並同時須承擔公職法律制度對公務人員所規定的紀律責任。如果前提要件成立，更須承擔民事責任。

另外，“網絡安全常設委員會”除負責訂定本澳整體的網絡安全政策外，亦負責監察整個網絡安全監察架構的日常運作，包括對“網絡安全事故預警及應急中心”及各領域的監察實體的工作的監察。如果被監察的關鍵基礎設施營運機構或任何人懷疑網絡安全監察實體行使公權力的行為違法或不公，法律已規範相關申訴途徑，而《網絡安全法》亦會訂出一套不同層級的監察機制，保證網絡安全的各項監察活動不損害個人資料，以及不侵犯言論自由及新聞自由。

小結

業界意見對“各領域的監察實體”的組成全部表示贊成，部分公眾持不贊成意見，主要由於他們對監察實體在監察網絡安全方面的技術能力，以及監察活動對言論或新聞自由的影響存有疑問。

5. 法定義務

諮詢文本指出，網絡安全的防範管理制度需要各相關機構的積極配合，故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。

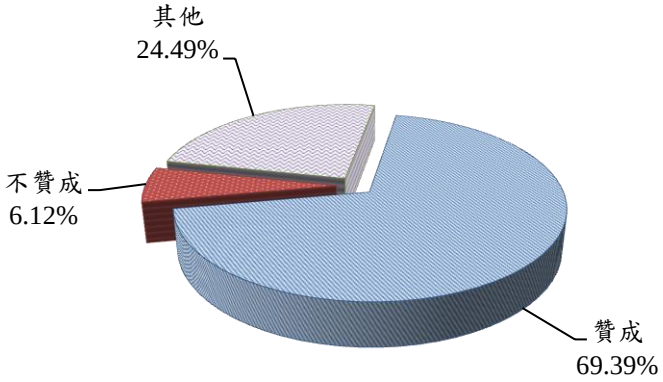
5.1 組織方面的義務

諮詢文本建議關鍵基礎設施私人營運者需要設置專責網絡安全管理的單位及負責人，對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，並建立涉及網絡安全的投訴和舉報的機制及渠道。

就“組織方面的義務”，對“設置專責網絡安全單位及負責人”有 68 份贊成意見，6 份不贊成意見；對“網絡安全負責人及關鍵職位的人員進行背景審查”有 56 份贊成意見，7 份不贊成意見。另外，有 45 份意見對網絡安全負責人的資格、責任和背景審查流程提出建議。

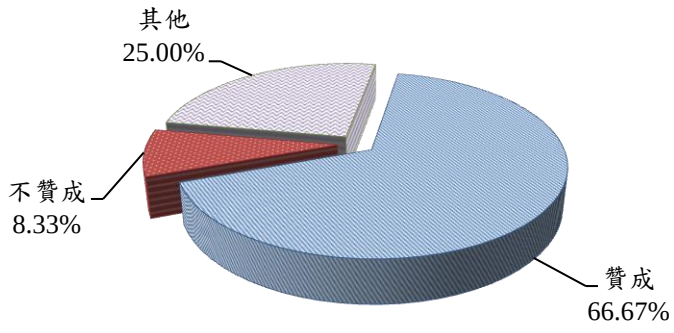
設置專責網絡安全單位及負責人

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	38	30	1	5	24
百分比	69.39%		6.12%		24.49%



網絡安全負責人及關鍵職位的人員進行背景審查

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	31	25	1	6	21
百分比	66.67%		8.33%		25%



■ **意見摘要**

業界主要對網絡安全負責人員的擔任資格、專業經驗、居住地身份以及是否能夠外判等方面作出提問。

分析與回應

網絡安全負責人的角色主要為管理者而非執行者，政府並沒有為網絡安全負責人專業經驗訂定特定要求，僅在適當資格上要求必須就有關人員的犯罪記錄透過司法警察局提供的協助進行背景審查。

諮詢文本中沒有規範網絡安全負責人由澳門居民或非澳門居民擔任，為確保負責人的溝通及中介角色，法案將要求網絡安全主要負責人應該在澳門特別行政區有慣常居所，以便網絡安全事故預警及應急中心可以在任何時候聯絡該負責人；該負責人出缺或不能視事時，亦須確保有另一名具備資格且熟悉有關系統的代表在本澳候命。如非澳門居民擔任網絡安全負責人職位，其必須按照在澳門法律規定，符合出入境逗留法律的相關規定及依法受聘，並需要出示外地的刑事紀錄資料，以便政府進行審查工作。

此外，為清晰網絡安全工作外判的情況，法案將有所補充，確保關鍵基礎設施營運者不會因外判安排而降低和減輕須遵從的義務及須承擔的責任，以防止出現規避法律責任的情況。

■ **意見摘要**

就諮詢文本中背景審查方面的適當資格要求，有市民建議禁止所有曾因刑事罪行（不論該罪行可處徒刑的年期）被作出有罪判決的人士擔任有關職務。

分析與回應

諮詢文本建議某些犯罪紀錄的人不可被聘為網絡安全負責人，旨在限制曾觸犯與網絡安全負責人職務要求有抵觸的犯罪行為，或曾經觸犯嚴重罪行的人士出任該職務，至於其他犯罪紀錄的人士，則由有關的營運機構自行衡量是否適合聘用其擔任網絡安全負責人的職位。

■ **意見摘要**

業界希望了解諮詢文本所指的“涉及網絡安全的投訴和舉報的機制及渠道”，是否要求每日 24 小時無間斷運作，而所有投訴和舉報事故是否必須備案及須向哪個實體作出通報。

分析與回應

政府在《網絡安全法》公佈實施後，將透過業界指引，進一步明確私人營運者的義務中有關建立“涉及網絡安全的投訴和舉報的機制及渠道”的具體要求及指引。

■ **意見摘要**

有意見者擔心當企業發生網絡安全事故時，網絡安全負責人需要為企業承擔全部責任。

分析與回應

《網絡安全法》是以關鍵基礎設施營運者為適用對象，不遵守或違反網絡安全方面的義務所引致的法律責任由該等機構負責，即使機構認為是由於某員工的過失而引致其違反《網絡安全法》所規定的義務，該機構仍須負起相關的法律責任。

小結

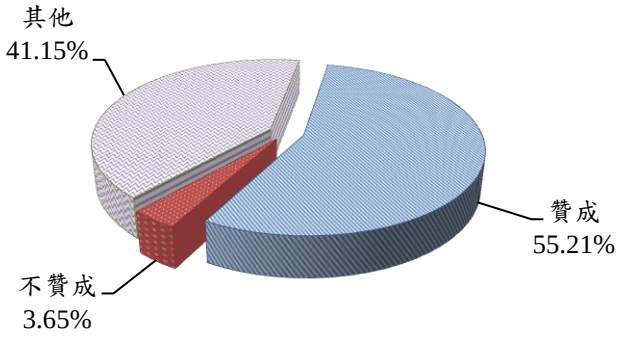
業界和公眾普遍贊成設置專責網絡安全單位及負責人，並對網絡安全負責人及關鍵職位的人員進行背景審查，對此表示不贊成者主要為公眾，原因是他們對諮詢文本中所列的審查犯罪記錄規定有不同意見，或者不贊成本澳就網絡安全防護體系進行立法。

5.2 程序、預防及應變方面的義務

諮詢文本建議關鍵基礎設施營運者需要制訂網安管理制度及內部操作程序，落實內部網絡安全保護、監測、預警及應急措施，以及向“網絡安全事故預警及應急中心”通報網安事故，告知相關監察實體並同時展開應急工作。

就“程序、預防及應變方面的義務”，贊成意見為 106 份，不贊成意見為 7 份；有 79 份意見對日後實際運作及制定具體的指引等方面提出討論或建議。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	35	71	1	6	79
百分比	55.21%		3.65%		41.15%



■ **意見摘要**

業界普遍關心各監察實體會否對相關的管理制度和操作程序提供具體及統一標準的指引，建議政府就網絡安全事故設立分級制度，並就通報機制、通報準則等作出更詳細的規定。

分析與回應

“網絡安全事故預警及應急中心”將按照國際慣例的做法，訂定網絡安全事故分級制度，同時，“網絡安全常設委員會”、“網絡安全事故預警及應急中心”以及各領域的監察實體將會與相關領域的關鍵基礎設施營運者互相合作，按照各領域行業的實際情況，訂定適合的網絡安全管理制度、操作流程及網絡安全具體標準，當中亦包括對網絡安全事故進行分級及通報的指引。

■ **意見摘要**

業界及公眾均認為關鍵基礎設施營運者須定期測試和更新應變程序。

分析與回應

“網絡安全常設委員會”、“網絡安全事故預警及應急中心”以及各領域的監察實體將會聯同各關鍵基礎設施營運者，定期舉辦網絡安全事故應急演習活動，藉此強化各個參與機構應急處置網絡安全事故時的協調能力及技術水平。

小結

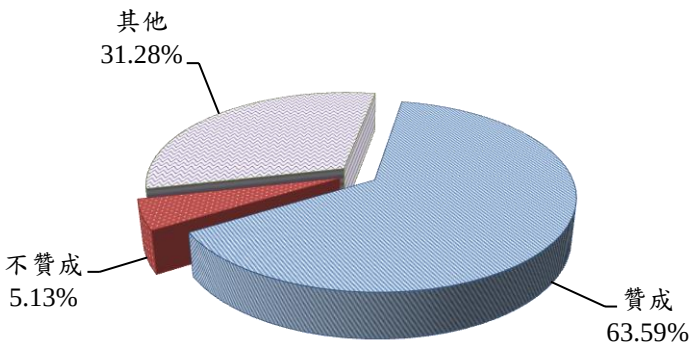
業界和公眾對於諮詢文本中建議的程序、預防及應變方面的義務普遍表示認同，對此持不贊成立場的主要來自於公眾，原因是他們認為保障網絡安全是各公私營機構應盡的責任，並應該由有關機構自行設立相應的程序措施保護其網絡安全，因而毋須設立《網絡安全法》進行有關規管。

5.3 自行檢測評估及報告義務

諮詢文本建議關鍵基礎設施營運者需要自行或委託專業機構檢測評估本身的網絡安全狀況及風險，並向所屬監察實體提交報告。

就“自行檢測評估及報告義務”，贊成意見為 124 份，不贊成意見為 10 份；有 61 份意見就評測基準及負責評估網安風險的專業機構等方面提出討論。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	46	78	3	7	61
百分比	63.59%		5.13%		31.28%



■ 意見摘要

業界主要就檢測標準、檢測範圍、評估的形式與次數，以及提交報告的方式和內容等方面提出意見和建議。

分析與回應

“網絡安全常設委員會”、“網絡安全事故預警及應急中心”及各領域的監察實體將會訂定適合於相關領域的評測範圍、標準、方式、報告格式及

內容要求等指引，以顧及關鍵基礎設施的規模與負擔能力。另外，當監察實體收到網絡安全檢測評估報告後會進行分析及評估，在有需要時，可提請“網絡安全事故預警及應急中心”提供技術意見。就報告收集時間及保密措施等細則事宜，《網絡安全法》正式公佈後將透過指引及傳閱文件等予以規範。

■ **意見摘要**

有業界及公眾意見指出，部分國家和地區強制規定必須由第三方進行網絡安全方面的檢測，建議本澳可以參考有關做法。

分析與回應

諮詢文本建議關鍵基礎設施營運者需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，主要是涉及安全方面的考量，因有些公共部門基於保密或安全原因，不具條件由第三方來檢測，故被監察實體應按照自身的實際情況需要作出適當的決定。

小結

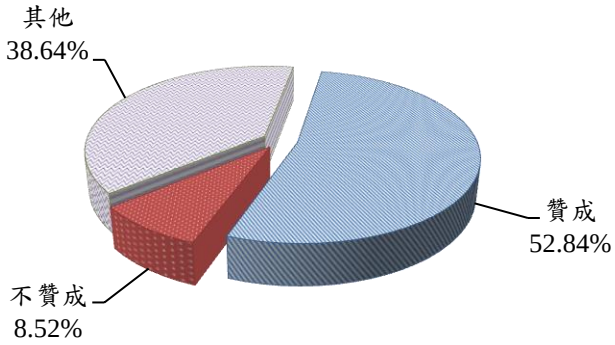
業界與公眾對“自行檢測評估及報告義務”大多數持贊成立場，並對具體評測要求及報告內容提出了多項完善建議，當局將於完善法律草案內容時予以考慮。

5.4 合作義務

諮詢文本建議在審查程序、預防或應變性義務履行情況的必要範圍內，關鍵基礎設施營運者允許“網絡安全事故預警及應急中心”或監察實體人員進入設施，並提供所需資料，以便進行審查。

就“合作義務”，贊成意見為 93 份，不贊成意見為 15 份；有 68 份意見主要就監察人員進入關鍵基礎設施的流程、逗留時間以及要求索取的資料內容提出建議。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	27	66	1	14	68
百分比	52.84%		8.52%		38.64%



■ **意見摘要**

來自業界的意見主要集中於“網絡安全事故預警及應急中心”或監察實體人員於執行相關職務時，其適用範圍、權限及可取得的資訊種類。

分析與回應

“網絡安全事故預警及應急中心”及監察實體僅在有充分跡象顯示被監察實體沒有履行《網絡安全法》所規定的義務，或於被監察實體發生或有可能發生了網絡安全事故時，方能夠派員到被監察實體工作地點，審查其網安作業程序以及各類義務的履行情況，或收集與網絡攻擊犯罪相關的證據，政府於執行上述職務前會盡早通知相關被監察實體。

此外，政府將對法律草案涉及程序、預防及應變方面義務的內容作出修改，明確關鍵基礎設施營運機構的網絡僅在例如遭受入侵或襲擊時，監察實體人員方可前往該等機構的設施了解實情。

■ **意見摘要**

有市民及傳媒建議法案要明確列出“合作義務”中關鍵基礎設施營運者會被要求提供哪些資訊，以免條文被濫用，或成為侵犯個人隱私、通訊保密、新聞自由等基本權利的工具。

分析與回應

在履行“合作義務”的情況下，關鍵基礎設施營運者的網安負責人可以在現場共同參與“網絡安全事故預警及應急中心”及監察實體人員的檢視過程，以確保“中心”及監察實體人員合理取得數據，避免提取關鍵基礎設施營運者的業務營運數據、客戶個人資料等涉密資訊。另一方面，個人資料及通訊內容不屬監察人員有權查閱及提取的數據範圍，僅在被監察實體明示同意或法官基於刑事偵查程序的需要而根據《刑事訴訟法典》規定允許下，方可被查閱或提取。

小結

絕大部分的業界意見對“合作義務”表示贊成，對此表示不贊成的意見主要來自於公眾，他們擔心在“合作義務”前提下市民的個人資料有可能被任意獲取，或者誤以為政府有權隨時直接進入傳媒機構並要求提供資料，損害新聞自由，甚至干預發佈新聞內容的數據資料。

基於此，政府在法律生效後將透過不同渠道加強有關的宣傳教育工作，釋除公眾疑慮，同時亦會對“網絡安全預警及應急中心”和監察實體在執行有關工作時訂定更明確的工作規範。

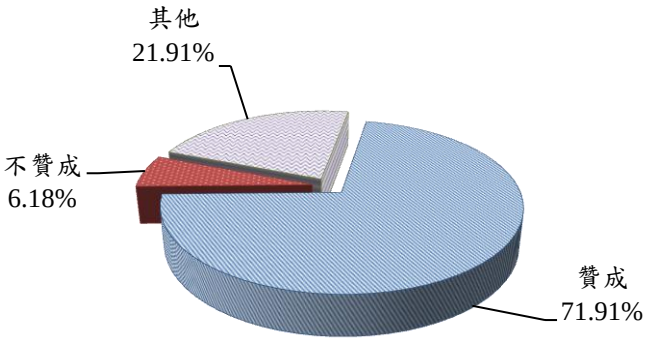
5.5 公共網絡經營者的特別義務

除“組織方面的義務”、“程序、預防及應變方面的義務”、“自行檢測評估及報告義務”及“合作義務”外，諮詢文本建議公共網絡經營者還須履行“實名制”及“日誌保存”兩個特別義務。

業界和公眾對“實名制”共有 128 份贊成意見，11 份不贊成意見；對“日誌保存”有 35 份贊成意見，8 份不贊成意見。另外，有 52 份提出了其他意見，包括對實名制的具體登記方式提出建議，以及對日誌保存的時間、會否涉及個人資料等問題進行討論。

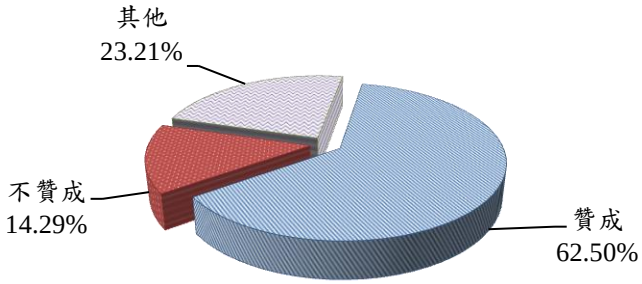
實名制

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	21	107	0	11	39
百分比	71.91%		6.18%		21.91%



日誌保存

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	16	19	0	8	13
百分比	62.5%		14.29%		23.21%



■ **意見摘要**

業界主要對“實名制”義務的適用範圍、具體執行方式及個人資料保護等多方面提出意見及建議，並建議監察實體先與各公共網絡經營者商議，再列出詳細技術及責任指引。

分析與回應

按照國際慣例，在“實名制”推行下，手機用戶在購買電訊營運商的電訊服務時，須提供真實身份資料作登記用途。按照澳門現時的電訊業務情況，除了預付卡外，現時澳門固網電話及手提電話用戶均以真實身份資料登記。“實名制”旨在要求購買預付卡的人士同樣需要提供真實身份資料以作登記，防止不法之徒利用不記名預付卡作為犯案工具，以逃避警方進行的刑事偵查，從而更好地維護社會治安、保障市民大眾的合法權益。因此，要求

預付卡用戶提供真實身份資料是“實名制”一項基本要求，亦是交易行為上普遍的規則，世界各地早已遵循此規則以保障社會利益。

另外，“實名制”義務同樣適用於向公眾提供互聯網接入服務的實體，即包括提供公共無線上網服務（如 WiFi-Go）的實體亦在適用範圍內。政府將透過不同渠道與相關的公共網絡經營者進一步商討“實名制”的施行細則及適用的技術措施。

■ **意見摘要**

業界及公眾就“實名制”建議公共網絡營運商引入簡便的登記設備及措施，並盡量透過電子方式進行登記，減低對市民的影響。

分析與回應

在推行“實名制”的過程中，政府會對個人資料保護、身份資料核實及更新、便捷性、對小型電訊零售商的影響等多項因素進行綜合考量，務求將“實名制”更好地推行。另外，政府對有關措施將會分階段執行，並與營運者溝通及協調，盡量以不影響目前市場運作的方式推行有關登記程序。

為優化“實名制”的規定，法案作出相應的修改，適當引入過渡條文，規定法律生效前已購買的預付卡，在法律生效後的一段期間內，其用戶將須補交真實身份資料，逾期者電訊營運商毋須對有關預付卡再作激活。

■ **意見摘要**

部分公眾對於“日誌保存”義務持不贊成意見，認為有關規定會對市民的個人隱私、網絡通訊或言論自由構成侵害。

分析與回應

諮詢文本所建議的“日誌保存”，是指將互聯網用戶上網時所使用的互聯網地址（即公有 IP 地址）與內聯網地址之間的對應轉換關係進行記錄保存，當中並不涉及用戶的網上行為或網站訪問記錄，保存目的是為了在偵查電腦網絡犯罪時，能夠追蹤使用涉案互聯網地址（即公有 IP 地址）人士的真實身份。為此，政府擬將“日誌保存”的名稱調整為“保存及提供網絡地址轉換紀錄”，並建議在第 11/2009 號《打擊電腦犯罪法》增加與“日誌保存”有關的條文，明確刑事警察機關須經法官根據刑事訴訟法律制度作出許可後，方可獲取網絡經營者所保存的“日誌”。

小結

業界和公眾普遍認為執行“實名制”和“日誌保存”有助打擊涉及網絡犯罪的源頭，亦有利於刑事犯罪調查，增加對市民的保障。

對“實名制”或“日誌保存”義務表示不贊成立場的意見共有 19 份，全部來自公眾，然而有關反對意見內容純粹基於意見者對兩者的執行並不了解所致。

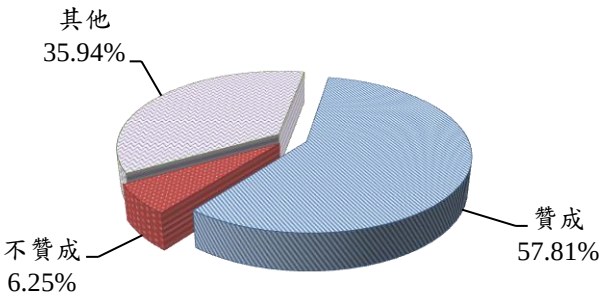
基於此，政府建議對法案進行修改，將“日誌保存”的名稱調整為“保存及提供網絡地址轉換記錄”，讓公眾清晰有關義務並不涉及用戶的網上行為或網站訪問記錄。

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與私人營運者同樣要遵守“程序、預防及應變方面的義務”、“自行檢測評估及報告義務”和“合作義務”，但對於“組織方面的義務”，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。

對此贊成意見為 37 份，不贊成意見為 4 份；有 23 份意見就構建公共部門網絡安全的防護措施提出建議。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	18	19	0	4	23
百分比	57.81%		6.25%		35.94%



■ **意見摘要**

業界表示，目前有公共部門透過外判方式由私人機構協助提供網絡服務，建議法案就公共部門能否採用外判方式進行網絡安全評估檢測作明確規範。

分析與回應

“網絡安全常設委員會”和“網絡安全事故預警及應急中心”將會研究制訂適合本澳政府部門的網絡安全管理制度、操作流程及網絡安全具體標準，另外亦會對公共部門將網絡安全工作外判的情況作更清晰的規定。

小結

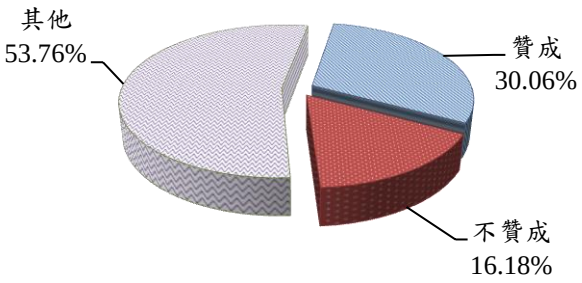
業界和公眾對於諮詢文本建議關鍵基礎設施營運者要遵守的義務普遍表示贊成。

6. 對不遵守義務的行政處罰和紀律責任

諮詢文本指出，對於不遵守“法定義務”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。對嚴重不遵守義務者，可單獨或合併科以附加處罰。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。

對此贊成意見為 52 份，不贊成意見為 28 份；有 93 份意見希望政府明確輕微與嚴重違反者的定義，並建議對違反義務的行為採取其他處罰，包括接受強制教育措施或負上刑責。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	12	40	4	24	93
百分比	30.06%		16.18%		53.76%



■ **意見摘要**

業界認為需要對不遵守義務的嚴重級別及相應處罰規則作清晰定義，並建議加入累犯制度。

分析與回應

《網絡安全法》規定的行政違法行為，除了受該法所規範外，亦受行政違法行為的一般規定，即十月四日第 52/99/M 號法令所規範。關於對行政違法行為如何適當作出處罰，經必要配合適用現行《刑法典》第六十五條第二款關於刑罰份量的確定的規定，政府會考慮所有對行政違法者的情節，綜合違反者的各種客觀情況，在法定的處罰種類及幅度內，恪守《行政程序法典》規定的各項原則，尤其合法性原則、適度原則、善意原則及公正無私原則，訂定適當的罰款以及附加處罰，而被監察實體亦可根據現行《行政程序法典》及《行政訴訟法典》的規定提出行政申訴和司法申訴。政府亦將在法律草案中加入與累犯行為相關的條文，明確規定累犯的概念及相關罰則。

■ **意見摘要**

業界建議清楚釐定公共網絡經營者不遵守“實名制”及“日誌保存”義務的相關罰則。

分析與回應

為使“實名制”及“日誌保存”的內容直接與互聯網服務的法律制度有關，政府將對法律草案內容進行調整及修改，擬按照現行第 24/2002 號行政法規《設立進入及經營提供互聯網服務業務的制度》所訂定罰款最高金額，處罰不履行的經營者。

■ **意見摘要**

有公眾建議對於嚴重違反法定義務的人士採取刑事處罰。

分析與回應

由於網絡安全制度在性質上屬於防範性管理制度，違反防範性規定的行為通常不以刑事方式處理，這符合澳門政府法律制度中的“刑法最少介入原則”，故在不妨礙其他法律或法規追究刑事責任的情況下，不宜對其網絡安全負責人處以刑責。

小結

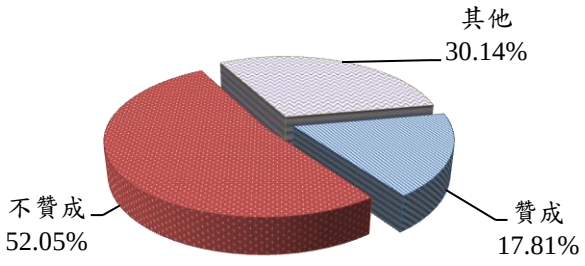
業界普遍贊成諮詢文本建議“對不遵守義務的行政處罰和紀律責任”的內容，然而相當部分的公眾認為諮詢文本所訂的罰則太輕。

7. 對生效日期的特別考慮

諮詢文本建議《網絡安全法》於公佈後 30 日起生效，而對網絡經營者的兩項特定義務（“實名制”及“日誌保存”）則另訂生效日期。

對此，贊成意見為 26 份，不贊成意見為 76 份，業界普遍表示需要更多時間落實有關網絡安全措施；有 44 份意見認為政府可適當地給予業界過渡期，並建議在法律生效前進行充分的宣傳。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	9	17	20	56	44
百分比	17.81%		52.05%		30.14%



■ **意見摘要**

對於法案的生效日期，業界普遍認為時間太快，表示需要更多時間落實網絡安全措施，包括方案制定、專業人員招聘、人員培訓及採購設備等。

分析與回應

考慮到各關鍵基礎設施營運者需要就網絡安全制度作出準備及適應，政府將調整法律的“待生效期”，以便相關方面妥善為法律的實施作出必要的準備。

■ **意見摘要**

業界表示需要時間推行“實名制”認證程序，以及安排系統處理及保存互聯網地址與內聯網地址的轉換對應關係（“日誌保存”），建議政府與電信營運商就有關內容再作詳細商討。

分析與回應

諮詢文本就網絡經營者的“實名制”及“日誌保存”義務未建議具體的生效日期，是希望與立法機關詳細討論及得到共識後才訂定，盡量減低對業界和市民大眾的影響。

小結

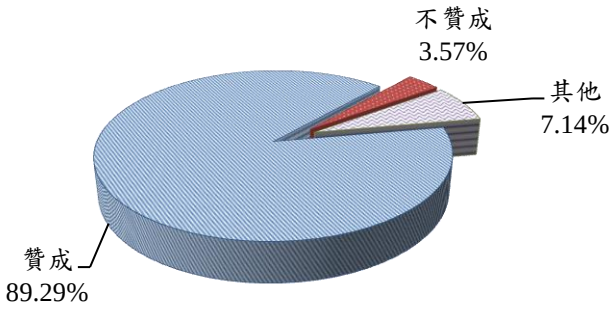
由於大多數業界及公眾對法律的生效日期（公佈後三十日）表示不贊成，認為有關時間太短，特區政府經考慮後，擬延長法律的“待生效期”，建議自《網絡安全法》公佈後一百八十日生效，以便各關鍵基礎設施營運者就網絡安全制度作出妥善的準備。

8. 細則性規定

諮詢文本指出，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。

對此贊成意見為 25 份，不贊成意見為 1 份；有 2 份意見，建議政府在訂定細則性規定前，深入了解不同業界在實施網路安全法時可能面對的技術性難題。

意見	贊成		不贊成		其他
	業界	公眾	業界	公眾	
數量	15	10	0	1	2
百分比	89.29%		3.57%		7.14%



■ **意見摘要**

對此表示不贊同的意見認為，有關內容應交由立法會對相關內容作討論，以配合特區政府施政方針及加強對法律的認受性。

分析與回應

政府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，是根據（經立法會審議通過的）第 13/2009 號法律《訂定內部規範的法律制度》所賦予政府的權力，就政府內部的組織架構內容以行政法規的形式予以規範。

小結

業界及公眾普遍對此不持異議，政府將着手起草相關行政法規以規範有關機構的運作。

第三部分

諮詢文本內容以外的意見和建議

在《網絡安全法》公開諮詢過程中，業界及公眾也提出了不少諮詢文本內容以外的意見和建議，現列出其中比較重要的意見和建議進行分析。

1. 提高社會大眾對網絡安全的認知

有不少意見認為，《網絡安全法》的適用對象應該涵蓋全澳市民及遊客，因為本澳各機構及個人都有責任保護好自身的網絡安全。

分析與回應

《網絡安全法》主要是構建網絡安全防護性行政管理體系，訂明關鍵基礎設施營運者的義務和責任，故此《網絡安全法》的適用對象為關鍵基礎設施營運者，而非一般的公司或個人。《網絡安全法》的立法與推行需要政府與社會各界共同合力落實，特區政府各相關部門將會繼續開展針對性的宣傳教育活動，而“網絡安全事故預警及應急中心”投入運作後，亦會向社會發放與本澳相關的網絡安全資訊，從而提升社會各行業、各階層的網絡安全防護意識，達到有效防護網絡安全的目的。

2. 關於設備的安全認證與評分

業界建議政府對關鍵設備和網絡安全專用產品的安全進行認證，以及對提供網絡安全服務的供應商或承包商引入評審或分級機制。

分析與回應

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，重點並不在於所使用的設備或服務供應商，故期望透過《網絡安全法》所訂定的恆常性、針對性措施與制度，及早發現網絡安全的異常狀況，繼而制訂相應的改善措施，為網絡安全提供保障。

3. 關於關鍵基礎設施營運者的指引內容

有公眾認為應該公佈政府向關鍵基礎設施營運者發出的指引內容，以及列出因應《網絡安全法》而使用的監控設備規格與功能等等。

分析與回應

各監察實體將因應各領域的特殊情況向關鍵基礎設施營運者發出相應的網絡安全指引，為此，政府會透過適當的途徑與業界溝通，令網絡安全得有效落實，但由於內容可能涉及業界具體操作情況及行內訊息，故政府需視乎情況審慎公開，例如使用的監控設備規格與功能是不適宜公開的，否則網絡將受到更大的侵害。

4. 關於網絡安全監察標準的協調性

有意見建議相關監察實體在訂定行業指引前可先收集業界意見，以確保指引的實務性和可行性，並注意網絡安全監察標準在運作時的協調性。

分析與回應

“網絡安全常設委員會”、“網絡安全事故預警及應急中心”以及各領域的監察實體，將會與相關領域的關鍵基礎設施機構互相合作，按照各領域的行業實際情況，訂定適合於相關領域的網絡安全管理制度、操作流程及網絡安全具體標準，並會因應資訊科技的發展狀況，適時作出檢討及更新。另外，“網絡安全事故預警及應急中心”亦會為各監察實體及被監察實體提供所需的技術指引及適當培訓，而監察實體在推行各領域的監管標準時會與“網絡安全事故預警及應急中心”共同確保標準的協調性。

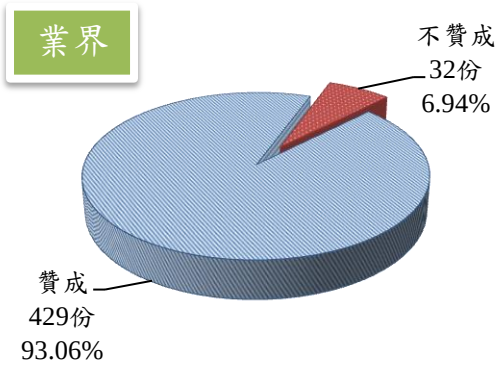
第四部分

總結

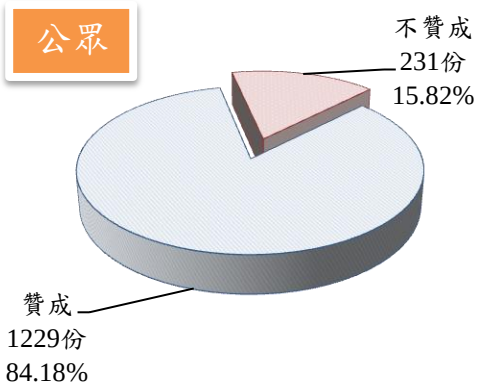
澳門特別行政區《網絡安全法》的公開諮詢工作已經順利完成，特區政府衷心感謝社會各界和市民大眾在諮詢期間提供的寶貴意見，這對於優化法案的內容具有積極意義。

《網絡安全法》公開諮詢的參與部門眾多，工作團隊來自保安司司長辦公室、行政公職局、經濟局、海事及水務局、交通事務局、能源業發展辦公室、環境保護局、民航局、金融管理局、博彩監察協調局、民政總署、衛生局、郵電局及司法警察局共 14 個公共部門、機關及實體，期間亦得到個人資料保護辦公室積極提供意見及參與公開諮詢的講解會，充分體現特區政府對建立網絡安全防護體系的重視。

《網絡安全法》公開諮詢旨在廣泛聽取市民意見，凝聚社會共識。特區政府綜合所收集的意見，得悉業界及公眾對《網絡安全法》的立法方向及建議內容普遍表示贊成，而且很多寶貴的建議對優化與完善法律草案起到重要的作用。



業界的立場



公眾的立場

在整理本諮詢報告期間，特區政府亦正着手跟進《網絡安全法》法案的草擬和完善工作，並根據公開諮詢所收到的意見，檢視有關內容，務求進一步清晰法案內的文字表述以減低公眾誤解，使法案能夠凝聚全體市民的共識，將來得以共同信守，以助鞏固社會的網絡安全。