全國農業金庫入侵偵測防禦系統1年授權及保固
規格及特別條款

全國農業金庫（以下稱本公司）採購「入侵偵測防禦系統1年授權及保固」（以下稱本案系統)乙案，其規格及特別條款規定如下：

甲、規格

壹、一般規定

一、本案廠商應於投標時提供下列證明文件：

(一)提供原廠或代理商所開立之經銷授權證明文件。

(二)本案廠商於公開招標日近3年內，應具備2家以上金融機構(銀行業、證券業、保險業)或金融周邊機構之入侵偵測防禦系統相關專案服務經驗。

(三)至少2位以上工程師具備下列至少1項之國際資安管理證照。

- ISO 27001資訊安全管理系統主導稽核員考試合格證書。
- Certified Information System Security Professional (CISSP)。
- Certified Information Security Manager (CISM)。
- EC-Council Certified Ethical Hacker (CEH)。
- EC-Council European Citizen Science Association (ECSA)。
- EC-Council Certified Incident Handler Course (ECIH)。
- EC-Council Computer Hacking Forensic Investigator (CHFI)。
- EC-Council Certified SOC Analyst (CSA) 。
- Offensive Security Certified Professional (OSCP)。
- Offensive Security Exploit Developer (OSED)。
- Offensive Security Web Expert (OSWE)。

(四)上述工程師於本案廠商服務之勞健保證明或在職證明。

二、本案廠商須提供保固期間內所需之軟體升級服務，本公司不另行付費。

三、本案廠商須依本規格及特別條款甲之「貳、軟體規格」及「參、功

能規格」需求，於本公司資訊環境建置、設定本案軟硬體設備，直至本公司能順利運轉本系統資安防護機制，以符合需求。

四、本案廠商應按投標金額5%之現金、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，未得標者無息退還押標金。

五、本案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條規定之期限內，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、軟體規格

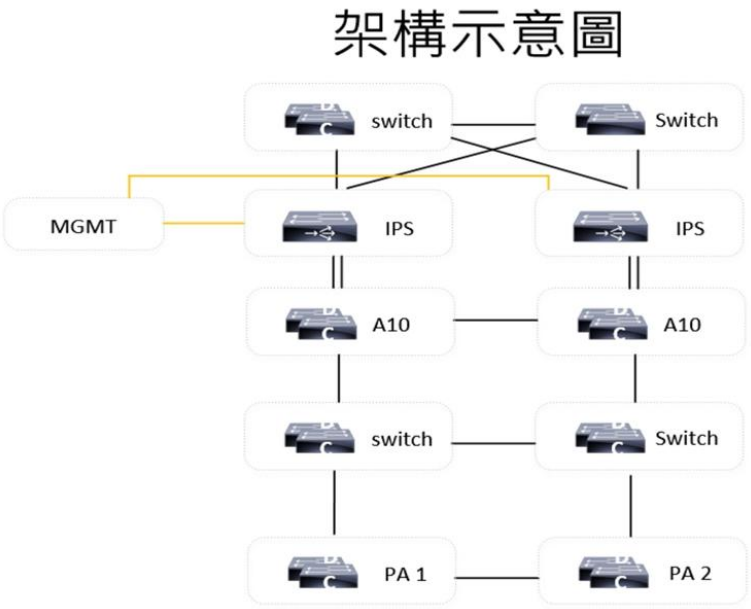
一、系統授權：

(一)入侵偵測防禦系統 1 年授權及保固(Radware DefensePro X10 - 500M)

二、授權及維護期間：民國(以下同)115 年 5 月 20 日起至 116 年 5 月 19 日止。

參、功能規格

一、系統架構圖：



二、系統規格：

(一)系統效能達 500 Mbps，未來可透過 License Upgrade 到 5Gbps。

(二)網路介面最高可達 16 個 10/100/1000 Mb copper 埠及 8 個 10G SFP+ 埠清洗流量介面，提供 8 個 10/100/1000Mb Copper 埠。

(三)具備獨立管理網路介面及 Console 埠，提供分權管理機制可由不同屬性管理者分別管理。

(四)DoS/DDoS 攻擊抵禦處理效能 Mitigation Throughput 達 10Gbps。

(五)DoS/DDoS 攻擊抵禦處理效能 DDoS Flood Attack 達 14Mpps。

(六)網路延遲效能低於 60 micro seconds。

(七)SSL/TLS 訊務處理效能可達 43k Connections per Second (RSA 2k)。

(八)支援 TLS 1.3 Perfect Forward Secrecy (PFS) 硬體加速模組。

(九)DoS/DDoS 攻擊抵禦處理效能 Max Attack Concurrent Session 無上限。

(十)可即時動態產生異常流量 Signature。

(十一)提供 Behavioral DoS 緩解機制，可用機器學習演算法自動防禦已知的及零時差 DoS/DDoS flood 攻擊，包含 TCP Floods、 UDP Floods、ICMP Floods、IGMP Floods 及 TCP/UDP fragmented Flood。

(十二)具備多種攻擊回應機制，包含 Drop packet、reset(source、destination、both)、suspend(source port、destination port or any combination)、Challenge-Response for HTTP and DNS attacks。

(十三)支援 Inline、SPAN Port Monitoring、Copy Port Monitoring 及 Out-of-path mitigation 等運作模式。

(十四)支援 VLAN Tagging、L2TP、MPLS、GRE 及 GTP 等 Tunneling 網路協定。

(十五)支援 IPv6 網路，並可阻擋 IPv6 攻擊。

(十六)可防禦針對 DNS 伺服器的 flood attacks。

(十七)可防禦針對 HTTP 伺服器的 http flood attack。

(十八)可防禦針對 Mail servers、FTP servers、SIP servers、MS-SQL servers 及 MySQL server 的 Brute-force 及 dictionary 列舉攻擊。

(十九)提供 connection limit 功能，可防禦 half open SYN attacks、request attacks 及 full session attacks。

(二十)提供國別阻擋功能(GeoIP)與 IP 信譽清單(EAAF)，限制來自特定國家的網路流量。

(二十一)防禦各種主要服務及伺服器已知弱點，包含 Web、Mail Server、FTP、DNS、SIP、SNMP、Worms、Viruses、Backdoors、Trojans、Cross-site Scripting、SQL Injection、Spyware。

(二十二)提供中控平台(Cyber Controller X 10 Gbps attack capacity)，含: 多設備管理和監控功能、即時監控儀表板、攻擊統計分析報表、自動排程功能、自動告警功能。

(二十三)須建立入侵防禦系統容錯負載機制，如遇單點失敗問題可自動切換保持防護正常運作。

乙、特別條款

壹、本案廠商同意履行以下情事：

一、本案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。本案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。

二、本案廠商應依本公司各項作業委外相關業務規章訂定之標準作業程序，執行消費者權益保障、風險管理、內部控制及內部稽核制度，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。

三、本案廠商同意金融監督管理委員會、中央銀行、中央存款保險股份有限公司、農業部農業金融署等機關或依農業金融法第7條規定之

機關及本公司自行辦理或委託獨立第三方單位進行辦理本契約應辦事項之稽核或依金融機構作業委託他人處理內部作業制度及程序辦法進行本契約相關事項年度查核與稽核作業。本案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。

四、本案廠商若有違反契約約定情事發生，除契約另有約定外，本公司得於通知本案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。

五、本案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。

六、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，本案廠商應立即以口頭、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。

七、保密義務:

1. 本案廠商因履行契約應辦事項所知悉或存放於本案廠商雲端空間之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本案廠商員工，本案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本案廠商負賠償責任；契約經終止、解除或期限屆滿後亦同。

2. 本案廠商於契約履行期間應提供本案廠商服務人員名冊（含公司簽章）及「廠商服務人員保密同意書」至本公司備查，且應加強對其聘僱人員之管理，包括人員進用、考核及處分等情事，以避免有不適任或有不法情事發生。

八、本案廠商提供本公司使用之軟硬體應為合法，如有第三者主張本案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本案廠商，本案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）、所受之損害等均由本案廠商負擔。

九、因本契約作業項目之性質、產品內容或服務如(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），本案廠商無法提供服務水準或補償性控制措施時，雙方之權利義務得依雙方協議

內容另定之。

十、本案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。

十一、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；本案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，本案廠商應與分包商負連帶損害賠償責任。

十二、本案廠商資訊安全責任：

1.本案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，此外本公司保有對本案廠商執行稽核權利，包含稽核結果之改善追蹤機制，本公司可自行辦理或委託獨立第三方執行資訊安全訪視作業，或由本案廠商提供公正第三方之驗證報告。

2.本案廠商於契約經終止、解除、完成履約後或其人員異動時（完成階段性任務或離職等情形），本案廠商應完成本公司資訊資產與資料返還、移交、刪除或銷毀，並移除本案廠商於服務期間所取得之實體與邏輯存取權限，並保留執行紀錄。

3.本案廠商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。

4.本案廠商所提供之服務如發生變更，應於變更前主動以書面文件告知本公司相關事宜，包括但不限於契約變更、本案廠商組織重大調整、業務重大異動或契約提前終止等；如本案廠商服務內容異動對資訊安全有所衝擊，本案廠商應重新協助本公司需求單位進行存取風險之辨識評估及對高風險變更之處置對策，並填寫相關風險評估表。

5.因本案廠商及其人員或分包商之因素，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懲罰性違約金予本公司，若因此造成本公司相關損害，本案廠商應與及其人員或分包商依契約內容負連帶賠償責任。

十三、本案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。

十四、本案廠商依本契約提供本公司服務時，如使用開源軟體，禁止使用高拘束性授權(如：AGPL授權)、中國開發套件或嚴重風險與高風險弱點套件。

十五、本案廠商因履行契約應辦事項所應負之損害賠償責任，悉依民法及相關法令辦理。

十六、本案廠商應遵循相關法令法規及其他適當資訊安全國際標準。

十七、本案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；本案廠商若無法提供時，應提供資通安全管理措施或配合本公司自行辦理或委託獨立第三方執行資訊安全訪視作業。

十八、本案廠商所提供之程式、檔案與軟體，無條件供本公司存查，惟不得公開予無關之第三者。於契約履行期間所開發應用程式與所交付軟體，本案廠商應善盡義務執行資訊安全檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、後門程式、間諜軟體及勒索軟體等）及隱密通道（Tunnel channel）等，並出具相關資安檢測證明文件。於上線前應清除正式環境之測試資料與帳號及管理資料與帳號，並採取防止電腦病毒散布之處置措施，以確保本公司之資訊系統安全無虞；如本案廠商未盡上述義務，致本公司因此所受一切損害（含本公司依法對第三人應負賠償責任及應給付之罰鍰），廠商應負賠償責任。

十九、本案廠商需指派專人配合本公司資訊安全要求，並負責督導本案廠商專案成員辦理各項本公司資訊安全要求事項，例如弱點掃描等，資安檢測發現之風險弱點項目，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、本案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。

二十一、本案廠商所提供之程式若有採用第三方套件(非本案廠商自行開發 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；於契約履行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。

二十二、契約履行期間內，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，本案廠商應協助評估及處理，如係非本

案廠商單方修正程式得以解決（如需作業系統、資料庫、產品升級或原廠產品已終結等），且經本公司確認者，則不受前款規定限制，雙方得另議處理方法。

二十三、本案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，應由本案廠商負賠償責任。

二十四、本案廠商應配合本公司要求進行相關檢測，系統及設備應於上線前通過弱點掃描，並提交相關無弱點檢測文件，本公司不另行付費。

二十五、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，本案廠商應出具資訊安全聲明書。

二十六、本公司如因業務需要對本案廠商所提供之程式或文件得作適當之修改。

二十七、本案廠商須配合本公司進行營運持續計畫(BCP)演練。

二十八、因可歸責於本案廠商而終止契約，本公司得要求本案廠商應將終止前已進行但尚未完成之工作成果及相關文件，依現狀交付予本公司，並同意本公司得就其未完成之工作成果自行或委由第三人繼續完成，本案廠商不得對該未完成之工作成果及相關文件主張任何權利。

貳、維護及保固：

一、本案廠商依本案系統授權期間，負責系統維護及硬體保固 1 年，本公司不另行付費。

二、本案廠商必須提供本案系統之技術工程師於本公司營業時間(上午 9 點至下午 5 點)待命維修之服務，以維護本案系統之正常運作，如於非本公司營業日遇有本案系統異常之情事，則最遲於次1營業日完成維修恢復運作。

三、到場技術支援地點為本公司及機房，時間以本公司營業時間(上午9點至下午5點)為原則，如遇機房搬遷、緊急系統異常情形等，須配合本公司非營業時間外出勤支援事件排除作業，本公司不另行付費。

四、本案廠商須提供專業技術服務及售後服務項目應至少包含下事項：

1.如原廠發布本案系統相關弱點須立即以電子郵件、簡訊、電話

等方式進行通知本公司，並提供事件分析報告與處理步驟。

2.提供線上諮詢與處理、如有遠端無法處理，需到場協助處理。

3.本案廠商應負責本案系統問題排除及技術支援，如本公司發生資安事故，需到場協助處理相關因應措施：

(1)攻擊流量封鎖：配合調整本防禦系統阻擋策略，確保本公司網路可用性。

(2)攻擊特徵分析：提取並分析本系統之安全日誌紀錄，協助判定攻擊類型及來源。

(3)規則校調優化：針對已知漏洞或特定攻擊，即時更新防護規則並進行壓力測試，防止二次事故。

4.提供月報表分析，每月到場進行系統維護與分析說明，並提出相關防護建議。

5.提供系統更新升級服務，於原廠發布新版本時，需協助本公司進行系統升級更新作業。

6.本案廠商應協助本公司撰寫系統備援演練計畫，必要時配合進行演練作業。

7.其他經本公司與本案廠商雙方協議需由本案廠商提供之維護。

參、報價

本案廠商以新臺幣(以下同)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
一	入侵偵測防禦系統1年授權及保固(Radware DefensePro X10 - 500M)	乙式	000	000
總金額				000

*以上報價應依規格內容報價（含稅）。

肆、交貨

一、本案廠商須於本公司簽約次日起2個月內交貨，如逾此期限，本案廠商須依照下列公式計付懲罰性違約金予本公司。

懲罰性違約金 = 契約總價款 * 0.1% * 逾期日數

二、如逾期超過2個月仍未完成交貨時，除仍應依前述規定計付懲罰性違約金外，本公司得通知終止或解除契約之部分或全部，並沒收履約保證金。

三、本案逾期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、履約或保固保證金中扣抵。

四、本案為維運中系統，僅需更新授權，無需另外安裝與測試。

伍、驗收與付款

一、本案廠商依約交付以下相關文件後，提出經本公司簽認之驗收文件交付簽認單，由本公司派員辦理驗收，驗收合格後，支付契約總價款。

二、應交付相關文件如下:

1.入侵偵測防禦系統(Radware DefensePro X10-500M)1 年授權及保固證明文件。

陸、本案廠商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。

資訊安全與服務水準協定(SLA)罰則

一、資訊安全與服務水準規範：

項目	項次	項目	規範標準
資訊安全	1	資訊安全管理	如有洩密、疏失、管理不善等情事，致本公司遭致損失。
	2	存取控制及保全	因故意或過失導致本公司資訊資產遭不當取得、刪除或變更等情事。
	3	事件通報	引起本公司發生資訊安全事件且未即通報造成損失。
	4	威脅及弱點修補	系統重大弱點公布後或內部弱點掃描檢測未於規定之時間內修補完畢。
服務水準	1	系統可用性	每月以 95%以上的服務可用時間為服務承諾。
	2	客服支援時段	技術支援服務時間規定為本公司之營業日（上午 9 點至下午 5 點），若因國定假日異動則以公告為準。
	3	服務中斷	服務可用性每月中斷時間累計不得高於 6 個小時以上。
	4	問題回應時間	接獲本公司通知後（含電話、 簡訊、E-Mail、傳真、書面或其他通訊軟體等），須於通報後 5 日內回應,一般處理時間不應超過收件後隔日起算 10 日內，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 3 日內到場服務。
	5	復原點目標	發生故障時，將 VM 故障點之服務狀態還原至其他虛擬主機繼續提供服務。

二、相關說明：

(一)本案廠商違反資訊安全與服務水準規範，如須延長日期或非本案廠商之問題(不納入計罰)，須經本公司同意。

(二)本案廠商違反資訊安全與服務水準規範時，每違反 1 次，本公司得按契約總價之 0.1%計算懲罰性違約金。

(三)本案廠商指派之專案負責人及工作成員，未經本公司同意，不得更換，如有未經本公司同意自行更換時，每更換 1 次得依契約總價之 0.1%計算懲罰性違約金。

(四)本案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，包含版面及內容皆須嚴格要求一致性及正確性。交付之文件經本公司審閱，所發現錯漏處達 10 處以上，或業經本公司要求修訂仍未修訂者，本公司得按每字新臺幣 1,000 元計算懲罰性違約金。

(五)如違約金總額達契約總價之 20%時，本公司得通知本案廠商終止契約或解除契約之部分或全部，且不補償本案廠商所生之損失。

(六)本案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。