附件 7「政府機關資訊安全管理系統(ISMS)公正第三方驗證」RFP 資安需求範例

○○年度

資訊安全管理系統(ISMS)公正第三方驗證委外服務案

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)」第三方驗證委外服務案(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 專案目標

對本機關之資訊安全管理系統(ISMS)進行驗證，以確保確實符合 ISO27001 資安標準。

1.4 專案範圍

本案以本機關「○○業務/資通系統」所涉及之作業為驗證範圍(以下簡稱驗證範圍)，驗證該範圍內之資訊安全管理系統(ISMS)。

1.5 專案期程

自簽約日起至民國○○年○○月○○日止。

1.6 專案預算

本案預算金額為新台幣○○萬元。

2. 專案工作需求

2.1 專案整體需求

本案應涵蓋以下項目：

- 廠商執行 ISO27001 標準驗證作業，所有人天數需符合相關標準規範。
- 提供 ISO27001 驗證稽核報告。當有不符合項目時，應提供相關追蹤報告文件。
- 於本機關通過 ISO27001 資安驗證時，提供合格證明。。

2.2 資通安全需求

2.2.1 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。
- 投標廠商須符合資通安全管理法所定義資訊安全管理系統標準公正 第三方驗證之機構。

2.2.2 資安要求事項

- 得標廠商基於本案需要，所取得各種形式之資訊，包含文書、圖片、紀錄、照片、錄影(音)及電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱讀或理解之文書或物品，應負資訊保密及確保資訊安全責任，並簽訂保密協議書。
- 得標廠商對特別以文字標示或口頭明示為機密資料者，非經本機關書面同意，不得洩漏資料予第三者，致使造成之法律責任或賠償，廠商應負完全責任。
- 得標廠商對於可能接觸與本案相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署保密切結書(切結書形式由廠商自訂)。
- 契約終止時，廠商應將有關本案過程中處理之任何形式資訊，整理歸檔後退還本機關或經本機關同意後銷毀。
- 履約期間造成保密與安全事件，得歸咎於廠商之責任時，廠商應負所有法律與賠償責任。
- 本機關對得標廠商保留實地稽核權，以確保廠商於委外服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。
- 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。

3. 專案管理需求

3.1 專案期程

自簽約生效日起至民國○○年○○月○○日止，對本案所載之驗證範圍進行 ISO27001 驗證。

3.2 專案管理

- 得標廠商於專案期間應辦理啟始會議與結束會議，會議討論內容與結果需作成紀錄。
- 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。

3.3 專案組織與人力

- 為確保專案如期如質完成，廠商應針對本專案之需求，妥慎成立專案小組，執行本專案所需之各項作業，並指派專案經理負責督導工作項目。
- 本案團隊人力至少應包含專案負責人/專案經理與 ISMS 稽核人員。而 ISMS 稽核人員應具備以下所列舉之經歷及相關專業證書，以確保服務水準，並於建議書中檢附成員姓名、專業證書及服務實績證明等影本以供審核。應具備資格說明如下:。

  – 合格之稽核員證書證明。

  – 具二年(含)以上之 ISMS 稽核相關經驗。

3.4 專案費用

- 本案○○年度預算金額為新台幣○○萬元整。
- 本採購保留未來向得標廠商增購之權利，第 2 及第 3 年後續追查稽核驗證(Surveillance Audit)相關費用(包含申請、驗證、改版轉證、證書年費...

等)。擴充期間 YYY+1、YYY+2 年度費用各約◯◯萬元整，總經費為新台幣◯◯萬元整。

3.5 交付項目與規範

3.5.1 交付項目與時程

表1　交付項目與時程

項次	交付項目	交付時程	內容說明
一	工作計畫書	決標日起2週(日曆天)內交付	▪工作計畫書應以廠商投標時之「服務建議書」為基礎，並依採購評選意見修改 ▪內容除包含對本案之執行敘述，應含專案管理、組織、人力、分工、職掌、細項工作規劃內容、執行方式及時程說明等。
二	驗證稽核報告	依工作計畫書載明之交付時程	文件內容應包含稽核相關資訊與發現，若有驗證稽核發現之不符合事項，應包含相關追蹤報告文件。
三	驗證合格證明	依工作計畫書載明之交付時程	通過驗證時，驗證合格之證明

3.5.2 交付文件格式

各項文件應提供紙本◯份，光碟電子檔◯份。

3.6 履約規範與罰則

3.6.1 履約規範

- 得標廠商應於本案啟動時，召開會議以進行驗證前說明，會議目的為說明驗證執行流程與問題解決與協調方式。
- 實地驗證期間，得標廠商應遵循本機關之資安控管措施。
- 驗證結束後，亦應召開驗證結束會議，並於約定期間交付應交付項目。
- 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下表 2：

表2　服務水準規範一覽表

項次	項目	服務水準
一	驗證稽核報告	▪詳列稽核相關資訊與發現 ▪若有不符合事項，其追蹤報告文件
二	驗證合格證明	通過驗證時，驗證合格之證明

3.6.2 罰責

- 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. 驗收與付款

4.1 驗收

4.1.1 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。

4.1.2 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。

4.2 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%。
- (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。

5. 建議書製作規定

5.1 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
  - 專案目標
  - 專案時程
- 專案執行計畫
  - 專案時程規劃
  - 專案執行方式
  - 專案交付項目
  - 資安管理計畫
- 專案管理
  - 專案組織與人力
  - 專案品質與風險管控
- 成本單價分析
  - 詳列稽核人員人/天價格(所需之差旅及交通費用請內含於稽核人員費用中)。
  - 有證書年費者請載明證書年費與證書申請費用等。
  - 詳列第 2 及第 3 年後續追查稽核驗證費用。

- 廠商經驗與能力
  - 簡略介紹廠商組織、規模及營業狀況。
  - 稽核報告書面範例。

5.2 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。

6. 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。

6.1 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。

6.2 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 3)，予以評分，總分 100 分，得分總計達 70 分(含)以上者為合格。

表3　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		

6.3 優勝廠商評定方式

6.3.1 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。

6.3.2 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。