國家資通安全發展方案(106年至109年)修正對照表

修正內容	現行內容	說明
貳、二、(三)新加坡之資安政策發展 新加坡有若干與網路安全有關的法規，如：「電腦濫用與網路安全法」(Computer Misuse and Cybersecurity Act, CMCA)、「通訊法」(Telecommunications Act)、「垃圾信件控制法」(Spam Control Act)、「電子交易法」（Electronic Transactions Act）等，並於2016年公布「網路安全策略」(Singapore’s Cyber security Strategy)，主要內容包括：(1)強化關鍵資訊基礎設施的韌性。(2)藉由動員企業與社區、面對網路威脅、打擊網路犯罪，及保護個人資料來創造更安全的網路空間。(3)發展包含技術勞力、具備先進技術的企業以及強大研究能量之網路安全生態系統（Cyber security ecosystem)，以支持新加坡的網路安全需求，同時	貳、二、(三)新加坡之資安政策發展 新加坡有若干與網路安全有關的法規，如：「電腦濫用與網路安全法」(Computer Misuse and Cybersecurity Act)、「通訊法」(Telecommunications Act)、「垃圾信件控制法」(Spam Control Act)、「電子交易法」（Electronic Transactions Act）等，並於2016年公布「網路安全策略」(Singapore’s Cyber security Strategy)，主要內容包括：(1)強化關鍵資訊基礎設施的韌性。(2)藉由動員企業與社區、面對網路威脅、打擊網路犯罪，及保護個人資料來創造更安全的網路空間。(3)發展包含技術勞力、具備先進技術的企業以及強大研究能量之網路安全生態系統（Cyber security ecosystem)，以支持新加坡的網路安全需求，同時	配合新加坡「電腦濫用對網路安全法」修正案及「網路安全法」分別於2017年及2018年通過並正式生效，修正相關內容。(第11頁至第12頁)

修正內容	現行內容	說明
也帶動經濟成長。(4)由於網路威脅沒有國界之分，因此致力於強化國際夥伴關係。 2017 年通過「電腦濫用與網路安全法」修訂案，主要是為了因應電腦犯罪本質的改變，及跨國性與網路犯罪手法的變化，防範電腦不受未經允許的存取及修改，亦授權政府在需要偵測、辨認，或應對網路威脅時得以強制關鍵基礎設施業者提供關於其網路之資訊。 2018 年並通過「網路安全法」(Cybersecurity Act)主要目的在建立與維護國家網路安全架構、有效降低網路威脅風險及確保關鍵資訊基礎設施受到保護，使國家能更有效率及完善地因應網路攻擊。該法並要求各關鍵基礎設施提供者通報網路安全事件，並採取防護措施以確保其系統的復原力（resilience)；此外也將賦與2015 年成立的新加坡網路安全局（Singapore’s Cybersecurity Agency, CSA）	也帶動經濟成長。(4)由於網路威脅沒有國界之分，因此致力於強化國際夥伴關係。 2017 年分別提出「網路安全法」(Cybersecurity Act)草案，及修訂「濫用電腦與網路安全法」(Computer Misuse and Cybersecurity Act, CMCA)。前者主要目的在建立與維護國家網路安全架構、有效降低網路威脅風險及確保關鍵資訊基礎設施受到保護，使國家能更有效率及完善地因應網路攻擊。該法並要求各關鍵基礎設施提供者報告網路安全事件，並採取措施來確保其系統的復原力（resilience)；此外也將賦與2015 年成立的新加坡網路安全局（Singapore’s Cybersecurity Agency, CSA）管理網路安全事件及提升網路安全標準的權力。後者主要是為了因應電腦犯罪本質的改變，即跨國性與規模擴大，網路犯罪的威脅擴大以及網路罪犯的犯罪手法的成長變化，以確保電腦不受未允許的存取及	

修正內容	現行內容	說明
管理網路安全事件及提升網路安全標準的權力。	修改，亦授權政府在需要偵測、辨認，或應對網路威脅時得以強制關鍵基礎設施業者提供關於其網絡之資訊。	
肆、三、(一) 1.完備我國資安相關法規及標準 1.1 完成「資通安全管理法」立法及進行相關法規調適 (1) 完成我國資安專法—「資通安全管理法」立法，並納入公務機關、關鍵基礎設施提供者及公營事業、政府捐助之財團法人等民營機構。	肆、三、(一) 1.完備我國資安相關法規及標準 1.1 完成「資通安全管理法」立法及進行相關法規調適 (1) 完成我國資安專法—「資通安全管理法」立法，並分階段逐步納入公務機關、關鍵基礎設施提供者及公營事業、政府捐助之財團法人等民營機構。	配合「資通安全管理法」施行作法，酌修文字。 (第 27 頁)
肆、四、表 1、部會分工表 「5.2 結合國內產業與民間社群能量，建立國內外公私協防機制」之主辦部會：行政院資安處、通傳會	肆、四、表 1、部會分工表 「5.2 結合國內產業與民間社群能量，建立國內外公私協防機制」之主辦部會：行政院資安處、國防部	因應台灣電腦網路危機處理暨協調中心(TWCERT/CC)業務自 108 年 1 月起由國防部監督之行政法人國家中山科學研究院交由通傳會所轄之財團法人台灣網路資訊中心(TWNIC)接手，異動主辦部會。 (第 37 頁)

修正內容	現行內容	說明
肆、五、圖 4、重要績效指標 KPI-1：推動政府機關資安治理成熟度達第 3 級(Level 3)	肆、五、圖 4、重要績效指標 KPI-1：推動政府機關資安治理成熟度第三方評審機制	配合資安治理成熟度評審機制，調修「完備資安基礎環境」之重要績效指標。 (第 39 頁)
肆、五、重要績效指標 (一) 推動政府機關資安治理成熟度達第 3 級(Level 3) 根據趨勢科技 2016 年度資訊安全總評報告，顯示 2016 年網路威脅屢創新高，勒索病毒造成全球企業損失金額高達 10 億美元（相當於新台幣 300 億元），且勒索病毒新家族數量較 2015 年相比成長 7 倍，而臺灣遭受此攻擊次數更排名全球前 20%，屬高資安風險國家。 為有效降低並控管政府機關資安風險，落實資安治理制度是必要的措施。我國自 103 年起開始輔導政府機關試行導入資安治理成熟度評估模式，以衡量組織之資安治理成效，截	肆、五、重要績效指標 (一) 推動政府機關資安治理成熟度達第 3 級(Level 3) 根據趨勢科技 2016 年度資訊安全總評報告，顯示 2016 年網路威脅屢創新高，勒索病毒造成全球企業損失金額高達 10 億美元（相當於新台幣 300 億元），且勒索病毒新家族數量較 2015 年相比成長 7 倍，而臺灣遭受此攻擊次數更排名全球前 20%，屬高資安風險國家。 為有效降低並控管政府機關資安風險，落實資安治理制度是必要的措施。我國自 103 年起開始輔導政府機關試行導入資安治理成熟度評估模式，以衡量組織之資安治理成效，截	配合資安治理成熟度評審機制，調修相關內容。 (第 40 頁)

修正內容	現行內容	說明
止 105 年底止，累計有 10 家政府機關推動試行。未來除了積極推動各政府機關全面導入資安治理成熟度評估模式，將透過定期辦理自評方式，引導各機關強化資安治理作為，朝制度化型(Established)、可預測型(Predictable)，甚至是創新型(Innovating)組織邁進，使 A、B 級政府機關資安治理成熟度達第 3 級(含以上)，健全各政府機關之資安體質。	止 105 年底止，累計有 10 家政府機關推動試行。未來除了積極推動各政府機關全面導入資安治理成熟度評估模式，定期辦理自評外，並建立政府機關第三方評審機制。透過公正的第三方評審，引導各機關強化資安治理作為，朝制度化型(Established)、可預測型(Predictable)，甚至是創新型(Innovating)組織邁進，使 A、B 級政府機關資安治理成熟度達第 3 級(含以上)，健全各政府機關之資安體質。	
肆、五、表 2、分年里程碑 106 年： 推動 A、B 級政府機關試行導入資安治理成熟度 107 年： ● 精進資安治理成熟度評審機制 ● 完成 3 個 A 級政府機關導入資安治理成熟度自評作業	肆、五、表 2、分年里程碑 106 年： 推動 A、B 級政府機關完成資安治理成熟度自我評估 107 年： 建立資安治理成熟度第三方評審機制 108 年： 推動 30 個 A 級政府機關落實資安治理成熟度第三方評審，成	配合資安治理成熟度評審機制，調修分年里程碑。 (第 43 頁)

修正內容	現行內容	說明
108 年： 推動 30 個 A 級政府機關落實資安治理成熟度自評作業，成熟度達第 2 級以上 109 年： 推動所有 A 級政府機關落實資安治理成熟度自評作業，成熟度達第 3 級以上	熟度達第 2 級以上 109 年： 推動所有 A 級政府機關落實資安治理成熟度第三方評審，成熟度達第 3 級以上	
柒、附件 1、2.1 強化通訊網路資安防禦與應變能量 1. 107 年底前完成國家通訊暨網際安全中心(NCCSC)建置。	柒、附件 1、2.1 強化通訊網路資安防禦與應變能量 1. 107 年底前完成通訊傳播資通安全防護中心(NOMC)建置。	通訊傳播資通安全防護中心(NOMC)業於 107 年底更名為國家通訊暨網際安全中心(National Communications and Cyber Security Center, NCCSC)，爰調修相關內容。 (第 47 頁)
柒、附件 1、3.2 推動政府機關導入資安治理制度 1. 106 年推動 A、B 級政府機關試行導入資安治理成熟度自評作業。 2. 107 年精進資安治理成熟度評審機制，並推動 3 個 A	柒、附件 1、3.2 推動政府機關導入資安治理制度 1. 106 年推動 A、B 級政府機關完成資安治理成熟度自我評估。 2. 107 年建立資安治理成熟度第三方評審機制。	配合資安治理成熟度評審機制，調修分年重要進程。 (第 48 頁)

修正內容	現行內容	說明
級政府機關完成資安治理成熟度自評作業。 3. 108 年推動 30 個 A 級政府機關落實資安治理成熟度自評，成熟度達第 2 級以上。 4. 109 年推動所有 A 級政府機關落實資安治理成熟度自評，成熟度達第 3 級以上。	3. 108 年推動 30 個 A 級政府機關落實資安治理成熟度第三方評審。 4. 109 年推動所有 A 級政府機關落實資安治理成熟度第三方評審。	
柒、附件 1、5.2 結合國內產業與民間社群能量，建立國內外公私協防機制 主(協)辦部會：行政院資安處、通傳會	柒、附件 1、5.2 結合國內產業與民間社群能量，建立國內外公私協防機制 主(協)辦部會：行政院資安處、國防部	因應台灣電腦網路危機處理暨協調中心(TWCERT/CC)業務自 108 年 1 月起由國防部監督之行政法人國家中山科學研究院交由通傳會所轄之財團法人台灣網路資訊中心(TWNIC)接手，異動主辦部會。 (第 50 頁)
柒、附件 1、7.1 連結國家防衛需求，發展國內資安產業生態系 2. 109 年底前輔導資安新創團隊達 20 家，協助媒合新創團隊	柒、附件 1、7.1 連結國家防衛需求，發展國內資安產業生態系 2. 109 年底前輔導資安新創團隊達 30 家，協助媒合新創團隊	配合「資安產業發展行動計畫(107 年至 114 年)」2020 年目標，調修輔導資安新創團隊家

修正內容	現行內容	說明
與創投基金。	與創投基金。	數。 （第 50 頁）
柒、附件 1、10.2 拔擢在職人士培育產業所需之資安專業人才 3. 109 年底前進行資安先進課程本土化及產業擴散。	柒、附件 1、10.2 拔擢在職人士培育產業所需之資安專業人才 3. 108 年底前進行資安先進課程本土化及產業擴散。	調修資安先進課程本土化及產業擴散之推動期程。 （第 51 頁及第 52 頁）