第五代行動通信系統資通安全維護計畫參考框架

國家通訊傳播委員會

108 年 10 月 31 日

目錄

壹、前言.....1
貳、適用範圍.....8
參、撰寫說明.....9
肆、相關法規及參考文件.....28

壹、前言

一、 依據

行動寬頻演進至第五代行動通信系統（以下簡稱 5G 系統），其創新的架構與技術，不僅進一步提升超寬頻傳輸速度，更是要提供大規模的傳輸容量與超低延遲的傳輸品質。這些能力將成為推動與支援數位時代下各種新興服務與創新應用，如物聯網、智慧交通、智慧工廠與智慧醫療等的關鍵基礎建設。因此，世界各國在要達到數位國家、數位經濟與第四代工業革命的願景上，於促進產業轉型與發展的政策都是以 5G 系統為發展基盤，以打造數位國家創新生態的目標。

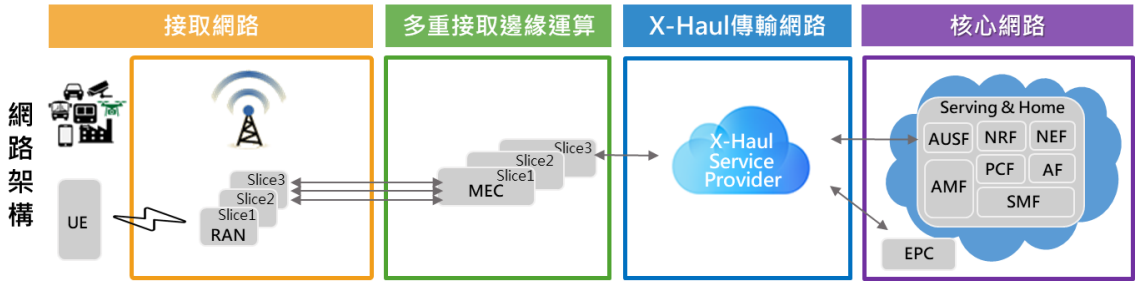
為此，5G 系統在架構設計上就是以具備強大功能擴充彈性為理念，以因應未來各種潛在應用服務為目標，包含導入無線電接取網路之 CUPS、以服務為根基的核心網路架構、網路切片（Network Slicing, NS），以及邊緣運算的設置型態。因此，不同於 4G 系統架構，5G 系統高程度地將過往硬體為主的網路系統設置模式做大幅的分解，將網路功能軟體化（Network Function Softwarization），以達到網路功能的快速擴充與彈性。從運算、存儲及軟體運作的角度，5G 系統將納入更多元與廣泛的資訊技術（Information Technology, IT）與通訊技術（Communications Technology, CT）以及平臺與產品在整體網路運營及服務提供上面。對電信業者而言，這些新穎的架構與開放除將帶來成本和部署的敏捷性外，同時亦將使得 5G 系統面臨更為複雜與多元之資通安全風險與威脅。

通訊網路是我國八大關鍵基礎設施之一，為完備 5G 系統建設與相關產業的發展，第一波釋照得標者需負擔公共義務。**通傳會爰依據電信法及行動寬頻業務管理規則第 40 條第 5 項載明得標者應行之資通安全事項**，於得標後申請籌設許可時，應向通傳會提報 5G 系統設置「事業計畫書」與

「第五代行動通信系統資通安全維護計畫」。其中後者載明 17 項資通安全維護義務之要求，敘明業者所設置之 5G 系統之資通安全防護政策、目標、範圍、措施等之時程、人力與資源配置、流程管理、風險評估及設置等事項，確保得標者所設置的 5G 系統是安全、可信賴的，以保障我國關鍵基礎設施之資通安全及消費者權益，鼓勵創新服務與健全電信產業發展。

二、 5G 系統設置之風險、威脅及挑戰

根據 3GPP 標準文件，本參考框架可將 5G 系統設置概分為無線電接取網路（Radio Access Network, RAN）、多重接取邊緣運算（Multi-access Edge Computing, MEC）、X-Haul 傳輸網路（X-Haul Transport Networks (X-Haul, TN), 包含 Fronthaul, Midhaul, and Backhaul transport networks）以及核心網路（Core Network, CN）四大區塊，如圖一所示。



圖一、5G 系統架構圖

5G 系統架構因為採取網路功能軟體化的做法，我們預期未來 5G 系統將會有大量的軟體功能模組，如軟體定義網路（Software-Defined Network, SDN）、網路功能虛擬化（Network Functions Virtualization, NFV）、網路切片、基地臺基頻單元（Base Band Unit, BBU）邏輯分離等，亦即在配合包括網路控制功能軟體化、網路化等設計下，將大幅度地導入資訊技術與

通訊技術之軟硬體及平臺，此舉將使網路功能元件與元件間之實作及連接介面更開放與具備互通、整合與擴增的彈性。然而 5G 系統建置並非一蹴可幾，得標者多半將分階段進行，例如建置初期預期會以非獨立（Non-Standalone, NSA）形式為主，亦即先行佈建5G系統之無線電接取網路，並與現行 4G 系統整合以提供 5G 服務，再於下一階段逐步導入 5G 系統之核心網路功能，提供獨立（Standalone, SA）形式之 5G 服務。

以 5G 系統為發展基磐，5G 系統將扮演促進創新服務與市場及推動我國含括國家、社會、經濟、產業、企業及國民在增進數位競爭力與優勢的重要角色。因此，5G 系統架構的設計理念就是以能夠彈性並快速支援未來各種可能的新興應用服務及其設置型態為核心，其中無線電接取網路採取分離傳統基地臺基頻單元為中央單元（Centralized Unit, CU）與分布單元（Distributed Unit, DU）；多重接取邊緣運算利用前端無線電接取網路結合雲端運算資源，在網路邊緣提供資訊技術與通訊技術融合的快速與敏捷性的服務提供；核心網路的設計更是以服務導向架構（Service-based Architecture, SBA）為根基，讓得標者可根據新興服務的需求彈性、快速地進行服務提供所需的功能建置或擴展，以及達到自主軟體運作、區隔及獨立維運；在達到端對端（End-to-end）大寬頻、低延遲、全面 5G 系統服務覆蓋的網路建置，支援無線電接取網路與核心網路之間高頻寬傳輸需求之 X-Haul 傳輸網路，將扮演極為重要的角色。因為 5G 系統架構將網路功能軟體化列為主要實踐目標之一，我們預期 5G 系統的建置將大量使用資通訊科技在網路系統的實作並開放網路功能和系統的介面，形成 5G 系統設置的開放性、彈性與整合性。

此亦致使 5G 系統設置面臨比傳統 3G、4G 系統設置更為多元與嚴峻的資通安全風險、威脅與挑戰：（1）資通安全控制措施不足之風險情境，

例如組態配置錯誤、缺乏適當的驗證與授權機制；（2）5G 供應鏈相關之風險情境，例如對於 5G 資訊技術與通訊技術及產品品質保證之缺乏、單一供應商之依賴性、供應鏈上下游之依賴性；（3）威脅來源的發動攻擊的風險，例如第三方對於供應鏈之干預、攻擊 5G 系統的部分功能以阻斷服務或竊取用戶隱私資料；（4）5G 系統與關鍵基礎設施相依性之風險情境，例如透過 5G 系統進而攻擊其他關鍵基礎設施、因電力系統中斷導致 5G 系統無法運作；（5）與用戶設備有關之風險情境，例如利用物聯網設備攻擊 5G 系統。此外，在建置初期，5G 系統因採用非獨立形式建置並與 3G、4G 系統整合，會面臨既有 3G、4G 系統之風險，而 5G 無線電接取網路之中央單元與分布單元邏輯分離核心模式，可能面臨潛在性技術風險包含實體層攻擊（Physical Attack）、用戶隱私資料竊聽（User Data Eavesdropping Attack）與阻斷服務攻擊（Denial-of-Service Attack）、偽基地臺（Rogue Base Station）、資料完整性攻擊（Data Integrity Attack）、空中介面攻擊（Air Interface Attack）等威脅；中央單元隨著軟體化而產生新的風險，亦對管理制度帶來挑戰，例如，中央單元相關的軟體更新制度與流程，組態變更之控制管理，皆產生不同面向之風險。

多重接取邊緣運算架構的理念是可讓 5G 系統服務提供者在為達到特別是低延遲服務效能的目標下可以直接使用 5G 系統之網路邊緣所部署的運算、儲存資源或數據，大幅減少連結遠端雲端運作所需的傳輸延遲，以提供用戶端更佳的服務品質與體驗。因此，得標者未來可能提供第三方服務提供者多重接取邊緣運算服務或是開放允許他們設置相關系統於 5G 系統的網路邊緣，此舉對比於前二代相對封閉式的網路與系統設置，在資通安全維護上將產生新的風險、威脅及挑戰。例如，得標者提供包含運算、儲存等基礎設施與運作平臺，允許第三方服務提供者將其服務系統運作其

上，此一政策得標者則必須審慎採取必要措施確保各系統間的運行、效能與安全之隔離與管理，避免可能的資源濫用、翻牆、滲透與入侵，建立妥適的資通安全管理制度、流程與機制；倘若第三方服務提供者之服務系統有連結外部系統或是網路的需求，此舉可能有因其程式或系統缺陷而導致遭受攻擊或被駭客入侵，埋入惡意應用程式，蔓延擴散而影響整體 5G 系統正常運作的高度風險，必須慎重應對。或是，得標者對於多重接取邊緣運算之部署政策是允許第三方服務提供者放置其設備於得標者機房，相關機房管理政策與制度應包含實體層面、維運及人員管理之風險及威脅納入考量。如何建立完整有效的整體多重接取邊緣運算資安維護之政策、管理制度與防禦機制是一項新的挑戰。

5G 系統 X-Haul 傳輸網路之設置架構在 4G 系統常見採用光纖傳輸，其資安威脅包含可能的傳輸竊聽（Eavesdropping Attack）等攻擊。倘若得標者非自建而採取租用或共用他方之傳輸線路，在資通安全維護之政策與管理制度應考量所有可能的風險及威脅，包含線路提供者所可能帶來的風險，或是與線路共用者間之資通安全管理責任與防護作為，應有明確區分與相關管控措施。

以服務為基礎的核心網路裡，網路切片可能遭受惡意攻擊的威脅，為防止威脅擴散，應強化其隔離之安全性。此外，網路切片透過軟體化技術，協同多個網路功能模組提供服務，各功能模組面臨之威脅，例如前述之軟體更新與組態管理等風險，亦增加資通安全管理之挑戰。

三、 目的

本參考框架之目的是提供 5G 執照得標者在 5G 系統資通安全維護計畫內容擬定與撰寫的參考。具體而言，是對 5G 系統設置之資通安全維護計

畫的各項目主題敘明其內容目標與重點議題，涵蓋以下五大面向：

1. 達到安全、可信賴之 5G 系統設置與管理：

   建立安全可靠之 5G 服務環境為得標者之關鍵任務，得標者訂定第五代行動通信系統資通安全維護計畫時，應以 5G 系統架構全景及其網路系統特性為基礎，評估 5G 整體相關業務之資通安全需求與可能風險，訂定與落實第五代行動通信系統資通安全維護計畫。

2. 安全的軟體更新與部署管理（Secure Software Update and Distribution Management）：

   得標者在面對軟體更新與部署、組態變更之控制管理等安全防護時，管理制度上必須考量如檔案更新流程、版本制度、相關伺服器主機維運管理、密鑰安全防護、軟體開發流程、軟體發布與部署環節、安全軟體發展生命週期、軟體供應鏈及整體 5G 系統流程管理等資通安全防護及控制措施，並全面掌握可能發生之威脅、風險及盤點防護面向。

3. 安全的上下游供應鏈管理（Secure Supply Chain Security Management）

   得標者可於 5G 產業生態鏈中，包含得標者、電信設備供應商、應用服務提供商及終端用戶此一脈絡展開，了解其可能影響到 5G 系統、服務及營運之資通安全議題與風險，尤其隨著 5G 系統服務逐步走向開放式架構，5G 系統資通訊系統將結合更多委外或第三方供應商之服務，得標者對於供應鏈與相關人員、軟體開發之之管理，應更加掌握及透明（Transparency），以降低潛在資安風險。

4. 建立資安事件通報與應變機制：

   在面對瞬息萬變的 5G 產業需求與環境變化，得標者應與主管機關配合，制訂相關通報因應機制，以強化自身之強韌性（Resilience），

並透過事前演練，了解與熟悉相關應變機制。

5. 5G 資通安全維護措施的持續精進：

得標者在規劃與設置資通安全偵測與防護之執行方案時，除前述資通安全議題外，應在確保用戶資料安全與保護用戶隱私之前提下，從設置網路、提供應用服務及營運管理等持續精進相關管理機制與保護措施，完善 5G 系統之整體資通訊安全。

貳、適用範圍

本 5G 系統設置說明適用於參與中華民國一百零八年開放特許執照之競價程序，並依行動寬頻業務管理規則第 36 條規定，向主管機關一次繳清得標金，或繳納得標金頭期款及得標金餘額及其利息之支付擔保後之得標者。

前述得標者，依行動寬頻業務管理規則第 40 條，檢具第五代行動通信系統資通安全維護計畫向通傳會申請核發籌設同意書，或已為經營者之得標者，向通傳會申請第五代行動通信系統資通安全維護計畫之變更，內容均應符合 5G 系統設置資通安全維護計畫參考框架之說明。

參、撰寫說明

依行動寬頻業務管理規則第 40 條第 5 項規定，「第五代行動通信系統資通安全維護計畫」應載明十七個項目，以下就每一項目敘明應載明事項：

一、 資通安全政策及目標（Policy & Goals）

背景說明

有鑒於 5G 系統將是我國通訊傳播網路基礎設施很重要的一部份，且是促進我國創新服務及推動數位國家、數位經濟的重要基磐。

自述重點

請得標者對所設置之 5G 系統在資通安全維護提出政策方案與目標。

得標者之資通安全維護政策應包含以下面向：

- 於網路建置、運作與營運管理
- 於服務提供與管理
- 於與其他關鍵服務之相依性（Dependency），包含現行行動寬頻網路
- 於遭遇災害時之強韌性
- 利害關係人及其需求，例如中央主管機關及用戶
- 相關法規遵循
- 於網路資料傳輸與儲存之隱私保護

得標者應對自述之政策提出具體且明確欲達成的目標。本項目所述之政策與目標，應鏈結並扣合本維護計畫第二至十七項之內容。

二、 核心業務及其重要性（Core Business & Significance）

背景說明

得標者為經營 5G 業務需執行一系列活動。得標者應檢視並評量其業務之主要領域及活動，視為核心業務。在認定業務或活動之重要性上，可透過分析業務遭受衝擊時可能造成的影響，盤點並釐清 5G 業務在功能面、管理面及法遵面於得標者營運時的重要性及相依性，以建立 5G 核心業務之全景，並了解核心業務在運作及服務提供上於機密性、完整性、可用性、可靠性及適法性等的要求是關鍵且必要。同時，當各業務失效（Business Failure）包含遭受威脅攻擊與天然災害時，可能產生網路或服務無法完整運作與提供，應考量強韌性需求，包含隔離影響區域或業務、緊急應處、災難復原、恢復正常作業，以維持業務不中斷。

業務相依性之內容，除 5G 與其他外部關鍵服務之相依性需敘明外，支持 5G 業務之內部服務其相依性也應納入考量。

自述重點

請得標者對於所欲建設及經營之 5G 系統，請先說明所使用之評量基準，再列出判定為核心業務的項目及說明其重要性。

得標者之核心業務及其重要性與相依性應考量以下面向：

- 於整體網路運作、服務提供及營運目標之重要性
- 於整體網路運作、服務提供及營運之可靠性、機密性、完整性、可用性及適法性
- 於所負擔之指定義務，如災害防救、動員準備或通訊監察等業務的相依性
- 於業務失效時可能產生之影響

- 於維持網路服務持續運作之強韌性

此一項目之內容，得標者應扣合第一項「資通安全政策及目標」所提出之政策與目標，力求一致，並參酌上述說明。

三、 行動寬頻系統資通安全維護範圍（Scope of Protection）

背景說明

得標者應說明，為落實第一項「資通安全政策及目標」所提出之政策與目標，以及第二項「核心業務及其重要性」之內容，盤點出要納入本計畫之資通安全維護範圍，例如業務項目、電信設備、營運系統、營運機房、營運人員等。

自述重點

得標者擬定資通安全維護範圍時，應考量以下面向：

- 於核心業務項目
- 於 5G 通信網路基礎設施，包含無線電接取網路、多重接取邊緣運算、X-Haul 傳輸網路與核心網路
- 於 5G 營運系統
- 於與得標者既有異質行動通信網路及固定通信網路之整合介接
- 於與外部其他電信網路之介接
- 於用於 5G 系統營運之軟硬體資源之上下游供應鏈管理

- 於如有允許第三方服務提供商之設備且/或系統建置於得標者之5G系統內之相關資通安全政策與管理措施，以及是否納入本計畫之資通安全維護範圍

四、 資通安全推動組織（Cybersecurity Executive Organization）

背景說明

為落實資通安全政策與達成資通安全目標，得標者應成立專責且獲充分授權之資通安全組織，訂定各項資通安全之政策與制度、規劃與協調跨部門資通安全維護之權責與分工，包括涵蓋第三項「行動寬頻系統資通安全維護範圍」之業務單位；週期性持續之資通安全措施規劃、防護、績效評估及改善等相關作業；核定各項資通安全維護範圍內之業務之資通安全負責人員以督導相關工作事項，落實到各業務單位。資通安全組織成員應具資通安全相關經驗或相關能力證明，成員名單、職掌及權責應予以造冊並適時更新。得標者應依據本資通安全維護計畫內容，提供建立、執行及持續改善等作業所需之資源。

自述重點

得標者於成立資通安全組織時，應考量參酌上述背景說明，扣合本文件第一項、第二項及第三項之自述內容，訂出資通安全組織相關辦法。

得標者之資通安全組織應考量以下面向：

- 專責且於組織架構中具相當位階
- 訂定資通安全政策與相關制度
- 規劃資通安全組織之組成、分工、職掌、權責等內容

- 跨部門協調資通安全維護之權責與分工包含明訂必須涵蓋之第三項「行動寬頻系統資通安全維護範圍」之業務單位
- 週期性持續之資通安全措施規劃、防護、績效評估及改善等相關作業原則與管理辦法
- 資通安全組織成員之資格與能力，例如應具備之資通安全相關經驗與能力
- 於規劃執行資通安全維護計畫內容時所需人力、預算及資源

五、 專責人力及經費之配置（Dedicated Personnel and Budget Allocation）

背景說明

為落實資通安全政策與達成資通安全目標，得標者應考量第四項所述之「資通安全組織」之工作與執掌內容，配置專責人力、經費與資源，並明訂制度做定期之檢視、檢討與改進。資通安全預算配置應於得標者整體預算中佔合理之比例且符合整體 5G 系統資通安全維護之政策、目標與需求。此項目應納入資通安全維護計畫持續改善與績效管理評量項目之一。

自述重點

得標者應考量參酌上述背景說明，扣合第四項「資通安全組織」自述之內容，配置 5G 系統所需之專責人力、經費與資源。

得標者之資通安全專責人力、經費與資源之配置應考量以下面向：

- 符合第四項「資通安全組織」所述之工作及執掌內容敘明應配置之人員人數、資格及資源

- 符合整體 5G 系統資通安全維護之政策及目標之資通安全預算於得標者整體預算中佔之比例
- 5G 系統之資通安全維護作業應涵蓋第三項「行動寬頻系統資通安全維護範圍」之業務單位
- 應週期性且持續審視資通安全組織之人員與經費等資源配置

六、 資通安全長之配置（Chief Security Officer）

背景說明

得標者應設置專責人員擔任 5G 系統資通安全執行長，負責本計畫所訂定之業務之執行，包括領導 5G 系統資通安全組織，推動相關政策，及協調跨部門 5G 系統資通安全維護之權責與分工。資通安全執行長應熟習公司組織結構及業務，避免職務重疊或利益衝突，並具備充分之資通安全管理之專業知識及實務資歷與經驗。

自述重點

得標者應參酌上述背景說明，扣合第四項「資通安全組織」之內容，敘明資通安全執行長之職掌與權責、資格、派任等。

得標者之資通安全執行長配置應考量以下面向：

- 依據第四項「資通安全組織」所述之內容，明訂執行長之職掌與權責
- 於組織管理架構中之位階
- 人選資格
- 派任方式

七、 資訊及資通系統之盤點規劃（含系統設備符合 ITU 或 3GPP 發布之資通安全規定）（Identification of Information and Communications Systems (including Equipment in Compliance with ITU or 3GPP Regulations）

背景說明

得標者應就第三項「行動寬頻系統資通安全維護範圍」所述之內容，對所有納入本計畫之資通安全維護範圍的業務項目、電信設備、營運支援系統（Operations Support Systems）、營運機房等，就其於業務執行、功能運作與維護時所採用之資訊技術與通訊技術及產品包含硬體、軟體、網路功能、系統等進行盤點。前述盤點出之 5G 系統相關設備，應進一步確認其是否符合 ITU 或 3GPP 發布之資通安全規定。此外，5G 系統初階段之建置，如有與現行 3G、4G 系統共存並整合，亦應同時盤點這些網路之系統與整體 5G 業務執行、功能運作與維護之相關介面、模組等。

自述重點

得標者應考量參酌上述背景說明，扣合第三項「行動寬頻系統資通安全維護範圍」自述之 5G 系統資通安全維護範圍，就其業務執行、功能運作與維護時所採用之資訊技術與通訊技術及產品包含硬體、軟體、網路功能、系統等進行盤點。特別注意的是 5G 系統初階段之建置，如有與現行 3G、4G 系統共存並整合，亦應同時盤點這些網路之系統與整體 5G 業務執行、功能運作與維護之相關介面、模組等。

得標者進行盤點時應考量以下面向：

- 5G 系統涵蓋四大區塊，於各區塊下用以支援其業務執行、功能運作與維護所採用之資訊技術與通訊技術及產品包含硬體、軟體、網路功能、系統

- 於 5G 系統初階段之建置，如有與現行 3G、4G 系統共存並整合，應同時盤點這些網路之系統與整體 5G 業務執行、功能運作與維護之相關介面、模組等
- 於盤點出之模組、技術及產品，確認是否符合 ITU 或 3GPP 發布之資通安全規定

八、 資通安全風險評估（Cybersecurity Risk Assessment）

背景說明

為建立安全、可靠及具強韌性之 5G 系統與服務環境，得標者應考量 5G 系統下各區塊之功能架構與運作特性，就其業務執行、功能運作與維護，及其營運支援系統採用資訊技術、通訊技術與產品可能之威脅種類與威脅者（Threat Actors），以及扣合第二項「核心業務及其重要性」、第三項「行動寬頻系統資通安全維護範圍」及第七項「資訊及資通系統之盤點規劃」自述之內容，就納入本行動寬頻系統資通安全維護範圍之資產各自的重要性，及用以支援其業務執行、功能運作與維護所採用之資訊技術與通訊技術及產品等硬體、軟體、網路功能及系統等潛在之不同程度的弱點（Vulnerability），評估可能的主要風險與情境。此外，檢視威脅種類與威脅者應包含得標者之組織運營、制度、程序及人員作業等各層面可能產生的風險。

自述重點

得標者應參酌上述背景說明，評估可能的主要資通安全風險與情境。

得標者之資通安全風險評估應考量以下面向：

- 於達到建立安全、可靠及具強韌性之 5G 系統與服務環境，並考量 5G 系統下各區塊之功能架構與運作特性，請就納入本行動寬頻系統資通安全維護範圍之資產的重要性，及用以支援其業務執行、功能運作與維護所採用之資訊技術與通訊技術及產品等硬體、軟體、網路功能及系統等，評估：1) 可能之威脅種類與威脅者；2) 潛在之不同程度的弱點（Vulnerability）；及 3）可能的主要風險與情境類別包含營運策略、資源管理、供應鏈管理、災害應變、作業管理、實體安全、技術管理，軟硬體與其上下游供應鏈管理、第三方服務供應商等
- 檢視威脅種類與威脅者應包含得標者之組織運營、制度、程序及人員作業等各層面可能產生的風險。

九、 資通安全防護及控制措施（Cybersecurity Protection and Control Measures）

背景說明

得標者應扣合於第八項「資通安全風險評估」所提出的評估資料，提出妥適的資通安全防護及控制之架構與措施，措施應包含系統的基準配置（Baseline Configuration of Systems）、系統開發生命週期、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理。並應就所提之架構與措施，評估其防護之效益，以及一旦失效時可能帶來的衝擊。

自述重點

得標者應考量參酌上述背景說明，在擬定資通安全防護及控制之架構與措施應涵蓋選擇合適的資通安全防護技術，或使用安全設計原則以設計運作管理流程與實體設施安全管控機制。

得標者之資通安全防護措施應考量以下面向：

- 於第八項已識別之風險與情境，提出妥適的資通安全防護及控制之架構與措施，措施應包含系統的基準配置、系統開發生命週期、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序與流程管理、技術、人員管理
- 於所提之架構與措施，評估其防護之效益，以及一旦失效時可能帶來的衝擊
- 於落實第一項所自述之資通安全政策與目標
- 於資通安全防護與控制措施之執行單位與執行方式

十、 資通安全事件通報、應變及演練相關機制（Notification, Response, and Exercise of Cybersecurity Event）

背景說明

因為得標者設置之 5G 系統，將會成為我國通訊關鍵基礎設施的一部份，因此，對於發生的資安事件，應遵循資通安全管理法訂定資通安全事件通報及應變處理之程序、流程與作業辦法，以確保能夠及時、快速地反應並處理所發生的資安事件，最大程度地減少損失，減輕被利用的漏洞，恢復服務和流程並降低未來事件帶來的風險。

自述重點

得標者應根據資通安全管理子法（資通安全責任等級分級辦法、資通安全事件通報及應變辦法）、行動寬頻業務管理規則第五十五條之一，並參酌上述背景說明，扣合第二項「核心業務及其重要性」、第三項「行動寬頻系統資通安全維護範圍」、第七項「資訊及資通系統之盤點規劃」、第九項「資通安全防護及控制措施」等自述之內容，敘明資通安全事件通報、應變及演練相關機制。

得標者自述之資通安全事件通報、應變及演練相關機制應考量以下面向：

- 擬定資通安全事件應變小組成員與執掌，成員應至少包括資安長、資安技術人員和資訊技術人員、所涉及的部門的資安人員，及其他核心業務的代表人員
- 擬定資通安全事件應變計畫，其內容應包含事件發生時與發生後的處置含應處程序，流程與作業；事件發生時相關單位之協調溝通；事件發生時損害控制措施；事件發生後之復原、鑑識、調查及改善機制
- 擬定建立資通安全事件發生時之通報作業辦法，其內容應包含於資通安全事件發生時，依照主管機關訂定之資通安全事件通報作業規範，訂定通報處理程序、流程與作業例如通報時限與方式及通報項目。同時，應就資通安全事件相關單位之協調溝通包含組織內與組織外的單位例如政府執法單位、應變處理涉入之人員指派與應變處理的溝通協調所應遵循的程序與流程
- 擬定資通安全事件應處與通報計畫之定期演練計畫，以驗證防護措施有效性，並做為持續改善資通安全成熟度之參考

十一、 資通安全情資之評估及因應機制（Cybersecurity Threat Intelligence Evaluation and Response）

背景說明

5G 系統架構因採網路功能軟體化與虛擬化，建置時將大量使用資通訊科技於網路系統之實作，並開放網路功能和系統的介面，形成 5G 系統設置的開放性、彈性與整合性。同時也增加 5G 系統之資通安全威脅，且威脅之面向更為多元，資通安全情資需考量 5G 系統本身的威脅，以及所使用之各種資訊技術與通訊技術所可能帶來的威脅，據此建立資通安全威脅情資之評估及因應的機制。

得標者應擬定資通安全威脅情資程序（Cyber Threat Intelligence Cycle），其包含訂定所欲蒐集之情資、情資來源、情資分析，及情資結果分享與評估。情資來源應涵蓋多個來源，例如透過建立共享機制、同業間的聯繫、供應商發布之安全通告等，即時掌握情資；針對所蒐集情資，進行情資分析應有一套嚴謹思維與方法，採用可靠的分析技術以確保能夠有效識別和管理所蒐集情資資訊裡可能的偏差與不確定內容，且情資評估分析的結果，需依照情資因應機制決定其處理方式。

自述重點

得標者應參酌上述背景說明，扣合第二項「核心業務及其重要性」、第三項「資通安全維護範圍」及第八項「資通安全風險評估」以訂定資通安全情資之評估及因應機制。

得標者之資通安全情資之評估及因應機制應考量以下面向：

- 擬定資通安全威脅情資程序，訂定情資蒐集種類、情資來源、情資分析、情資分享、因應機制等

- 於評估情資，應參酌第二項、第三項之自述內容，掌握情資是否涉及核心業務與其影響範圍

十二、 資通系統或服務委外辦理之管理措施（The Management of Outsourcing）

背景說明

5G 系統架構的設計理念是以能夠彈性並快速支援未來各種可能的新興應用服務及其設置型態為核心，尤其隨著 5G 系統服務逐步走向開放式架構，得標者所建置之 5G 系統例如軟體或是服務可能委外辦理或由第三方供應商提供，對於其開發與管理之供應鏈及相關人員，必須要有相當之掌握包含了解影響產品或服務安全級別的元件或軟體之來源（Origin）及產品開發或供應之上下鏈結的生態系，以及產品和服務之維護、更新與修復的透明度，以降低並能管控可能潛在的資通安全風險。得標者應就 5G 系統如有資訊技術或通訊技術及產品包含硬體、軟體、網路功能、系統等訂定委外辦理的管理辦法與機制。

自述重點

得標者應參酌上述背景說明，並扣合第二項「核心業務及其重要性」、第三項「行動寬頻系統資通安全維護範圍」及第八項「資通安全風險評估」，評估委外辦理可能涉及之核心業務與風險，訂定委外辦理管理措施。

得標者之資通系統或服務委外辦理之管理措施應考量以下面向：

- 訂定委外辦理管理辦法與機制，包含委外需求評估需考量可能涉及之核心業務與風險；委外服務提供商之選擇應掌握其資通安全

管理能力；對於涉及系統開發與管理之供應鏈與相關人員，必須要有相當之掌握包含了解影響產品或服務安全級別的元件和軟體的來源與開發供應者之上下鏈結的生態系，以及產品和服務之維護、更新和修復的透明度

十三、 所屬人員辦理業務涉及資通安全事項之考核機制（Performance Evaluation of Personnel with Job Assignment Involved 5G Security）

背景說明

得標者應針對 5G 系統資通安全維護計畫施行範圍內之相關人員，包含 5G 業務之所屬人員及服務委外機構如有涉及 5G 系統資通安全維護事項，應訂定契合資通安全維護政策與目標之考核機制，例如資通安全維護措施之執行績效、資通安全事件通報與應變績效，以完善 5G 系統資通安全維護與持續精進。

自述重點

得標者應參酌上述背景說明，並扣合第一項「資通安全政策及目標」、第二項「核心業務及其重要性」及第三項「行動寬頻系統資通安全維護範圍」，訂定所屬人員辦理業務涉及資通安全事項之考核機制。

得標者之所屬人員資通安全考核機制應考量以下面向：

- 於參酌資通安全政策及目標，訂定資通安全績效指標，激勵所屬人員達成資通安全之目標

- 於所屬人員考核績效之回饋，如遇未達資通安全目標者，應依分析其原因並作為持續改善之參考依據，且應將該項未達標之風險納入評估以調整防護措施

十四、 資通安全維護計畫與實施情形之持續精進及績效管理機制（Continual Improvement and Review of 5G Network Protection Plan）

背景說明

得標者為確保所訂定之 5G 系統資通安全防護計畫之內容能有效保障 5G 系統、服務及營運之資通安全，確保用戶資料安全與保護用戶隱私，得標者應針對資通安全維護計畫實施情形，建立持續精進程序與績效管理機制，藉以提升資通安全治理成熟度，且得標者所設置之 5G 系統在面對層出不窮、與日俱增之各種潛在威脅、風險及攻擊時能夠持續不斷檢視與改善弱點、降低風險並維持資通安全管理及防護措施有效運作。

自述重點

得標者應針對資通安全維護計畫各項防護措施及實施情形，自述持續精進程序與績效管理制度，包括資通安全維護計畫與實施結果之績效管理審查以及稽核機制。

得標者之持續精進及管理機制應考量以下面向：

- 資通安全維護計畫實施情形的績效管理，應包含定期稽核與擬定可行有效的稽核方案，以及召開資通安全管理績效審查會議，定期檢討資通安全維護計畫所訂定之措施及其實施情形，是否符合計畫目標及內容

- 如有資通安全績效未達目標或有待改善項目者，應提出改善措施並追蹤後續改善績效，以確保 5G 系統資通安全維護計畫之有效實施及所採用之防護措施的有效性
- 資通安全維護計畫實施情形的績效管理應持續進行，以精進防護措施並確保整個計畫執行之適切性與有效性

十五、 資通安全偵測與防護之建置及執行方案（含資通安全防護架構、防禦縱深及其建置時程）（Implementation Plan for Detection and Protection（Including Architecture, Defense In-Depth Measures, and the Timetable））

背景說明

得標者依據第一項至第十四項之自述內容，提出具體、周全、可行的建置與執行方案，也就是提出實施計畫（Implementation Plan）確保在事業計畫書所規劃建置之 5G 系統會是安全、可靠且具強韌性。實施計畫之內容，第一、應提出整體 5G 系統資通安全防護架構與建置方案，其中需針對 5G 系統四大區塊各自之資通安全防護架構及其防護之實施提出規劃與具體解決方案，以及整體網路之整合防護計畫。第二、對於在各區塊用來實作資通安全偵測與防禦所建置之各種資通訊設備與安全防護系統，亦須說明防護其安全之措施，以確保這些建置與設施亦是安全、可靠的。第三、對於執行 5G 系統資通安全防護計畫之建置與實施計畫，應說明整體資通安全管理制度、流程、專責之資通安全組織、其轄下之資通安全執行長及所有專職人員的配置、執掌與分工，及建置時程等，以確保達成本計畫所設定之政策與目標。

自述重點

得標者應參酌上述背景說明，並依據第一項至第十四項之自述內容，敘明 5G 系統整體與四大區塊各自需建置之資通安全偵測與防禦之執行方案。

得標者之實施計畫應考量以下面向：

- 整體 5G 系統資通安全防護架構
- 5G 系統所含之四大區塊各自的資通安全防護架構及其建置與執行方案
- 整體網路之整合防護方案
- 對於在各區塊用來實作資通安全偵測與防禦所建置之各種資通訊設備與安全防護系統，說明防護其安全之措施，以確保這些建置與設施亦是安全、可靠的
- 對於所提出之建置與實施計畫，應說明整體資通安全管理制度、流程、專責之資通安全組織，以及其轄下之資通安全執行長及所有專職人員的配置、執掌與分工
- 建置時程
- 提出可驗證所提之建置與執行方案執行成效之方法與機制

十六、 執行前述執行方案所蒐集、儲存、處理及利用用戶資料之安全保護措施（Security Measures for Subscriber Data Protection in terms of Collection, Storage, Process and Use）

背景說明

5G 系統架構以能夠彈性並快速支援未來各種可能的新興應用服務為核

心，得標者在建立安全可靠具強韌性之 5G 服務環境時，除前述資通安全議題外，應確保用戶隱私及資料之安全保護。因此，包含網路管理、服務提供、營運管理及資通安全防護目的，得標者於用戶相關資料之蒐集、儲存、處理及利用應提出用戶隱私及資料保護政策與措施並定期檢視執行績效與妥適性。

自述重點

得標者應參酌上述背景說明，及我國個人資料保護法、個人資料保護法施行細則等相關法規，於網路管理、服務提供、營運管理及資通安全防護等目的作業下，如有用戶網路與服務使用相關資料之蒐集、儲存、處理及利用，應提出用戶隱私及資料保護政策與措施，以及定期檢視執行績效與妥適性。

得標者之於各種營運目的對用戶隱私及資料保護應考量以下面向：

- 於網路管理、服務提供、營運管理及資通安全防護等目的作業下，對用戶網路與服務使用進行資料之蒐集、儲存、處理及利用之用戶隱私及資料保護政策與措施
- 於合作之第三方服務提供商如有網路與服務使用進行資料收集及資料分享，應提出用戶隱私及資料保護政策與措施，並確保執行方案的透明
- 定期檢視執行績效與妥適性方案

十七、 通過資通安全管理驗證之執行方案（Formal Certification of Cybersecurity Management）

背景說明

建立安全可靠之 5G 系統與服務環境為得標者之關鍵任務，為落實其資通安全維護計畫之自述內容，應提出資通安全防護措施之管理驗證執行方案，以確保於制度面與管理面等程序落實資通安全政策與達成資通安全目標，例如通報與應變機制、5G 系統之軟體更新與部署等，以及 5G 資通安全防護措施之持續精進。

自述重點

得標者應參酌上述背景說明，擬定 5G 系統資通安全管理驗證之執行方案，內容應具體、可驗證並扣合第一項至第十六項之自述內容，且應定期由第三方公正單位稽核得標者之執行成效，以確保於制度面與管理面等程序落實資通安全政策與達成資通安全目標。

得標者在擬定通過資通安全管理驗證之執行方案時，應考量以下面向：

- 於第一項至第十六項自述內容框列驗證項目與範圍
- 擬定驗證執行方案，包含時程、內部驗證機制與第三方驗證機制
- 擬定缺失改善管理辦法

肆、相關法規及參考文件

1. 電信法
2. 行動寬頻業務管理規則
3. 資通安全管理法
4. 資通安全管理法施行細則
5. 電信管理法