行政院農業委員會農田水利署桃園管理處

桃園管理處土地改良物水利設施委託盤點登載等工作委託服務(開口合約)

需求說明書

壹、委託案目標

執行機關土地改良物水利設施委託盤點管理等工作。

貳、委託專案履約期間

廠商應於決標日起 180 日曆天完成履行採購標的之供應或本服務案預算金額(契約金額上限)用罄，兩者不論何者先屆，即表示完成履行採購標的之供應。

參、委託項目(工作項目)

一、土地改良物水利設施資料清冊彙整及建檔作業

1. 由本處提供約90~110年土地改良物相關資料，廠商依據資料進行土地改良物財產資料清冊彙整比對及建檔作業。
2. 清冊資料彙整建檔總表。

二、土地改良物水利設施盤點及造冊作業：

1. 完成本處約2500件(以每件實作數量決算)土地改良物水利設施盤點盤點等工作。
2. 廠商依據清查明細表辦理外業調查土地改良物使用現況，並依據現地進行繪製使用現況略圖(施工位置圖)，紀錄表內容包含地籍資料(需有圳路名稱或地段地號或具鑑別性名稱或TWD97二度分帶座標) - (預算書或相關資料上有註記該處所二度分帶座標時，廠商需務必填列該座標加前三項資料之一項以上)、地上物管理等欄項資料(財產盤點統計表、帳務不符盤點情形)。
3. 現況使用照片(含電子檔)：照片以可得知悉該件土地改良物現況為基準，每件土地改良物至少1張(若有處所則每處所至少1張)。
4. 依據盤點調查成果整理成清冊及數化成本處要求之格式(PDF、WORD、EXCEL 等)。

三、土地改良物資料庫建置

1. 土地改良物資料庫建置，可新增、編輯、刪除功能，並於可整合本處利水興農系統中，可在"利水興農"圖台上可點擊顯示土地改良物屬性資料資料。**土地改良物資料庫建置:得標廠商需自行建置及架設**

一套土地改良物空間資料庫系統，並需提供開放資料庫系統API介接，以利"利水興農"系統商介接整合，另外建置本資料庫系統需符合本處資安規定。

2. 廠商需將本案土地改良物盤點清查成果匯入土地改良物資料庫。

四、資訊安全作業：

1. 本案範圍內之系統應符合本處服務系統資訊安全需求原則(202201版)(如需求說明書第 4~5 頁)。
2. 本案範圍內之系統應符合本處對該系統風險評鑑需求對應之「資通安全責任等級分級辦法 -資通系統防護基準」(如需求說明書第 6~12 頁)。
3. 本案範圍內之資通訊軟硬體(含委外承攬作業時)，禁止使用大陸廠牌(含貼牌)資通訊產品，禁止使用大陸研發之軟體，應符合「各機關對危害國家資通安全產品限制使用原則」，不得使用該法規主管機關核定之廠商及產品清單。
4. 遵守資通安全管理法、其相關子法、本處 ISMS 規範及行政院所頒訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規定。
5. 廠商投入本案之員工，應依本處委外廠商人員保密切結書規定簽訂保密切結書。如專案人員於專案期間內發生變更，應經機關同意後辦理，並依機關相關作業安全規定，進行工作申請。
6. 廠商如知悉本公司或機關發生資安事件或違反資通安全相關法令時，均必須於 1 小時內通報機關，提出緊急應變處置，並配合機關做後續處理。
7. 確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合機關對系統品質及資通安全的要求。
8. 廠商需配合資安法應辦事項、弱點掃描檢測修補、機關 ISMS 作業之相關支援、資安事件回應事項，例如營運持續運作計畫之演練、災難復原演練。

五、其他注意事項：

1. 廠商應確保其指派辦理本契約工作人員在工作期間切實遵守中華民國法令、規章。
2. 本契約規定之土地改良物盤點紀錄表應依機關所提供之需求辦理。

肆、成果交付與付款條件：

- 一、決標日起 15 日內，廠商提送「工作計畫書」一式 3 份(含光碟檔案 3 份) 提送機關審查核定，經機關驗收合格撥付(土地改良物資料庫建置費及管理費合計契約金額 25%)。
- 二、自決標日起 180 個日曆天內完成所有土地改良物盤點及及造冊作業，造冊一式 3 份(含光碟檔案 3 份) 及總結報告書，本案執行期間可依完成數量進行 3 期(除尾款，每期以 2 個月或完成數量超過 20%為原則)估驗。

伍、預算金額：新臺幣 1,435,800 元整

項次	項目	單位	預估數量	備註
1	土地改良物水利設施資料清冊彙整比對及建檔作業	件	2500	以實作數量決算
2	土地改良物水利設施盤點及造冊作業	處	2500	以實作數量決算
3	土地改良物資料庫建置	式	1	
4	管理費(報酬風險、雇主及第三人意外責任險、利潤及稅捐等)	全	1	(不超過 1~3 合計 10%)
5	營業稅			(1~4 合計 5%)

- 參閱 OWASP(Open Web Application Security Project)安全測試指南，規範與檢測應用程式安全風險：
OWASP 網站應用安全 Top 10 (OWASP 2021 Top 10 或更新版本)
(https://owasp.org/Top10/zh_TW/)
移動裝置應用安全 Mobile Top 10 (OWASP Mobile Top 10 或更新版本)
(<https://owasp.org/www-project-mobile-top-10/>)
- 應至少檢附包含 OWASP Top 10 檢測標準項目的安全檢測報告(網站安全檢測或源碼安全檢測或移動裝置應用程式上架審核紀錄)。
- 系統應符合本處對該系統風險評鑑需求對應之"資通安全責任等級分級辦法資通系統防護基準"。
- 請提出資訊安全管理計畫，並至少涵蓋下列項目說明

管理項目	項目內容說明
系統存取控制之安全	系動中啟動之應用程式，如非必要，不以 administrator 或 root 權限帳號來執行，降低應用系統被入侵的風險。
身分驗證管理	前台與後台之帳號管理與身分驗證機制。
紀錄配置	在線監控、登入紀錄、在線紀錄、存取失敗情形及法規所需之紀錄事件，及日誌紀錄項目、寫入位置、合規性存放時間的容量估算。
組態設定安全	組態設定檔的安全設定、預設密碼應修改，不安全的設定易導致目錄揭露等安全問題
資料被查詢與異動之軌跡紀錄	敏感資料洩漏防護
防範惡意碼與安全漏洞措施	採取預防措施，以防止與偵測惡意碼、未經授權行動碼的植入及程式安全漏洞修復。
後門程式清理	如為開發方便系統維護所設置的後門程式應清除，避免日後產生安全威脅風險。
發現系統或程式弱點之修復方式	如為中級以上利用風險威脅，應盡早修復。

管理項目	項目內容說明
系統維運期間之定期弱點掃描措施	修補前進行測試預估可能的影響，排定修補時程。
資訊安全事故管理	應訂定緊急應變與回復作業程序，事故發生後檢討盤點與資安積極作為。 廠商需於接獲本處通報時間起算 24 小時內到達本機關並完成資安事件之初步緊急應變處理。 並於事件處理完畢 7 個天內，將處理經過作成報告(包括防止類似事件再發生之補救措施的規劃執行)。
災害復原	設定恢復點目標(RPO)、復原時間目標(RTO)並對映設置復原策略。
復原策略	定期備份、備份間距、備份方法、備份內容(系統相關之設定檔、網頁資料、伺服器檔案、資料庫資料、其他重要影響服務的資料及設定)

5. 安全服務需求：保持安全的作業系統及應用程式平台版本，定期維護與更新。
6. 正式上線及服務中應用系統應有軟體版本更新紀錄，並提供「Web 網頁應用程式目錄清單」，每次程式更新時同步更新「Web 網頁應用程式目錄清單」對應內容更新記錄。
7. 系統中安裝之套裝應用程式與版本應敘明。
8. 服務系統平台各項服務使用的防火牆通訊埠應敘明。
9. 維護或進行應用系統設定、網路設定、遠端桌面連入等設定應通知取得相關資訊人員同意後方可進行；各項設定及變更應有操作紀錄。
10. 定期清查[已停止更新]及[服務閒置]的應用或系統平台；並與承辦人員確認後，將服務移轉至支援更新服務的平台，或排定服務下架時程以及移除相關網路設定。
11. 廠商每年定期自行或由第三方公正單位進行至少一次的安全檢測，並交付檢測報告。
12. 廠商投入本案之員工，應依本處委外廠商人員保密切結書規定簽訂保密切結書

建議參閱

資通安全責任等級分級辦法：附表九-資通系統防護需求分級原則、附表十-資通系統防護基準

政府資訊作業委外安全參考指引

Owasp Testing Guide 安全測試指南

附表九 資通系統防護需求分級原則

防護需求等級 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性、法律遵循性構面中，任一構面之防護需求等級之最高者定之。

附表十 資通系統防護基準修正規定

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	<p>一、機關應定義各系統之間置時間或可使用期限與資通系統之使用情況及條件。</p> <p>二、逾越機關所許可之間置時間或可使用期限時，系統應自動將使用者登出。</p> <p>三、應依機關規定之情況及條件，使用資通系統。</p> <p>四、監控資通系統帳號，如發現帳號違常使用時回報管理者。</p> <p>五、等級「中」之所有控制措施。</p>	<p>一、已逾期之臨時或緊急帳號應刪除或禁用。</p> <p>二、資通系統間置帳號應禁用。</p> <p>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。</p> <p>四、等級「普」之所有控制措施。</p>	<p>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。</p>
	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	<p>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。</p> <p>二、等級「普」之所有控制措施。</p>	<p>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。</p> <p>二、使用者之權限檢查作業應於</p>	

			<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

			時間(UTC)或格林威治標準時間(GMT)。
	日誌資訊之保護	<p>一、定期備份日誌至原系統外之其他實體系統。</p> <p>二、等級「中」之所有控制措施。</p>	<p>一、應運用雜湊或其他適當方式之完整性確保機制。</p> <p>二、等級「普」之所有控制措施。</p>
營運持續計畫	系統備份	<p>一、應將備份還原，作為營運持續計畫測試之一部分。</p> <p>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。</p> <p>三、等級「中」之所有控制措施。</p>	<p>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。</p> <p>二、等級「普」之所有控制措施。</p>
	系統備援	<p>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。</p> <p>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。</p>	<p>一、訂定系統可容忍資料損失之時間要求。</p> <p>二、執行系統源碼與資料備份。</p>
識別與鑑別	內部使用者之識別與鑑別	<p>一、對資通系統之存取採取多重認證技術。</p> <p>二、等級「中」及「普」之所有控制措施。</p>	<p>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。</p>
	身分驗證管理	<p>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。</p> <p>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。</p> <p>三、等級「普」之所有控制措施。</p>	<p>一、使用預設密碼登入系統時，應於登入後要求立即變更。</p> <p>二、身分驗證相關資訊不以明文傳輸。</p> <p>三、具備帳戶鎖定</p>

			<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>

	發階段	<p>二、系統應具備發生嚴重錯誤時之通知機制。</p> <p>三、等級「中」及「普」之所有控制措施。</p>	<p>要控制措施。</p> <p>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。</p>	
	系統發展生命週期測試階段	<p>一、執行「滲透測試」安全檢測。</p> <p>二、等級「中」及「普」之所有控制措施。</p>	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	<p>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。</p> <p>二、等級「普」之所有控制措施。</p>	<p>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。</p> <p>二、資通系統不使用預設密碼。</p>	
	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	<p>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。</p> <p>二、使用公開、國際機構驗證且未遭破解之演算法。</p> <p>三、支援演算法最大</p>	無要求。	無要求。

		<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。
系統與資訊完整性	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权使用。</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。
	軟體及資訊完整性	<p>一、應定期執行軟體與資訊完整性檢查。</p> <p>二、等級「中」之所有控制措施。</p>	<p>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。</p> <p>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。</p> <p>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。</p>	無要求。

備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之系統防護基準。