全國農業金庫Checkmarx One SCA開源軟體管理工具系統規格及特別條款

全國農業金庫股份有限公司（以下稱本公司）採購Checkmarx One SCA開源軟體管理工具系統（以下稱本案系統），其規格及特別條款規定如下：

甲、規格

壹、一般規定

一、得標廠商須符合之專業資格：具備金融同業建置經驗。投標時提供截標日前3年內之採購契約、驗收文件或維護合約等任一文件影本。

二、得標廠商須依本規格與特別條款之「貳、功能規格」之需求，於本公司資訊環境安裝建置及設定。

三、得標廠商於交貨時應提供授權證明文件。

四、投標廠商應按投標金額之5%以現金、金融機構簽發之本票或支票、銀行保付支票、郵政匯票繳納押標金，得標後押標金轉為履約保證金，履約保證金經履約完成無待解決事項後轉為保固保證金，保固期滿且無待解決事項後無息發還保固保證金，未得標者無息退還。

五、投標廠商如有政府採購法第101條所列之情事，經刊登於政府採購公報者，於同法第103條規定之期間內，不得參加投標或作為決標對象或分包廠商。

六、本規格稱「以上、以下、以內、至少、高於、低於」俱含本數。

貳、功能規格

一、開源軟體管理工具：Checkmarx One SCA，不限安裝台數及型態，提供專案人員之專案系統掃描，授權數量需至少可30人上線使用，並且提供30個系統數量。

二、須支援本公司現有系統平台(含Android/iOS/Windows)之開放原始碼元件安全之檢測作業。

三、須支援多種應用程式語言(至少包含 Java、JavaScript/TypeScript、PHP、Python、Ruby、Objective-C、C#、C/C++、Perl、swift、GO、dotNet、Unity 等程式語言)之檢測作業。

四、須提供掃描結果之風險報告，並依開放原始碼元件安全弱點之風險等級進行分類，至少須包含三種風險等級(高、中、低)的分類。

五、提供開放原始碼元件之授權(License)資訊等級進行分類，至少需包含三種風險等級(高、中、低)的分類。

六、須提供Web使用操作介面，供程式開發人員與審查人員檢視開放原始碼元件分析結果。

七、須至少提供本次採購之30位使用者可同時登入系統，執行開放原始碼元件檢視作業。

八、並提供本機線上掃描及本機離線掃描方式進行，且不限受測檔案數量及容量。

九、須提供多面向報告資訊，提供開放原始碼元件之完整清單、授權資訊、弱點資訊；提供Web介面，相關人員可擁有登入權限，自行透過瀏覽器檢視開放原始碼元件檢測結果。

十、針對開放原始碼元件檢測結果與報告，提供安全問題說明(關連之CVE 編號、說明)及修復建議。

十一、須提供持續安全弱點偵測規則，以保持最新的弱點分析基礎，應對有新的風險弱點發佈。

十二、須提供快速搜尋功能，協助在尋找開放原始碼元件時，就可即時得知弱點、授權、品質及是否符合公司內規定等功能，以輔助開發人員尋找不符合之元件。

十三、須提供各個授權資訊及風險說明，支援單一元件多個授權資訊，以避免開放原始碼元件與程式碼賦予之授權方式不同。

十四、提供API介面取得掃描資料或系統專案設定。以RESTful格式為主要基礎以達自動資料介接目標，並能支援應用程式設定公司規範規則以及取得開放原始碼元件檢測結果與報告。

十五、自動偵測程式內是否引用到開放原始碼元件受弱點影響之功能，並提供程式碼如何與開放原始碼元件交互蹤跡以及實際使用的程式檔案及行數。

十六、須支援image掃描機制，並提供image的安全性之檢測結果。

十七、顧問服務：提供2次顧問到場服務及線上平台50點顧問技術支援。

乙、特別條款

壹、得標廠商同意履行以下情事：

一、得標廠商應提供第三方認證證明或公正第三方之驗證報告，如資訊安全管理國際標準要求或資訊安全管理系統國家標準（ISO/CNS 27001）有效證書；得標廠商若無法提供時，應配合本公司辦理資訊安全訪視作業。

二、得標廠商履行契約不得違反法令強制或禁止規定、公共秩序及善良風俗，對本公司經營、管理及客戶權益，不得有不利之影響，並應遵守農業金融法、銀行法、洗錢防制法、個人資料保護法、消費者保護法、中華民國銀行商業同業公會全國聯合會訂定之相關業務規章或自律公約及其他法令之規定。得標廠商應本於善良管理人之注意義務辦理本契約事宜，契約如有履行不能或履行困難之虞者，應即通知本公司。

三、得標廠商應建立標準作業程序，執行消費者權益保障、風險管理、內部控制及內部稽核制度，除應建立消費者爭端解決機制，包含解決時程、程序及補救措施外，另應提供聯絡窗口及電話詢答服務。

四、得標廠商同意金融監督管理委員會、中央銀行、中央存款保險公司、農業部農業金融署等機關或依農業金融法第七條規定之機關及本公司或委託獨立第三方單位進行辦理本契約相關事項之稽核。得標廠商應提供本契約之應辦事項相關資料或報告，配合金融檢查或稽核，並於期限內提供相關資料或報告。

五、得標廠商因履行契約應辦事項所應負之損害賠償責任以直接實際損害為限。但有關人身傷害（包含死亡）、物之毀損、專利權及著作權之損害、得標廠商之故意或重大過失造成之損害賠償則不在此限。

六、得標廠商若有違反契約約定情事發生，除契約另有約定外，本公司得於通知得標廠商後終止或解除契約，本公司於主管機關命為終止或解除契約時亦同。

七、得標廠商履行契約應辦事項，對外不得以本公司名義為之，亦不得進行不實廣告，若違反致本公司受損，應負賠償責任。

八、本契約應辦事項若有重大異常、缺失或發現疑似資訊安全或個人資料外洩等異常事件或事故時，得標廠商應立即以口頭、電話等方式

通知本公司，並配合本公司相關程序辦理異常排除及通報事宜，如必要應提供駐點服務。並於處理完成後，提供相關報告。

九、得標廠商因履行契約應辦事項所知悉一切有關本公司及本公司客戶等相關資料及內容，僅得揭露於本契約目的範圍內有接觸需要之得標廠商員工，得標廠商及其聘僱人員應保守秘密不得洩漏，並採取必要之安全措施，否則如致本公司遭受損害應由得標廠商負賠償責任；契約經終止、解除或期限屆滿後亦同。

十、得標廠商於契約履行期間應提供開發、維護（修）之服務人員名冊（含公司簽章）及經得標廠商之員工簽署之「保密同意書」至本公司備查，且對其操守行為負責。

十一、得標廠商提供本公司使用之軟硬體應為合法，如有第三者主張得標廠商提供本公司使用之軟硬體有侵犯智慧財產權時，本公司同意儘速以書面通知得標廠商，得標廠商應負責為本公司提出抗辯或和解談判，所有經法院判決確定或成立和解應由本公司負擔之費用、損害賠償及本公司因此所支付之費用（含委聘律師酬金）、所受之損害等均由得標廠商負擔。

十二、得標廠商不得將本契約或基於本契約所生之權利義務，全部或一部分轉讓或複委託予其他第三人，但經本公司事先書面同意者不在此限。

十三、經本公司事先書面同意之複委託，其範圍及限制、條件均不得超出本契約；得標廠商應確認分包商具備資訊安全措施、遵循本公司資訊安全管理制度並簽署保密協議，如因分包商之不當行為致本公司發生損害時，得標廠商應與分包商負連帶損害賠償責任。

十四、得標廠商及分包商應擬定本契約項目之服務水準(SLA)：

(一)如無法訂定本契約項目之服務水準時，須擬定補償性控制措施。

(二)違反本公司資訊安全要求或因人員疏失等原因，導致發生資安事件或未達本公司資訊安全要求之服務水準時，應依契約所定罰則計付違約金予本公司，若因此造成本公司相關損害，得標廠商應依契約內容負賠償責任。

(三)因本契約作業項目之性質、產品內容或服務，得標廠商無法提供服務水準或補償性控制措施時（如訂閱制服務、客制化套裝軟體、商業應用軟體、電腦週邊設備採購等），雙方之權利義務得依

雙方協議內容另定之。

十五、得標廠商資訊安全責任：

(一)得標廠商須遵守本公司現有各項系統管理作業規定及安全管理規範。

(二)得標廠商於契約履行期間，如得標廠商人員異動時（完成階段性任務或離職等情形），得標廠商應會同委託單位將其借用之設備、軟體或其他物件返還予本公司，並移除相關作業權限。

(三)得標廠商不得任意複製或攜出本公司非對外公開之業務資料。本公司所提供之資訊資產及資料等，得標廠商均應於契約終止、解除或期限屆滿時返還予本公司，並刪除或銷毀因執行本契約而儲存持有之個人資料檔案，且不得以任何形式留存備份。得標廠商履行契約相關事務之資料處理流程及傳輸方式，應依本公司資料安全管控規定辦理。

(四)如需使用自攜資訊設備，應經本公司檢核同意後始得使用，且不得連接本公司內部網路。

十六、得標廠商禁止使用中國廠牌資通訊產品、軟體（如應用軟體、系統軟體、開發工具、客製化套裝軟體、APP及電腦作業系統等）、硬體（包括具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備）及資通訊服務。

十七、得標廠商所屬人員倘因參加本案系統建置、維護，致本公司蒙受損害，得標廠商應與其所屬人員負連帶賠償責任。

十八、得標廠商應遵循相關法令法規及其他適當資訊安全國際標準。

十九、應本公司業務需要，得標廠商對於所開發之應用軟體同意本公司使用並重製於本公司所購置之機器中，本公司不另行付費。

二十、本公司如因業務需要對得標廠商所提供之程式或文件得作適當之修改。

二十一、得標廠商應依本公司業務需要，配合修改應用軟體之程式和文件。

二十二、得標廠商所提供之程式若有採用第三方套件（非得標廠商自行開發之程式），應明列於系統維護手冊中，且交付驗收前應確認無已知公開的風險；於保固及維護期間內若採用之第三方套件經揭露弱點風險，須配合本公司要求於期限內完成修正，本公司不另行付費。

二十三、於專案建置或維護期間內，為解決第三方套件經揭露弱點風險之修正，其解決方法、範圍、期限，得標廠商應協助評估及處理，如係非得標廠商單方修正程式得以解決者（如需作業系統、資料庫、產品升級或原廠產品已終結等），則不受前款規定限制，雙方得另議處理方法。

二十四、得標廠商所提供之程式及文件，無條件供本公司存查，惟不得公開予無關之第三者。於維護期間所開發應用程式與交付軟體，得標廠商應善盡義務執行資訊安全檢查是否內藏惡意程式，並出具相關資安檢測證明文件，本公司不另行付費。

二十五、得標廠商應配合本公司於系統軟硬體換版時，協助辨識複雜度及影響範圍，提供風險影響評估報告與上線及復原計畫操作手冊。

二十六、得標廠商依本契約提供本公司服務時，如使用開源軟體，應依該開源軟體之授權範圍，授權本公司利用，並以執行檔及原始碼共同提供之方式交付予本公司使用，得標廠商應於上線前交付開源軟體清單（包括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）。

二十七、得標廠商不得於提供之設備上做任何不當作業之行為及植入非法或足以損害正常作業與保密之功能，否則如致本公司遭受損害，應由得標廠商負賠償責任。於保固及維護期間得標廠商須配合本公司定期資安檢測作業或電腦資訊安全評估作業，例如弱點掃描、滲透測試、源碼檢測等，所檢測出之風險弱點項目，應配合本公司要求於期限內進行修正完成，本公司不另行付費。

二十八、得標廠商於上線前應配合本公司要求進行相關檢測，並提交相關無弱點檢測文件。如應用軟體程式應於上線前通過源碼檢測、系統及設備應於上線前通過弱點掃描、對外網頁版應用系統應於上線前通過滲透測試，本公司不另行付費。

二十九、依前款規定之弱點檢測如因市場工具未能支援無法提出相關檢測文件，得標廠商應出具資訊安全聲明書。

三十、 履約期間遇資安事件時，得標廠商應辦理事項：

(一)知悉發生資安事件之通報並採取適當應變措施：得標廠商知悉發生資安事件應於2小時內通知本公司（或接獲本公司通知2小時內），並採取適當之應變措施。逾時未完成，本公司得請求得標廠商按逾時時數，每小時支付契約總價款0.1％之違約金，逾時未達1小時者以1小時計。

(二)完成損害控制或復原作業：得標廠商應於知悉資通安全事件後72小時(重大資安事件為36小時)內完成損害控制或復原作業。逾時未完成，本公司得請求得標廠商按逾時時數，每小時支付契約總價款0.1%之違約金，逾時未達1小時者以1小時計。

(三)調查及處理資安事件：得標廠商完成損害控制或復原作業後，應於1個月內送交調查、處理及改善報告（或因應本公司所訂期限及指示事項提供協助調查處理相關事宜）。逾期未完成，本公司得請求得標廠商按逾期日數,每日支付契約總價款0.1%之違約金，1日以24小時計，逾時未達24小時者以1日計。

(四)前開違約金之累計總額以契約總價款之20%為上限，本公司並得自契約總價款、履約保證金或保固保證金中扣抵。如違約金總額達契約總價之20%時，本公司得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。

貳、報價

一、 得標廠商以新臺幣為報價基礎，且分別依下表列出價格：

單位：元

項次	品名	數量	單價	總金額
1	第三方元件管理與檢測 Checkmarx One SCA 訂閱授權 -30 Projects	1		
			合計	

*以上報價應依規格內容報價（含稅）。

參、交貨

一、得標廠商須於本公司簽約次日起2個月內交付本案軟體授權，如逾此期限，得標廠商須依照下列公式計付違約金予本公司：

違約金 = 契約總價款 * 0.1% * 逾期日數

二、如逾期超過前項約定期限1個月仍未完成交付時，除仍應依前述規定計付違約金外，本公司得通知終止或解除契約之部分或全部，並沒入履約保證金。

三、前開違約金之累計總額以契約總價款之20%為上限,本公司得自契約總價款或履約保證金中扣抵。

肆、驗收與付款

得標廠商依約交付相關文件後，由本公司派員辦理驗收，驗收合格後支付契約總價款。交付文件如下：

(一)軟體授權證明文件。

(二)交貨簽認單。

(三)教育訓練教材含教育訓練簽到表。

伍、維護及保固：

一、得標廠商於本公司完成驗收之次日起，負責維護及保固1年，本公司不另行付費。

二、得標廠商須提供服務水準應包含以下事項：

(一)維護時間為本公司營業日上午9時至下午5時。

(二)本公司發現本案系統異常時，得標廠商須於收到本公司通報後1小時內回應，並透過電話服務協助系統問題之判斷、偵錯與故障排除，如有進一步到場鑑定維護之必要，須於收到通報後4小時內（含交通時間）到場服務。

(三)得標廠商應於原廠發布系統新版本時，需依本公司要求進行更新版本作業。

(四)得標廠商應負責本案系統問題排除及技術支援

三、得標廠商違反上述服務水準規範時，每違反1次，本公司得按本契約總價之0.1%計算懲罰性違約金。

四、懲罰性違約金之累計總額以契約總價款之20%為上限。如懲罰性違約金總額達契約總價之20%時，本公司得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。

五、得標廠商依各款應付之懲罰性違約金可自契約總價、履約保證金或保固保證金中扣抵。

陸、得標廠商應提供本案相關教育訓練 2 小時以上，本公司不另行付費。

柒、得標廠商應對本案契約內容充分瞭解，並應依本公司之解釋切實執行辦理。