

「配電系統風險評估及策略管理系統建置」(含資通安全)採購規範書

一. 專案目標：

建置風險快篩方法，快篩各區營業處之變電所、高壓饋線之配電場室及高壓電桿，並進行後續設施盤查、風險評估、調適策略等工作，並加值氣候衝擊GIS圖資，以配電相關單位為使用對象，完成建置配電系統風險評估及策略管理系統，及進行系統維護(含資通安全)。

二. 專案工作內容與交付項目：

1. 規格：

模組名稱	工作項目	說明	交付項目/查核點
快篩模組開發及效能提升	開發快篩模組，並提升系統使用效能	因使用配電系統風險評估及策略管理系統，主要為各區營業處，且其轄下所含之變電所、高壓饋線之配電場室及高壓電桿等設施數量眾多，故須開發快篩模組，並採用幕後分批次計算等方式，提升系統使用效能。	交付快篩模組開發及效能提升之成果。/116年1月11日
建置配電系統風險評估及策略管理系統	1、帳號管理	配合管理單位需求，建置子帳號帳號管理及子帳號運用風險快篩、設施盤查、風險評估、調適策略、報告產製等系統各項功能。	完成「配電系統風險評估及策略管理系統」建置、交付系統程式碼/116年3月31日(完成驗收)
	2、風險快篩	應用所開發之快篩模組，於系統流程納入風險快篩之功能。	
	3、設施盤查	依據配電之設施類型及樣態，開發延續風險快篩流程之設施盤查功能。	
	4、風險評估	依據配電單位填報之資料以及設定之運算準則，協助配電單位使用者以參考方法學	

模組名稱	工作項目	說明	交付項目/查核點
		進行氣候變遷風險評估工作。	
	5、調適策略	依循配電設施風險評估結果，設計調適策略規劃填報之功能，協助使用者進行調適策略規劃工作。	
	6、報告產製	依據系統運算成果，產製相關報告內容。	
	7、加值氣候衝擊 GIS 圖資並整合至系統	配合氣候圖資更新，進行圖資測試及加值，更新圖資至配電系統風險評估及策略管理系統。	
系統維護及保固	1、系統服務故障無法運作時，進行維修以維持系統正常運作 2、系統程式錯誤(Bugs)或系統部份功能異常時，進行程式錯誤修改 3、系統功能操作及技術諮詢 4、依使用狀況進行系統資源調整與維運 5、保固期內，依業主需求或使用者回饋進行小幅功能增修，如增修幅度為契約總價 5% 以內，免費修正		交付系統保固相關文件/116 年 3 月 31 日(完成驗收)
資訊安全	1、網站系統資安檢核弱點掃描風險修正改善： 1.1、配合工研院資訊處或機關資安掃描結果，修正改善弱點風險 1.2、完成 115 年度之資安檢測，確保相關項目高嚴重等級檢測結果為 No Alert。 2、資訊安全表單填寫、資安承諾書、資安規格書內之工作項目 3、上線前第三方弱點掃描(黑箱掃描)及弱點調整		交付資安相關文件/116 年 3 月 31 日(完成驗收)

三. 專案經費給付：

1. 116 年 1 月 11 日前交付並完成交付快篩模組開發及效能提升之成果，撥付專案經費 50%。
2. 116 年 3 月 31 日前，完成全部工作，包含完成「配電系統風險評估及策略管理系統」建置、交付系統程式碼、交付系統保固相關文件及交付資安相關文件等各項工作，撥付專案經費 50%。

四. 注意事項：

1. 程式開發環境 WEB .NET C#；支援瀏覽器(Edge、FireFox、Google Chrome)；頁面採用 UTF-8 編碼，用戶端、管理端、資料庫無亂碼。如需修正或重新規劃開發時，現有資料庫原則上保留，視需求異動。
2. 資安要求：配合本院資安稽核及相關書面文件，並需遵守保密及資訊安全條款，相關條文如下：
 - (1) 本院在業務上認為不對外公開或定義為密、機密、極機密或絕對機密之一切文件及資料，包括與其業務或研究開發有關之內容。
 - (2) 依法令須保密或受保護之文件及資料，例如個人資料保護法所規定者。
3. 得標廠商承諾於本案有效期間內及本案期滿或終止後，對於所得知或持有一切本院未標示得對外公開之公務秘密，以及本院依契約或法令對第三人負有保密義務未標示得對外公開之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本案目的範圍內，於本院指定之處所內使用之。非經本院事前書面同意，得標廠商不得為逾越權限範圍之利用，或為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至本院或本院所指定處所以外之處所。
4. 得標廠商知悉或取得本院之公務秘密與業務秘密應限於其執行本案所必需且僅限於本案有效期間內利用。得標廠商同意本條所定公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之得標廠商團隊成員，並應要求該等人員簽署與本條款內容相同之保密同意書或保密切結書。
5. 得標廠商在下述情況下解除其依本條所應負之保密義務：
 - (1) 得標廠商原負保密義務之資訊，由本院提供以前，已為得標廠商所合法持有或已知且無保密必要者。
 - (2) 得標廠商原負保密義務之資訊，依法令業已解密、依契約本院業已不負保密責任、或已為公眾所週知之資訊。
 - (3) 得標廠商原負保密義務之資訊，係得標廠商自第三人處得知或取得，該第三人就該等資訊並無保密義務。

6. 得標廠商同意其人員、代理人、經本院同意複委託之受託人或使用人如有違反本條或其自行簽署之保密同意書者，視同得標廠商違反本條之保密義務。
7. 契約內容有須保密者，得標廠商未經本院書面同意，不得將契約內容洩漏予與履約無關之第三人。
8. 得標廠商履約期間所知悉之本院機密或任何不公開之文書、圖畫、消息、物品或其他資訊，均應保密，不得洩漏。
9. 得標廠商因履行本契約而須將本契約內容或因履行本案而取得之應保密文件及資料揭露予第三人時，應以該第三人與履約有關，且揭露之內容應為該第三人確有必要知悉者為限。
10. 得標廠商應使得標廠商執行本案之人員，包括但不限於經本院同意複委託之受託人、分包廠商等，以書面切結保密義務，並受本條之拘束。
11. 得標廠商參與本案工作人員，均應嚴守委託契約執行內容及本院之業務機密，並不得有侵害及損及本院權利之行為。得標廠商應與其所聘用執行本案工作人員成果歸屬方式、保密條款及得標廠商之聘用研究人員違反保密條款者，得標廠商應依法求償。
12. 得標廠商履行契約提供及使用之軟體，均需為合法軟體，不得違反智慧財產權、著作權及專利法之規定，如有違反事情發生，得標廠商須承擔所有法律責任。
13. 得標廠商人員從事與本院資訊相關作業時，均須瞭解與遵守本院之資訊安全政策及資訊安全相關規定，並須遵循本契約、本院資訊安全管理系統相關規定，本院保留對得標廠商提供服務之部門、人員、作業進行必要之資安稽核之權利，得標廠商應保留相關資安紀錄與備份，以配合稽核活動。
14. 得標廠商應遵守行政院所頒訂之各項資訊安全規範及標準（如行政院國家資通安全會報技術服務中心(網址：<http://www.icst.org.tw/>)所頒訂之共通規範)，並遵守本院「資訊安全系統(ISMS)」等相關資訊安全管理及保密規定，並應負責處理及通報本院有關本專案之資訊安全事件，並依本院所定之安全事件處理及回報程序辦理。得標廠商如未能即時處理或通報本院，致本院或第三人遭致損失者，得標廠商應負賠償責任。
15. 得標廠商處理個人資料應遵守「個人資料保護法」及相關規定；應記載系統使用紀錄，包括每筆資料之新增/刪除/修改/查詢等資料內容及使用者帳號、時間、IP 位址及事由，並於甲方需要時提供相關紀錄。
16. 得標廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式（如病毒、蠕蟲、特洛伊木馬、間諜軟體等）及隱密通道(covert channel)，且於上線前應清除正式環境之測試資料與測試帳號，並提供測試資料與

帳號之清除紀錄。

17. 得標廠商交付之計畫網站至少應包括跨網站腳本攻擊(XSS)及資料庫注入式攻擊(SQL-injection)等開放網路軟體安全計畫(OWASP)所列十大常見網站攻擊模式之測試及防護措施，以保證其提供之系統中不含後門程式、OWASP 十大網路應用系統安全弱點或其他之違反資安之程式漏洞；若經發現，得標廠商應免費即時移除或更新系統。
18. 得標廠商須針對支付之系統出具切結書，保證系統內不含後門程式及隱密通道。
19. 得標廠商執行本契約應依行政院及機關資通安全要求，提供維運系統之網路及資安防護措施相關報告，並執行必要之系統設定及修補等改善措施。
20. 得標廠商交付之系統若含有 Active X 元件，應於程式碼中加入數位憑證，並提供合格單位認證之簽章證明及 Active X 安全性檢測報告（至少包含弱點掃描、源碼檢測及滲透測試等必要項目）。
21. 得標廠商交付之應用系統應符合 IPv6 之規範，及配合政府組態基準(GCB)之要求進行更新，並提供檢測報告。
22. 得標廠商應依經濟部計畫網站資通安全管理要點要求施行計畫網站資通安全管理、改善並提供實施報告。得標廠商交付之計畫網站應設置於具有保護措施之環境，保護措施應至少包括防火牆及防毒機制，並適時修補系統安全弱點，且應依政府機關（構）資通安全責任等級分級作業規定，定期執行網站弱點掃描，及完成弱點修補，並應依計畫網站盤點及分級評估結果，採行必要之控制措施，以確保網站之安全防護水準。
23. 得標廠商交付之計畫網站應建置於本院專用之主機和資料庫，不得與其他機關或機構共用，且計畫網站之正式運行環境，不得同時作為測試及開發環境使用，並應保存網站建置、維護及更新紀錄。存放機敏性資料應啟用系統存取稽核軌跡記錄功能，且設有存取監控、系統可用性監控及異常警示通報機制。
24. 得標廠商交付之應用系統應具有輸入資料之檢核、敏感資料之加密及適切之權限管制設計，另於上線前進行系統的壓力測試，並提供相關測試之報告。
25. 得標廠商保證其派至本院提供勞務之駐院人員於本院工作期間以及本案終止後，在未取得本院之書面同意前，不得向任何人、單位或團體透露任何業務上需保密之文件及資料，並配合本院規劃參與資安教育訓練。得標廠商保證所派駐人員於契約終止（或解除）時，應交還本院所屬財產，及在履約期間所持有之需保密之文件及資料。
26. 個資要求：受本院委託蒐集、處理或利用個人資料及檔案（指自然人之姓名、身分證統一編號、職業、聯絡方式、社會活動、其他得以直

接或間接方式識別該個人之資料等等個人資料保護法所指個人資料)時，需遵守「個人資料保護條款」(委託廠商協助本院蒐集、處理及利用個資版本)。不得將本契約所涉任何人資料蒐集、處理及利用之義務複委託予第三人執行。需通過工研院資科中心資安檢測、稽核與相關規定。需遵守能源局契約書第二十五條、個人資料保護條款。

27. 本案委託客制開發系統之智慧財產權歸工研院所有。執行本案應注意不得侵害他人之個人資料、智慧財產權及其他權利，如因故意或過失不法侵害他人之個人資料、智慧財產權或其他權利或因債務不履行所產生之損害賠償，悉自負法律上之責任。
28. 得標廠商應交付：介面原始程式、程式碼、圖檔(非文件，應交付電子檔案)。