附件 6「政府機關資訊安全管理系統(ISMS)顧問輔導」RFP 資安需求範例

○○年度

資訊安全管理系統(ISMS)建置暨認證輔導服務案

建議書徵求說明書(範例)

○○○○○○

中華民國○○ 年○ 月

目　次

表　目　次

1. 專案概述

1.1 專案名稱

「資訊安全管理系統(ISMS)」建置暨認證輔導服務案(以下簡稱本案)。

1.2 專案機關與專案使用者

本案由[機關名稱](以下簡稱本機關)建立，其使用者為本案專案範圍內所有人員，包含正職、約聘、工讀生及第三方人員等。

1.3 專案背景

依行政院國家資通安全會報「政府機關(構)資通安全責任等級分級作業規定」中，訂定本機關為 B 級機關，故按「資通安全責任等級分級辦法」附表 3「資通安全責任等級 B 級之公務機關應辦事項」，本機關應辦理資訊安全管理系統(ISMS)之導入，並於○○年底前通過第三方認證。

1.4 專案目標

藉由資訊安全管理系統(ISMS)之建置，使本機關符合資訊安全驗證標準與國家法規法令要求。

1.5 專案範圍

本案以本機關「○○業務」所涉及之作業為專案範圍，並以專案範圍為驗證範圍(以下簡稱驗證範圍)，得標廠商服務範圍包含：

- 協助驗證範圍改善資訊安全管理機制以符合 ISO27001 規範。
- 協助驗證範圍建立符合資訊安全管理系統之相關政策、規範、程序及紀錄等文件。
- 協助驗證範圍辦理資訊安全管理系統認知與教育訓練等宣導活動。

- 協助驗證範圍辦理 ISO27001 預評與驗證事宜。
- 技術移轉資訊安全管理系統建置能力。

1.6 專案期程

自簽約生效日起，至民國○○年○○月○○日止，完成本機關驗證範圍之資訊安全管理系統(ISMS)建置，通過 ISO27001 資訊安全管理系統認證之評鑑，並提供取得驗證後一年內之後續審查相關輔導。

1.7 專案預算

本案預算金額為新台幣○○○萬元。

2. 現況說明

2.1 組織架構說明

(本段應說明驗證範圍內之組織架構，以組織架構圖表示為佳)

2.2 專案範圍說明

(本段應說明導入範圍內各單位之人數、職務或作業內容等)

3. 專案工作需求

本案「得標廠商」需提供必要之顧問服務，並需符合資訊安全管理系統(ISMS)運作需求及 ISO27001 標準，協助規劃、輔導、建立本機關驗證範圍之資訊安全管理機制，最終協助本機關取得 ISO27001 資訊安全認證。

3.1 專案整體需求

本案應涵蓋以下所列示之所有服務項目。

- 建置資訊安全管理系統(ISMS)
  - 進行資訊安全管理現況分析，提出資訊安全管控差異分析報告，其中應包含改善建議。
  - 協助進行資訊資產分類分級，並建立與實施風險評鑑管理機制，綜合 ISO27001 標準、法規法令及成本效益等因子，提出風險處置計畫與風險決策建議，供本機關訂定可接受風險等級與實施風險處置對策之參考。
  - 於專案期間，提供相關教育訓練課程與移轉本案之工具與知識。
  - 評估本機關現有與資安相關之政策、規範、程序、表單及紀錄等文件，提出需增修之文件清單，並協助文件負責單位將需變更之制度進行調整。
  - 協助建立符合 ISO27001 之資訊安全事件管理程序與重要業務流程之營運持續計畫。
  - 協助建立與實施 ISO27001 所要求之內部稽核機制，包含建立或調整資安內部稽核制度、進行內部稽核教育訓練、實施內部稽核、提出稽核結果並改善建議及協助進行矯正措施。

- 協助本機關通過 ISO 27001 最新管理標準之驗證
  - 協助整理與準備驗證作業之審查文件。
  - 協助本機關取得驗證合格證書。
- 通過認證後一年內協助本機關維運 ISO27001 以通過後續審查
  - 協助本機關更新資訊資產清單。
  - 協助本機關進行風險評鑑與風險處置計畫。
  - 協助本機關進行必要的資安制度調整。
  - 協助本機關進行資訊安全內部稽核與改善。
  - 協助本機關進行外部驗證單位審查作業。
- 繳交計畫成果報告書

  完成本案需求工作後，應繳交計畫成果報告書，其內容包含：(1)專案簡介，(2)專案工作說明，(3)專案推動方式說明，(4)專案執行情形說明，(5)專案建置成效分析及(5)結論與後續執行之建議。

3.2 資通安全需求

3.2.1 廠商資格

為確保資通安全與得標廠商所提供之服務水準，得標廠商應符合下列條件，並於服務建議書專章詳述:

- 凡在政府機關登記合格，無不良紀錄之廠商(檢附設立及登記證明、納稅證明及信用證明)且不得為陸資企業(包含子公司、分公司、獨資或合夥事業及其轉投資事業)。本案服務人員需具有中華民國國籍，不得為外籍勞工或大陸來台人士。

- 本案服務內容將涉及敏感資訊，得標廠商不得轉包或分包予其他廠商執行。
- 投標廠商須具備完善之資訊安全管理制度，通過 ISO 27001 或其他類似驗證，並於專案執行期間持續有效，以保護執行本案所取得之資料。
- (若想知道更多資訊可參考本文「投標廠商背景資格限制」一節)。

3.2.2 資安要求事項

- 得標廠商於因執行本案而取得本機關各項文件與資料，應負保密責任。
- 本案產出之各項文件，屬本機關之智慧財產，非經本機關正式書面同意，不得轉載或引用。
- 為確保本委外專案之資訊安全，得標廠商應於「服務建議書」中提出資安管理計畫，以明確說明得標廠商在專案進行期間將實施之資安管理機制，其內容應包含(但不限於)下列項目：
  - 專案期間將接觸之資訊資產範圍。
  - 資訊資產分類分級與其生命週期各階段之可接受使用原則。
  - 資訊資產所有權與智慧財產權之歸屬原則。
  - 專案人員籌組、資安角色與職責及異動時之規劃。
  - 專案人員於專案期間維持資安認知與持續接受資安管理訓練之規劃。
  - 對專案期間所接觸之資訊保密作為。
  - 於機關所屬場所內工作時將施行之資安作為。
  - 依資訊資產特性，防範異常或未經授權存取之措施。
  - 資通安全事件之管理機制。

– 專案終止之資安措施。

4. 專案管理需求

4.1 專案期程

自簽約生效日起，至民國○○年○○月○○日止，完成本機關驗證範圍之資訊安全管理系統(ISMS)，通過 ISO27001 資訊安全管理認證之評鑑，並提供取得驗證後一年內之後續審查相關輔導。

4.2 專案管理

- 專案進行期間，對於專案進度與品質應建立監控方法，以期有效解決問題與異常狀況，並明確說明雙方應配合與協調之事項。
- 廠商應依合約所訂定之交付項目與時程，依序進行專案工作。
- 廠商應依「服務建議書」，提交各階段應交付項目，以利本機關於各時間檢查點進行確認與驗收。

4.3 專案組織與人力

4.3.1 專案組織

得標廠商須成立專案組織，其資格說明如下：

- 得標廠商需有輔導 B 級機關通過 ISO27001 認證之經驗。
- 專案經理應具備資格：(依需求撰寫)。
- 資安顧問應具備資格：(依需求撰寫)。

4.3.2 專案人力要求

- 專案期間不得隨意更換專案經理與資安顧問，如需更換人選，須先經本機關同意，且更換同等資歷或以上資歷之人員。
- 專案輔導期間，若專案成員服務不佳或違反本機關相關規定，本機關得

提出更換人員要求，廠商不得異議，並須於 2 週內遞補同等資歷 以上資歷人員，且經本機關同意。

4.4 專案費用

- 本案○○年度預算金額為新台幣○○○萬元整。
- 本案所須之人力由得標廠商自由運用調配，並於建議書中詳述計費標準與成本分析。

4.5 交付項目與規範

4.5.1 交付項目

得標廠商執行本案期間之交付項目與時程，應依「表 1 得標廠商應交付項目一覽表」所列之原則分階段交付，並於「服務建議書」內載明預計交付日期，分述如下：

- 專案執行計畫書

  廠商於決標次日起 15 個日曆天內，提交「專案執行計畫書」，以確認專案進行方式、專案組織、相關時程及配合事項等，並經本機關同意。

- (請依需求撰寫)

表1　得標廠商應交付項目一覽表

項次	工作項目	交付項目	相關要求
一	專案規劃與啟動	▪專案執行計畫書 ▪專案啟動會議簡報與會議紀錄	得標廠商應於決標次日起，即日啟動本案，15 個日曆天內，提交本機關同意之「專案執行計畫書」，其內容應符合本案需求規格，做

項次	工作項目	交付項目	相關要求
			為日後驗收標準
	(請依需求撰寫)		

4.5.2 交付文件格式

本案之各式文件一律以中文撰寫，並給予適當文件與版本編碼，但一般通用「術語」仍得以原文呈現。專案執行過程如有文件翻譯需求，應由廠商自行負責。交付文件應以光碟方式提供電子檔與裝訂成冊之紙本文件各一份。

4.6 履約規範與罰則

4.6.1 履約規範

- 得標廠商須指派專案經理、資安顧問及相關工作人員，定期於本機關召開專案檢討會議，提出工作內容報告，並與本機關專案小組成員共同檢討各項工作事宜，於專案期間指派駐點人員，每週至少 16 小時。
- 本案進行期間，本機關與廠商定期或不定期召開會議，會議目的為檢討專案計畫執行狀況、研商待解決問題與協調事項等。廠商應由專案經理或專案負責人率領主要工作人員參與，並負責撰寫會議紀錄與工作報告等。
- 得標廠商須協助相關同仁了解資訊安全規範標準、協助本機關了解撰寫標準文件流程及協助溝通本案進行所發生之衝突等工作。
- 得標廠商應訂定品質管理流程，本機關得以稽核。
- 為確保本案品質，特制訂服務水準協定(Service Level Agreement，SLA)。詳細服務水準規範如表 2：

表2　服務水準規範一覽表

項次	項目	服務水準
一	風險評鑑	▪分析機關面臨之威脅與潛在問題，辨別威脅來源與脆弱點，釐清降低風險之安全控管點，進行衝擊分析，計算並決定可接受風險等級 ▪建議風險管理機制(如降低、移轉、避免或接受)，選取適當之安控目標與控制點，完成風險處理計畫並通過機關審查 ▪風險評鑑執行時程依核定之工作計畫書內容
二	ISMS 系統四階文件	▪依計畫進度完成符合最新版本 ISO 27001:2013 資訊安全管理系統標準要求，遵循內部控制制度之相關四階文件並完全通過機關審核。 ▪四階文件執行時程依核定之工作計畫書內容
三	內部稽核	▪修訂 ISMS 系統內部稽核制度與訂定年度稽核計畫，並持續改善機關資訊安全政策之落實 ▪製作 ISMS 系統(含法規遵循)之稽核查檢表，並詳列查核項目之查核重點。依機關稽核分組要求，稽核時廠商至少派 3 人(含)以上到稽核團隊，協助執行至少 1 次內部稽核，並於完成稽核工作後 5 個日曆天內提交含改善建議稽核報告 ▪稽核時程依核定之工作計畫書內容 ▪稽核後 1 個月內完成不符合事項改善之持續追

項次	項目	服務水準
		蹤與成效確認
四	第三方驗證缺失改善	▪協助持續維護管理系統複驗之相關事宜，並提供服務流程調整與稽核報告缺失之改善方案 ▪驗證審查後 1 個月內完成不符合事項改善之持續追蹤與成效確認

4.6.2 罰責

- 專案期間違反上述任何所述者，視同違反『未能於規定時間完成工作計罰』，如須延長日期或非廠商之問題(不納入計罰)，須經本機關同意。
- 得標廠商違反『未能於規定時間完成工作計罰』，其罰款(違約金)計算方式為每延遲 1 日(以日曆天計，星期日、國定假日及其他休息日均應計入，不滿 1 日以 1 日計算)，本機關得按契約總價之千分之一計算懲罰性違約金，款項可自契約總價或履約保證金項中扣抵。
- 違約金上限依採購法之採購契約要項第四十五點規定，違約金以契約總價之 20%為上限。如違約金逾 20%時，本機關得以書面通知得標廠商終止契約或解除契約之部分或全部，且不補償得標廠商所生之損失。
- 得標廠商應於議價後所提成本分析中，詳列各項工作項目成本，如於驗收時，經審查發現有不合格之工作項目，得標廠商應依期限予以改正。如未改正，本機關有權扣除該項工作之款項。
- 得標廠商指派之專案負責人與工作成員，未經本機關同意，不得更換，如有未經本機關同意自行更換時，每更換乙次得依契約總價之千分之一計算懲罰性違約金。

- 得標廠商應將文件品質保證納入專案品質保證項目，嚴謹製作本案各項文件，包含版面與內容皆須嚴格要求一致性及正確性。交付本機關之文件經本機關審閱時，所發現錯漏處達◯處以上，或業經本機關要求修訂仍未修訂者，本機關得按每字新台幣◯◯元計算懲罰性違約金，並自付款項中扣抵；其有不足者，得通知廠商繳納或自履約保證金扣抵。

4.7 教育訓練

- 得標廠商應於專案期間，提供資訊安全管理系統之相關教育訓練課程，課程需求說明如表 3。

表3　輔導資訊安全管理系統教育訓練需求表

項次	課程名稱	課程時數	備註
一	一般使用者資安宣導課程	每次上課 2 小時，開課 2 梯次	總時數 4 小時
二	高階主管資訊安全認知	每次上課 2 小時，開課 2 梯次	總時數 4 小時
三	導入資訊安全管理系統各階段專業訓練課程	每次上課 3 小時	總時數不得少於 42 小時

5. 驗收與付款

5.1 驗收

5.1.1 驗標標準

得標廠商應依「3. 專案工作需求」所列事項，以及符合服務水準協定(SLA)中所列事項，完成本案所需之各項作業，並依其所制訂之交付時程，完成相關文件與紀錄之交付。

5.1.2 驗收方式

本機關將於各項工作項目交付完成後進行審查作業，得標廠商需依本機關審查意見修正交付項目，並再送至本機關複驗。

5.2 付款

- 本專案分○階段驗收，第一階段為○○○，驗收合格付款金額為支付合約總價金之 30%。
- 第二階段為完成○○○，驗收合格付款金額為支付合約總價金之 30%。
- (以上為範例，請依需求撰寫)。

各階段驗收，廠商須將應交付項目，送經本機關使用單位確認無誤，並由使用單位出具合格證明文件，始得辦理驗收給付價金。

6. 建議書製作規定

6.1 服務建議書內容

廠商參與本案之投標須提交服務建議書，其內容說明如下：

- 專案概述

  專案名稱、專案範圍、專案時程、專案目標及預期效益等。

- 專案執行計畫

  – 專案時程規劃

    說明專案各項工作項目與預定時程之規劃。

  – 專案執行方式

    說明專案管理、資安管理及各階段作法與預計產出之文件。

  – 資安管理計畫

    說明得標廠商在專案進行期間將實施之資安管理機制。

- 專案管理

  – 專案組織與人力

    說明專案組織、人員配置、技術支援人力、職責分工、專案組織變更管理方式、專案成員專長及認證等。

  – 專案品質與風險管控

    具體說明專案進行期間，監控專案進度與品質之方法。

- 成本單價分析

  列舉說明投入本專案人力、時間及其他必要費用成本。

- 廠商經驗與能力

  簡介廠商內部組織人力、設備、營運現況及相關機關經驗實績(需於附件檢附證明文件)等。

  – 簡略介紹廠商組織、規模及營業狀況。

  – 承接類似本案之成功經驗與實績說明，應檢附承包相關專案之契約、完工證明以及專案通過認證之證明文件。

6.2 服務建議書製作與裝訂格式

- 應以 A4 大小之紙張橫式繕打，字體以 14 點細明體或標楷體為原則。
- 建議書封面應註明專案名稱、廠商名稱及建議書提出日期。
- 建議書須編製目錄，包含各章節與附件之頁次。
- 建議書除封面外，目錄與本文均應於各頁下端中央加註頁碼。
- 建議書請雙面列印，並裝訂線於左側。
- 電子檔以○○軟體製作為原則，電子檔案隨同建議書一併交付。
- 建議書之份數與交付日期，請依投標須知辦理。

7. 評選作業

本機關依據「政府採購法」第 22 條第 1 項第 9 款之規定辦理，透過書面審查與簡報答詢方式，以合於招標文件，標價合理且在預算金額內，經評選委員評選為合格之廠商，依序議價。

7.1 評選作業流程

- 本機關將邀集專家學者組成評選委員會，除對廠商之建議書進行書面審查外，並由本機關召開評選會議。由廠商提出 15 分鐘對建議書之簡報，其後並接受評選委員之詢問，答詢時間以不超過 10 分鐘為限，惟因評審委員詢問題目過多時，主席得酌以延長答詢時間。評選會議時間與地點，將於資格審查時當場宣布或另備文通知，而廠商之簡報順序，亦於資格審查時抽籤決定。
- 簡報與答詢結束後，各評選委員將根據本徵求建議書說明文件第柒之二「評選項目與評分」所列項目與配分評定各廠商名次及其是否為合格廠商 (以總得分 70(含)以上為合格)。
- 各評選委員評定結果不得有同名次或從缺情形。
- 過半數(含)評選委員評定為合格之廠商方列入排名與序分計算;另半數以上(含)評選委員評定不合格之廠商，視為不合格，若所有廠商均不合格時，主席應宣布廢標，重新辦理本案。
- 本案評選採序位法辦理，就各評審項目分別評定並換算為序位，再加總計算廠商序位，最低者為第 1 優先序位，次低者為第 2 序位，餘依此類推。
- 經評選委員會評定優勝廠商，依優勝序位，自最優勝者起，依序以議價方式辦理，但有二家以上廠商為同一優勝序位者，以建議書的標價低者

優先議價，若仍相同者，則擇獲得評選委員評定序位第一較多者決標;仍相同者，抽籤決定之。

- 評選結果簽請首長或授權人員核定後，由本機關另定時間通知廠商依序辦理議價。

7.2 評選項目與評分

本案由評選委員就廠商所提出建議書之內容，針對其經驗、能力與服務水準，依下列各項目及配分(如表 4)，予以評分，總分 100 分，得分總計達 70 分(含)以上者為合格。

表4　評選項目表

評 選 項 目	評選項目說明	配分
一、廠商實績與履約能力	1.廠商人力規模與商譽 2.資安實績與相關技術經驗	20
二、專案管理能力	1. 對本案工作內容之了解 2.進度時程控管、資料管制與品質保證 3.本案之團隊規模與專案負責人之經驗 4.本案團隊成員之專業證照符合程度	20
三、專案規劃完整性	1. 本案要求之各項服務項目的執行專業性 2. 本案要求之各項交付項目之完整性	30
四、專案成本分析	本案規劃、執行、專案管理及報告撰寫等各 項費用估算之合理性	20
五、簡報與答詢	廠商簡報與答詢內容是否清楚與完整	10
總分		100

評 選 項 目	評選項目說明	配分
是否合格		
名次序位		

7.3 優勝廠商評定方式

7.3.1 評選優勝廠商

- 出席評選委員將投標廠商建議書內容，依據本案「評選項目與評分」予以評審，並依據各評選委員之評定結果，經出席評選委員過半數評予規格總配分達 70(含)以上者為優勝廠商。
- 針對優勝廠商之規格總配分，由高至低分別給予 1、2、3...之「序位」，累加出席評選委員所給予同一優勝廠商之「序位」得其「序位總和」，就各優勝廠商「序位總和」由低至高分別給予 1、2、3...之「優勝序位」。
- 依優勝序位決定優先議價順序。
- 若有二家以上之「優勝序位」相同時，以標價低者優先；若標價仍相同時，則抽籤決定優先議價順序。
- 依採購法五十二條，決標時得不通知投標廠商到場，其結果將於決標○日通知各投標廠商。

7.3.2 議價與決標原則

- 決標方式依照投標須知辦理。
- 按優勝序位由第一順位優勝廠商議價，如議價結果未進入底價，依序洽次一優勝廠商辦理議價，餘類推。
- 如廠商決標後放棄得標、拒不簽約者，則按優勝序位由洽次一優勝廠商辦理議價。