

需求說明書

一、採購案名：113 年行動寬頻專網資訊平臺虛擬主機採購案（以下簡稱本案）

二、預算金額：新臺幣 130 萬元（含稅）

三、採購目的

為執行數位發展部數位產業署「行動寬頻專用電信網路服務推動與管理計畫」相關工作之順暢發展，將建置 5G 專頻專網資訊網站及 5G 專頻專網管理系統，並持續維護、更新與優化相關功能，提供 5G 專頻專網申請資訊、5G 產業現況、趨勢及成果展示、電子化申請作業、基地臺資訊、電波干擾資料庫、案件管理、相關統計報表等功能，促進產業數位轉型與升級，為提升網站運作之順暢，本案將採購虛擬主機器（Virtual Machine, VM）資源，提供執行運作空間、維運防護之效能，俾利專網資訊平台之推動。

四、需求說明

（一）專案目標

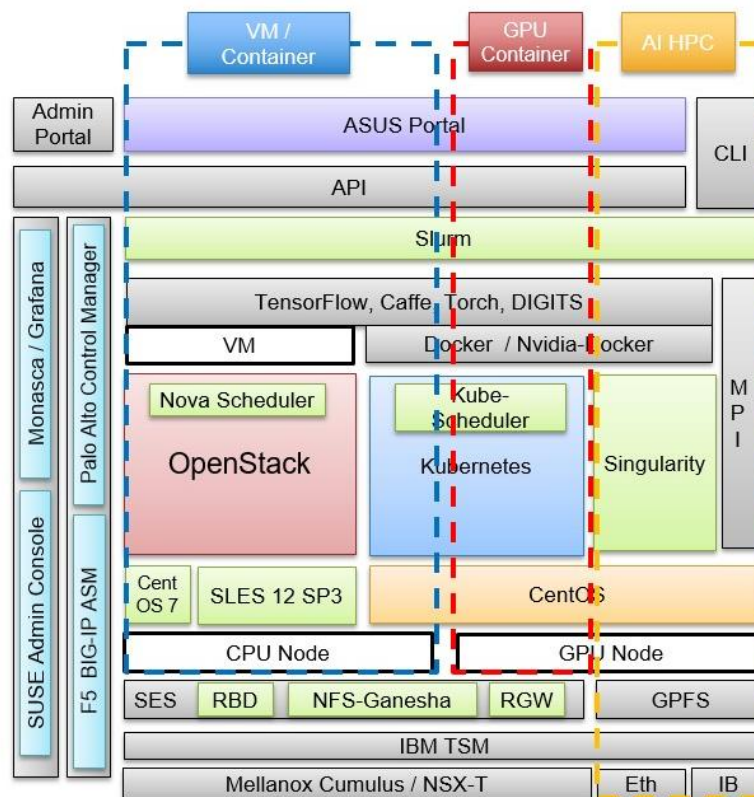
本案需求為建置並持續維護更新行動寬頻專網資訊平臺(內容包含 5G 專頻專網申請資訊、5G 產業現況、趨勢及成果展示等)、建置並持續維護優化 5G 專頻專網管理系統，並與數位部介接，建立備份備援機制，提供隱定、高效率、高可用率、自動化管理、監測、紀錄、通報，因此需租賃虛擬伺服器之空間同時建立安全管控機制以及專業資訊人員維護、即時障礙排除及客服人員等，並符合政府之資通安全、無障礙網頁規範及個人資料保護等相關規定。

（二）專案範圍

提供本專案所需開發環境建置與部署，包含虛擬主機、安全性、與稽核管理、文件、其他等。

需求說明書

1. 架構示意圖：



2. 網路管理環境：

除提供本專案使用之網路環境外，並預先規劃專案後續使用。

3. 單元虛擬主機：

專案需求網站主機 2 臺，附件主機 1 臺，資料庫主機 1 臺，管理平臺主機 1 臺，備份備援主機 1 臺，此 6 臺作業系統使用 Windows Server 2019 Std 版本。相關軟硬體規格詳下表一。

4. 稽核管理：

備稽核紀錄保存至少六個月以上。

(三) 專案需求時間

提供本專案所需開發環境建置與部署應於決標日起至 113 年 12 月 31 日 24 時止。

(四) 專案需求

針對現有開發人員需求，進行環境部署，並提供後續擴展可能性。建置環境單元虛擬主機需求。

表 1 租賃軟/硬體設備需求與規格

需求說明書

編號	項目	品名規格	數量
1	網站主機	CPU 至少 4Vcode	2
		記憶體至少 16GB	
		儲存空間至少 200GB	
		Windows 2019 std 作業系統以上	
		需安裝：1.net framework4.8 以上、2.IIS10 以上	
2	附件主機	CPU 至少 4Vcode	1
		記憶體至少 16GB	
		儲存空間至少 400GB	
		Windows 2019 std 作業系統以上	
		需安裝：1.net framework4.8 以上、2. IIS 10.0 以上、3.open office4.1.2 以上、4.Libre Office7.3.4.2 以上	
3	資料庫主機	CPU 至少 4Vcode	1
		記憶體至少 16GB	
		儲存空間至少 300GB	
		Windows 2019 std 作業系統以上	
		SQL Server 2019 以上	
4	管理主機	CPU 至少 4Vcode	1
		記憶體至少 8GB	
		儲存空間至少 200GB	
		Windows 2019 std 作業系統以上	
5	備份備援主機	CPU 至少 4Vcode	1
		記憶體至少 16GB	
		儲存空間至少 600GB	
		Windows 2019 std 作業系統以上	
		SQL Server 2019 以上	

(五) 安全性需求

1. 在本中心提供之軟硬體環境下，建置及維護資通安全防护措施中級相關措施，如附件一資通系統防護基準所示。
2. 提供穩定之網站資料傳輸流量。
3. 提供基礎負載平衡設備。
4. 提供防火牆、應用程式防火牆（WAF）至少 25 Mbps、入侵偵測機制（IDS）、具有入侵防禦機制（IPS）等符合資安機制之服務。
5. （SOC）24 小時網路監控及通報機制。
6. 提供備份備援環境架構，並滿足本案服務水準，本案復原資料目標（RPO）24 小時，復原時間目標（RTO）4 小時，最大可容忍中斷時間（MTPD）4 小時。
7. 所使用到 Windows 或 Linux 作業系統及相關資料庫軟體，需具備合法使用授權。

需求說明書

(六) 稽核管理需求

1. 機房或雲端服務須通過 ISO27001 等國際資安標準驗證，並設有安全保護措施（例如門禁管理、不斷電（UPS）系統、空調設備、消防設備等，機房各項安全措施是否定期檢查及維護，機房 24 小時操作人員輪值，並具有資訊安全防護中心。
2. 配合各項維運或稽核作業提供及佐證資料，如：營運工作報告、實際使用時間證明文件、技術支援紀錄、系統弱點掃描暨修補報告（一年二次，按本專案時程為一次）。

(七) 文件管理需求

1. 環境建置狀態報告
2. 環境建置基本操作手冊
3. 平臺操作手冊
4. 資源建置清冊

五、履約期限

☐ 應於 112 年○月○日以前完成。

☐ 應於決標之日起○日曆天/工作天完成。

☒ 其他：自決標之日起至 113 年 12 月 31 日止。

六、履約期程及交付項目表（以下簡稱表 2）

項次	履約期限	交付項目	交付格式
1	自決標日起 7 個工作天	1. 工作計畫書： 專案管理工作規劃（專案範圍、工作項目概述、專案組織、專案時程、風險管理、溝通計畫、經費規劃等） 2. 保密同意書	<input checked="" type="checkbox"/> 工作計畫書：電子檔 1 式 1 份 <input checked="" type="checkbox"/> 保密同意書：紙本 1 式 3 份
2	自決標日起 15 個工作天	1. 環境建置狀態報告（建置完成後的軟硬體架構、網段、防火牆狀態等資訊） 2. 環境建置基本操作手冊（環境建置的作業程序、緊急還原的程序） 3. 平臺操作手冊（平台業者給租戶的管理工具操作手冊，如設定防火牆規則、查詢使用狀態等。） 4. 資源建置清冊（使用的虛擬機資源資產清冊）	<input checked="" type="checkbox"/> 電子檔 1 式 1 份
3	113 年 12 月 5 日	1. 決標日起至 11 月營運工作報告（如平台監控到的流量或資源使用情形資訊，有無特殊事件處理的紀錄等）	<input checked="" type="checkbox"/> 電子檔 1 式 1 份

需求說明書

		2. 決標日起至 11 月實際使用時間證明文件（租賃時間使用證明） 3. 決標日起至 11 月技術支援紀錄（叫修或是技術人員協助處理的工作紀錄） 4. 系統弱點掃描暨修補報告（作業系層之弱點掃描報告及修補紀錄一次）	
--	--	---	--

七、履約地點

- ☐ 本中心高雄本部（高雄市路竹區路科一路 3 號）
- ☐ 本中心新北辦公室（新北市板橋區遠東路 1 號 3 樓）
- ☒ 其他指定場所：本中心指定場所。

八、驗收

(一) 數量及規格點收：

1. 廠商交付之採購標的須齊全（包含各原廠標準出貨時所附配件與使用手冊），應符合契約規定，無減少或減失價值或不適於通常或約定使用之瑕疵，且為全新未經拆封使用，並保留原製造廠商出貨時之完整包裝及貼封全新品（所有標的相關零配件及連接線亦同）。
2. 採購標的如廠商須先拆封測試者，須經本中心同意後才能進行拆封，拆封時亦須會同本中心人員。
3. 廠商交付採購標的後，經本中心初步數量、規格點收後，其中任何一項數量、規格不符或非新品，視同不合格。

(二) 系統測試：

1. 依「四、需求說明」中相關需求及確認後之需求內容進行測試，均能正常執行且正常運作於相關軟硬體設備與系統，並產出相關測試報告且功能測試合格後，本中心始認可廠商所提供之軟硬體設備。

(三) 其他：

1. 採購金額未達新臺幣 150 萬元採購案，廠商各期履約交付，應於履約標的預定完成履約日前或完成履約當日，將完成履約日期以書面通知(含電子郵件通知)本中心辦理驗收。廠商如以電子郵件通知，須通知本中心需求單位並副知採購單位承辦人。
2. 依本中心驗收規定辦理。

需求說明書

九、付款條件

☐ 一次付清：廠商於完成表 2 項次○至項次○所有履約交付項目，並經本中心驗收合格，且無待解決事項後，本中心一次付清決標價金總額。

☒ 分期付款：

第一期：廠商於完成表 2 項次 1 及項次 2 履約交付項目，並經本中心驗收合格後，且無待解決事項後，撥付決標價金總額 50%。

第二期：廠商於完成表 2 項次 3 履約交付項目，並經本中心驗收合格後，以及提供 12 月營運工作報告、實際使用時間證明文件、技術支援紀錄，且無待解決事項後，撥付決標價金總額 50%。

☐ 其他：

十、保固及維護需求

☒ 無

十一、資安需求

(一) 本案資通系統籌獲

1. ☐ 涉及本中心（或委託/補助機關）之核心資通系統（本款未勾選者，為非核心資通系統）
2. 本案資通系統之防護需求等級：（請購單位應依中心「資通作業委外管理作業程序」規定填妥「安全等級評估表」（IS-2MN08-02）用以評估資通系統防護需求等級，並就下列等級擇一勾選）

☐ 高

☒ 中

☐ 普

(二) 資安法需求

依照資通安全管理法施行細則之要求，廠商須配合事項如下：

1. 得標廠商辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 得標廠商應配置充足且經適當之資格訓練，擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員至少 1 名。
3. 本採購案不得轉包，得標廠商應依據契約書辦理。
4. 本案得標廠商☒不得分包；
5. 本採購案為☒客製化資通系統開發，得標廠商應提供本案資通系統之下列安全性檢測證明：

☒ 弱點掃描

☐ 滲透測試

☐ 源碼掃描

需求說明書

6. 得標廠商執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知本中心及採行補救措施。如因可歸責廠商之事由致本中心受有損害，廠商應就本中心所受損害負賠償之責。
7. 得標廠商應於委託關係終止或解除時，返還、移交、刪除或銷毀履行合約而持有之資料，並留存處理紀錄以供本中心查核。
8. 得標廠商應說明採取之其他資通安全相關維護措施。
9. 得標廠商應配合本中心以稽核或其他適當方式確認受託業務之執行情形。
10. 本採購案包含■客製化資通系統開發，廠商須配合下列事項：
 - (1) 得標廠商涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供開發者之相關證明文件（可追溯性）。
 - (2) 本案不得使用大陸地區開發之網頁元件。
11. ☐本採購案涉及國家機密，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

(三)其他資訊安全需求

1. 廠商需遵循資通安全管理法及相關法規、規範要求，並配合產業署指定之必要控制措施及資通系統防護基準辦理資通安全管理作業。
2. 建置及維護資通安全防護措施中級相關措施。
3. 建置及維護備份備援機制。
4. 建置及維護高可用性架構。
5. 建置及維護網站監控及通報機制。
6. 建置及維護網站安全防篡改機制。
7. 建置及維護個資保護措施，並提供網站上稿內容個資偵測及提醒功能。
8. 整合無效連結檢測服務，定期檢核網站連結、附件、服務有效性，以強化服務品質。
9. 整合 GA4、使用者瀏覽紀錄、網站維運、搜尋、點擊等多樣使用者行為分析數據，提供網站維運及優化參考。
10. 提供弱點掃描及相關弱點修正服務（如中（含）等級以上須辦理弱點修正服務）。
11. 本案交付之程式源碼須保證確保無惡意程式碼（如病毒、蠕蟲、特洛伊木馬、間諜軟體等）、隱密通道（covert channel）及 2021 年版 OWASP（The Open Web Application Security Project）前十大安全漏洞，並提供資安弱點掃描暨修補報告及原始碼檢測暨修補報告。
12. 廠商進行弱點掃描所使用之網站安全檢測工具須取得合法版權。倘若廠商採委外資安廠商進行檢測者，需提供委外資安廠商使用合法版權切結或其他具有效之證明文件。安全檢測所需之環境（含軟、硬體）及版權等衍生費用均由廠商自行吸收。
13. 得標廠商對資通系統之開發維運環境應具備資通安全管理措施及防護。
14. 本案於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。
15. 廠商須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。

需求說明書

16. 廠商應確實執行組態管理（Configuration Management），以確保系統之完整性及一致性，以符合對系統品質及資通安全的要求。

十二、履約保證金

☒ 無。

☐ 廠商於決標日起 14 日曆天內應繳納履約保證金，金額為合約金額 10%。

十三、保固保證金

☒ 無。

☐ 廠商於驗收合格日起 14 日曆天內應繳納保固保證金，金額為合約金額 3%。

十四、投標廠商資格文件

☒ 廠商設立或登記證明文件。

十五、採購方式

☒ 最低報價採購

☐ 審查評選採購

☐ 指定廠商採購

十六、聯絡方式

（一）請購單位：黃先生

電子信箱：Kelvin.Huang@ttc.org.tw/連絡電話：(02)2331-5136 分機 103

（二）採購單位：陳先生

電子信箱：Eric.Chen@ttc.org.tw/連絡電話：(02)8953-5956

需求說明書

附件一 資通系統防護基準

系統防護需求 分級		高	中	普
控制措施				
構面	措施內容			
存取控制	帳號管理	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、應依機關規定之情況及條件，使用資通系統。 四、監控資通系統帳號，如發現帳號違常使用時回報管理者。 五、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、遠端存取之來源應為機關已預先定義及管理之存取控制點。 二、等級「普」之所有控制措施。	一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。 二、使用者之權限檢查作業應於	

需求說明書

			<p>伺服器端完成。</p> <p>三、應監控遠端存取機關內部網段或資通系統後臺之連線。</p> <p>四、應採用加密機制。</p>
事件日誌與可歸責性	記錄事件	<p>一、應定期審查機關所保留資通系統產生之日誌。</p> <p>二、等級「普」之所有控制措施。</p>	<p>一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。</p> <p>二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。</p> <p>三、應記錄資通系統管理者帳號所執行之各項功能。</p>
	日誌紀錄內容	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。	
	日誌處理失效之回應	<p>一、機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。</p> <p>二、等級「中」及「普」之所有控制措施。</p>	資通系統於日誌處理失效時，應採取適當之行動。
	時戳及校時	<p>一、系統內部時鐘應定期與基準時間源進行同步。</p> <p>二、等級「普」之所有控制措施。</p>	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調

需求說明書

				時間(UTC)或格林威治標準時間(GMT)。
	日誌資訊之保護	一、定期備份日誌至原系統外之其他實體系統。 二、等級「中」之所有控制措施。	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對日誌之存取管理，僅限於有權限之使用者。
營運持續計畫	系統備份	一、應將備份還原，作為營運持續計畫測試之一部分。 二、應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 三、等級「中」之所有控制措施。	一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。
	系統備援	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。		無要求。
	內部使用者之識別與鑑別	一、對資通系統之存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	

需求說明書

識別與鑑別	身分驗證管理	<ul style="list-style-type: none">一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。三、等級「普」之所有控制措施。	<ul style="list-style-type: none">一、使用預設密碼登入系統時，應於登入後要求立即變更。二、身分驗證相關資訊不以明文傳輸。三、具備帳戶鎖定
-------	--------	--	---

需求說明書

			<p>機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。</p> <p>四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。</p> <p>五、密碼變更時，至少不可以與前三次使用過之密碼相同。</p> <p>六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。</p>
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	
	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性）進行確認。	
	系統發展生命週期設計階段	<p>一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。</p> <p>二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。</p>	無要求。
	系統發展生命週期開	一、執行「源碼掃描」安全檢測。	<p>一、應針對安全需求實作必要控制措施。</p> <p>二、應注意避免軟體常見漏洞及實作必</p>

需求說明書

	發階段	二、系統應具備發生嚴重錯誤時之通知機制。 三、等級「中」及「普」之所有控制措施。	要控制措施。 三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	
	系統發展生命週期測試階段	一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。	執行「弱點掃描」安全檢測。	
	系統發展生命週期部署與維運階段	一、於系統發展生命週期之維運階段，應執行版本控制與變更管理。 二、等級「普」之所有控制措施。	一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二、資通系統不使用預設密碼。	
	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
	獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
	系統文件	應儲存與管理系統發展生命週期之相關文件。		
系統與通訊保護	傳輸之機密性與完整性	一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、使用公開、國際機構驗證且未遭破解之演算法。 三、支援演算法最大。	無要求。	無要求。

財團法人電信技術中心

(112.2.9 版本)

需求說明書

		<p>長度金鑰。</p> <p>四、加密金鑰或憑證應定期更換。</p> <p>五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。</p>		
	資料儲存之安全	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	無要求。	無要求。
系統與資訊完	漏洞修復	<p>一、定期確認資通系統相關漏洞修復之狀態。</p> <p>二、等級「普」之所有控制措施。</p>		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
	資通系統監控	<p>一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。</p> <p>二、等級「中」之所有控制措施。</p>	<p>一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。</p> <p>二、等級「普」之所有控制措施。</p>	發現資通系統有被入侵跡象時，應通報機關特定人員。

需求說明書

整性	軟體及 資訊完 整性	一、應定期執行軟體與 資 訊 完 整 性 檢 查。 二、等級「中」之所有 控制措施。	一、使用完整性驗證 工具，以偵測未 授權變更特定軟 體及資訊。 二、使用者輸入資料 合法性檢查應置 放於應用系統 伺服器端。 三、發現違反完整性 時，資通系統應 實施機關指定之 安全保 護措施。	無要求。
----	------------------	--	---	------