附件 4 「Infrastructure 基礎設施建置與維運管理」RFP 資安需求範例

○○年度

「◯◯網路基礎設施建置與維運服務案」計畫

建議書徵求說明書(範例)

○○○○○○

中華民國○○ 年○ 月

目　次

1. 專案概述

1.1 專案名稱

本專案名稱為「○○網路基礎設施建置與維運管理服務案」(以下簡稱本專案)

1.2 專案目標

- 建立政府機關可靠、可擴充及安全的網路架構。
- 在簡化網路管理、程序及成本的前提下，執行高效能與效率的網路架構。
- 在最小化管理原則下，由投標廠商提供網路管理功能。
- 達成本專案服務水準需求。

1.3 專案範圍

(依各機關專案需求撰述專案範圍)

1.4 專案時程

(依各機關專案需求撰述專案時程)

2. 系統環境現況說明

(說明政府機關專案建置環境，包含資產、設備、地點、人員、政策、程序及其他正在進行的相關專案等)

3. 專案建置需求

3.1 專案整體需求

(依各機關專案敘述 WAN、LAN 及遠端存取等整體架構規劃需求)

3.2 基礎環境需求

3.2.1 投標廠商背景資格限制

- 廠商不得為大陸地區廠商或第三地區含陸資成分廠商。
- 分包廠商亦不得為大陸地區廠商與或第三地區含陸資成分廠商。
- 不得將開發工作移至本國以外地區或其指定排除之國家。
- 本專案廠商宜通過專業之認證，如 ISO 27001 及 CNS 27001 等。

3.2.2 實體與環境安全管理需求

- 設備安全：委外所需存取或委外作業人員攜入之資訊設備，包含個人電腦、個人數位助理、行動電話、智慧卡及所有形式的儲存設備等，於機關場所內使用任何資訊處理設備均應受管理。
- 門禁管理：委外作業人員進出本機關均應配帶臨時員工證件，非經許可不得至工作場所以外地區活動。

3.3 建置維護需求

3.3.1 實體環境建置需求

(依政府專案需求說明各項實體環境與相關設施建置需求，如機房環境、消防、監控、空調、電力及網路等。)

3.3.2 網路建置需求

(依政府機關專案需求敘述網路之規劃、配置及其他網路重要系統及設備需

求說明，包含 DNS、DHCP、無線網路、個人電腦、伺服器群、防火牆及路由器等。)

3.3.3 外部整合需求

(政府機關如有現有系統、設備須與專案系統及設備進行整合時，須說明整合之標的、範圍及需求。)

3.3.4 維護管理需求

(包含政府機關既有系統、設備，以及本專案所新增之各項軟硬體系統、環境設施及其他設備，應說明建置、保固及後續維護期程，如採 1 年建置【OO 年度】、2 年【OO~OO 年度】保固及 3 年【OO~OO 年度】維護方式辦理，保固期間除硬體設備保固外，並包含系統設備之授權與版本更新服務，廠商須於建議書內說明保固項目、保固內容及保固實施方式，並將後續維護費用納入契約價金計算。)

3.3.5 遠端存取服務

投標廠商應依本專案需求提供安全的遠端存取服務，以利遠端使用者透過公眾網路安全的連接本機關公務網路，並應說明其配置、規劃、運作及管理方式，同時符合相關工業或網路安全標準。

3.4 安全服務需求

3.4.1 網路安全防護需求

(投標廠商應規劃、配置及提供網路安全服務，以利本機關於履約期間各種實體與邏輯設備能安全的連接公共網路，包含網路防火牆、應用程式防火牆、入侵偵測系統及其他相關資安防護設備。)

3.4.2 網路管理

- 網路系統管理

– 網路系統管理與狀況排除(如故障、錯誤、傳輸效率問題及變更管理)。

– 頻寬管理。

– 協定使用統計。

– 配合本機關網路服務與相關架構執行各項作業活動。

- 網路設定管理

  管理本專案相關網路設備及其設定。

3.4.3 網路安全服務需求

- 漏洞修補更新需求：投標廠商於本專案所提供各項軟硬體設備，在履約期間及本機關網路架構下，應能達成自動即時更新修補漏洞目標，有效防止漏洞、弱點所造成危害，如相關漏洞、弱點無法自動即時更新，亦應提出替代方案，並說明改善方式及期程經本機關審查通過。

- 資訊安全改善建議：投標廠商應隨時研究與注意最新資訊安全現況，遇有系統或設備原廠重大系統安全漏洞更新發布或外界重大安全事件發生，或接獲修正通知時，應向本機關發布資訊安全改善建議，並協助辦理防護及修正、修補工作。

- 滲透測試服務

  – 廠商每年辦理滲透測試服務 1 次，測試標的(不超過 5 項)由本機關指定，並於作業◯日前通知廠商，廠商於提出滲透測試服務計畫書報經本機關同意後施行。

  – 廠商於滲透測試服務辦理完畢後◯日內提出書面報告，除說明現有系統弱點及安全狀況，並提供具體改善方法與建議。

– 本機關依據前述改善方法與建議自行完成改善作業後，廠商應配合本機關要求進行檢測，以確認相關風險改善無誤。

• 弱點掃描服務

– 廠商每年應針對本機關各項網路設備及伺服器辦理弱點掃描服務 1 次，掃描標的(不超過 20 項)由本機關指定，並於作業◯日前通知廠商，完成後◯日內廠商應提出書面報告，報告內應敘明電腦名稱、IP 位址、弱點數量、等級，以及具體改善方法與建議。

– 本機關依據前述報告自行完成弱點改善作業後，廠商應配合本機關要求進行第 2 次複掃，掃描標的由本機關指定，並於作業◯日前通知廠商，完成後◯日內廠商應提出書面報告(內容同前次報告)。

3.4.4 事件緊急應變處理與鑑識需求

廠商應根據日常監控與狀況，主動分析是否屬安全事件，並依照行政院國家資通安全會報相關通報應變標準啟動對應之處理程序，協助本機關執行相關處理程序。

對於本機關發生之重大資安事件，廠商應提供 7 天 X 24 小時全年無休之緊急應變處理服務，在本機關要求下於規定時限內指派支援人員至本機關進行事件緊急應變協同處理。(廠商人員進場、退場時機及報告及產生文件由廠商於服務水準協議書提出)。

本機關判斷須到場進行緊急應變處理時，廠商需於接獲通報時間起算 6 小時內到達本機關，並於事件處理完畢 3 個工作天內將處理經過作成報告(涵蓋防護提升作法及相關改善建議)交付本機關，廠商對本機關就本項履約服務辦理下列事項：

• 於接獲通報時間起 24 小時內完成本機關資安事件之初步緊急應變處理。

- 接獲通報時間起 72 小時內完成下列項目：
  - 協助本機關針對網路及系統安全入侵行為進行事件之分析、封鎖、圍堵及根除(含提供相關移除程式)。
  - 提出處理事件過程中所必要之系統備份及復原建議方案。
- 廠商參予本機關執行緊急應變服務時，應配合以下事項：
  - 廠商應於接獲通報時間起算 6 小時內配合本機關成立緊急應變小組協同處理，並隨時提供最新處理資訊。
  - 廠商參與應變處理人員負有保密義務，不得公開散佈或傳閱應變過程中所有執行之內容或文件。
  - 緊急應變過程所產出各項文件資料權利歸屬本機關。
- 本機關認為如有進行數位鑑識必要，廠商應於接獲本機關通知 30 天內，依數位鑑識標準作業程序完成數位鑑識書面報告交付本機關。
- 廠商應於建議書提出數位鑑識團隊成員，具有專業證照、資安事件鑑識經驗及採用工具，同時將數位鑑識管理程序列入作業安全管理計畫內。

3.4.5 資安攻防演練服務

廠商應針對本機關對外提供服務之網路或資訊系統，每年至少辦理資安攻防演練 1 次，演練期間應提供滲透測試服務至少 1 次，測試時間與標的由本機關指定，並於測試前 30 天通知廠商，廠商提出攻防演練計畫後經本機關同意後施行。

廠商於攻防演練辦理完畢後，應提出書面報告，除說明現有系統弱點及安全狀況，並提供本機關整體資安改善方法與建議。

3.4.6 資安稽核需求

本機關基於法令及合約需求，得要求實施定期或不定期稽查，以監督專案內各項安全管理執行情形，且投標廠商負有配合並提供本機關稽查所需相關文件資料之義務。

3.5 教育訓練需求

- 廠商每年須針對專案範圍辦理設備與網路安全教育訓練 1 次(訓練總時數不超過 24 小時)，本機關應於訓練◯日前通知廠商，廠商應於接獲通知◯日內提出教育訓練計畫書(含師資及課程項目)報經本機關同意後施行。
- 訓練所含講師費、訓練教材(含書面資料及電子檔)、教具、上機環境軟體安裝等費用，由廠商負擔或免費提供。

3.6 服務工作報告需求

為了解機關網路安全現況及相關履約執行情形，廠商至少每月提供服務工作報告，俾利做為機關風險分析及營運決策基礎，報表內容至少包含網路管理報表統計、各項設備定期維護紀錄、各項需求服務執行與改善完成情形，以及其他與本案相關之履約佐證資料，同時提供必要改善建議與諮詢服務。

除定期提供服務工作報告外，在發生資安事件或察覺相關異常警訊時，廠商得應本機關要求提供即時報表資料。

本項報表服務除書面資料 1 份外，至少須提供 Word 或 PDF 等格式電子檔。

3.7 專案管理

得標廠商應於決標後◯日內提交專案工作計畫書，經本機關審查通過後，做為工作交付項目並為執行專案之依據，內容應包含對本計畫之執行敘述，含專案管理、組織、人力、分工、職掌、計畫工作項目及時程、查核

點、建構管理、品質管理、需求異動管理及服務水準協議。

3.7.1 專案組織與職掌

3.7.1.1 成立專案小組及分工

- 投標廠商應成立專案小組，其成員包含：專案經理、網路工程師、資安工程師，負責本專案之各項需求規劃、協調、分析、設計、測試及資安維護等工作。
- 本專案參與人員需具資訊安全相關技能，並具有網路相關資安專業證照或其他類似之文件，例如：SSCP 與 CompTIA Security+等。

3.7.1.2 專案小組成員

投標廠商須提供專案小組成員之學經歷、專長、負責本專案之工作項目及內容，並檢附專案小組成員勞、健保等證明文件與資安相關證照。

- 專案小組成員應簽訂保密切結書，必要時得配合接受身家安全調查。
- 專案小組成員不得有非本國籍勞工，若有分包廠商，其成員亦同。

3.7.1.3 專案經理之資安職責

本專案廠商之專案經理應具備良好之協調及資訊專業能力，以掌控本專案之執行進度及成果，並符合本機關需要。

專案經理應負責與本機關承辦人員相關資安業務之協調，同時應推動、協調及督導下列資訊安全管理事項，包含：資訊安全責任之分配與協調、資安政策與規範的遵循、組織成員資安教育訓練、資訊資產保護事項及資訊安全事件之檢討等。

3.7.1.4 專案小組成員異動

專案執行期間，專案小組成員如有異動，得標廠商應於二週前(日曆天，含

異動當天)函請本機關同意，並檢附接替人員相關學經歷、專長、勞健保等相關證明文件以及保密切結書，經本機關審核通過後更換。

本機關對不符本專案執行需要之人員，得要求得標廠商更換，得標廠商應提供適當人選經本機關審核通過後更換，並於兩週內完成人員交接。

3.7.2 交付項目與交付日期

(依各機關專案需求撰述交付項目與交付日期)

3.7.3 建構管理

- 資料管理應包含：紙本資料管理、電子檔資料管理及程式碼資料管理。
- 型態管理應包含：型態項目、建立型態管理環境與型態項目識別方式、型態項目納管與記錄、型態項目版本之建立與發行、已納管型態項目之變更管制、型態管理紀錄留存、型態稽核及基準。

3.7.4 品質管理

除另有規定或經雙方同意外，每月應至少召開專案工作會議 1 次，確實檢討該段期間本專案各項作業進度與目標達成情形、下一段期間預定進度、各方待配合協調應注意及改善事項等事宜，並於會後 3 個工作天內做成會議紀錄，並經本機關審核通過。

本專案各項交付文件內容與產品，應於專案工作會議中提報本機關確認後，再行交付。

得標廠商應依據本專案規定之期限交付工作項目文件與產品，由本機關進行審查作業，審查項目如有不符本專案需求者，得標廠商應於 14 天內完成修正，並提供予本機關複審。

為確保得標廠商依據契約及相關計畫執行本專案之各項工作，本機關得就專案執行之相關事項進行查驗，範圍如下：

- 依據本文件所列之文件交付項目按規劃期程提交，以供本機關審查與簽署。
- 依據本機關專案管理要求，按時執行專案進度報告及專案管理會議，提報專案執行狀況，並回覆本機關之問題與建議。
- 配合本機關要求，提供各項專案執行紀錄文件，例如測試紀錄、異常報告、資源管理、作業程序等。
- 配合本機關要求，接受各項與專案相關之督導。

3.7.5 需求異動管理

請廠商提出需求異動之管理建議。

3.7.6 服務水準協議

- 效率、可用率及安全性規範，如全年系統各項功能，可正常提供使用者之時間百分比，不得低於◯◯%。
- 不中斷服務，如機關發現系統故障致不能運作時，得隨時在服務時間內以電話通知廠商維修，廠商接獲通知後，須於 4 小時內修復完畢。
- 滿意度調查，如機關應每季針對廠商之服務成效，針對使用者執行滿意度調查，其滿意度不得低於◯◯。

3.8 作業安全需求

3.8.1 作業安全管理計畫

投標廠商應依本專案需求提出作業安全管理計畫，內容包含如下：

3.8.1.1 服務範圍

主要在描述服務的時程、服務形態、服務範圍、風險要項、人員權責劃分

及系統資料成長預測等。

3.8.1.2 作業安全項目

- 作業人員職務的區隔。
- 配置、測試及作業程序規劃。
- 由第三者執行查核與驗證相關之配合作業。
- 作業變更管理。
- 服務交付方式。

  各類服務指標完成度、相關文件、軟硬體設備資產、稽核或偵測、驗證報告及資料檔案等。

- 資料被查詢與異動之軌跡紀錄。
- 交付之軟體與硬體元件來源不得為大陸地區。
- 保固維護期間發現漏洞、弱點改善建議與修復方式。
- 委外媒體的處置措施

  委外作業過程中之資料(包含書面與磁性媒體)，妥善的控管與處理；包含可攜式媒體的管理與系統文件的安全。

3.8.1.3 服務驗收或稽核服務之管理程序

3.8.1.4 專案人員應參與機關之資安管理規範與個資法等之教育訓練

3.8.1.5 專案人員籌組與異動時之規劃

例如：安全管理、教育訓練及人員安全查核(含僱用前、僱用中及結束僱用或改變職務)。

3.8.2 服務終止之措施

3.8.3 所有權與智慧財產之保障

- 廠商因履行契約所完成之著作，其著作財產權之全部於著作完成之同時讓與機關，得標廠商放棄行使著作人格權。得標廠商保證對其人員因履行契約所完成之著作，與其人員約定以得標廠商為著作人，享有著作財產權及著作人格權。
- 如使用開源軟體，應依該開源軟體之授權範圍，授權機關利用，並以執行檔及原始碼共同提供之方式交付予機關使用，廠商並應交付開源軟體清單（包含但不限於：開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、開源授權條款標示與全文）。
- 除另有規定外，得標廠商如在契約使用專利品，或專利性履約方法，或涉及著作權時，其有關之專利及著作權益，概由得標廠商依照有關法令規定處理，其費用亦由乙方負擔。

3.8.4 遵循適法性做法

- 遵守各項公務及業務機密保護法規。
- 遵守機關之資安政策與規範。

3.9 其他需求

3.9.1 保固服務

得標廠商於保固期間，當系統異常造成運作中斷或部分無法正常運作時，可歸責於得標廠商者，得標廠商有義務依契約規定，進行異常之排除。

3.9.1.1 後續服務規劃

- 投標廠商應提出日後簽訂軟硬體維護契約相關工作內容之說明(本項依契

約內容而定)。

4. 交付文件與產品

本專案得標廠商需根據建議書徵求文件、契約及得標廠商所提建議書，經本機關認同之各項工作結果，做為本專案之交付項目，本專案交付之文件與產品其所有權及使用權歸屬本機關所有，另因教育訓練及廠商提供獲得之經驗、文件等本機關可自行運用，日後開發各項新增功能與服務項目，毋須經由得標廠商同意，交付項目至少包含下列各項：

4.1 設備軟硬體部分

(依各機關需求詳列所交付之軟硬體清冊及軟體授權證明)

4.2 各項履約文件

5. 驗收

- 廠商履約所供應或完成之標的，應符合本契約規定，無減少或滅失價值或不適於通常或約定使用之瑕疵，廠商所提供設備必須是符合標準規定的生產廠商所製造且為新品，僅限於西元○○○○年 1 月以後出廠，並應於完成履約期限前交付原廠出廠證明(如有裝備序號者，並同時提交序號清冊)。

- 驗收程序：廠商於維護期間，應於每期完成履約標的維護後，依實際履約情形檢附服務工作報告書，內容包含系統設備維護紀錄、滲透測試服務報告及弱點掃描服務報告等相關資料向本機關報驗，本機關應於接獲廠商通知備驗或可得驗收之程序完成後○日內辦理驗收，並做成驗收紀錄。

- 廠商如提供設備應可於原製造廠(或生產國)官方網站取得相關功能及技術規格規範等諸元資料，並以市場流通之通用型號設備為主(如非通用型號或係針對本案開發設計之設備，並應於完成履約期限前交付國內、外公證第三者測試認證書)，並須註明交付設備明確型號及設備型錄並於建議書答標項目內容標示，如未註明則以該系列產品最高等級設備交付。

- 廠商不於本專案契約期限內履約(改正)、拒絕履約(改正)或無法履約(改正)者，本機關得採行下列措施之一：

  – 自行或使第三人履約(改正)，並得向廠商請求償還履約(改正)必要之費用。

  – 終止或解除契約或減少契約價金。

  – 因可歸責於廠商之事由，致履約有瑕疵者，本機關除依前二項規定辦理外，並得請求損害賠償。廠商依契約規定所負之損害賠償責任，僅限於直接損失，並不包含其他任何間接性或衍生性之損失。

6. 建議書製作規定

(依各機關專案需求撰述專案範圍)

7. 評選辦法

(依各機關專案需求撰述專案範圍，並應適時將資安要求列為評選加分項)

7.1 投標廠商限制

- 廠商不得為大陸地區廠商或第三地區含陸資成分廠商。
- 分包廠商亦不得為大陸地區廠商或第三地區含陸資成分廠商。
- 本專案禁止移至本國地區以外國家與地區開發。
- 本專案參加成員禁止非本國國民參加。

7.2 終止評選規定

本機關得因故終止評選事宜，通知投標廠商領回建議書。

7.3 未盡事宜

本專案依據機關委託資訊服務廠商評選及計費辦法與相關法規規定辦理。