國家資通安全研究院
National Institute of Cyber Security

第二屆產品資安漏洞獵捕
活動辦法

主辦單位：國家資通安全研究院

活動信箱：bounty@nics.nat.gov.tw

目　錄

1. 活動簡介

為強化政府機關常用軟體之資安韌性，降低軟體供應鏈遭利用所衍生之資安風險，國家資通安全研究院(NICS，以下簡稱資安院)將於 115 年 10 月至 11 月辦理「第二屆產品資安漏洞獵捕活動」。

本屆活動以「軟體供應鏈安全驗證」為核心，聚焦政府機關高使用率、高風險或具關鍵資安功能之軟體產品，由廠商(藍隊)提供產品與測試環境，透過漏洞獵捕機制，邀集資安專業人員(紅隊)針對指定測試標的進行安全測試、漏洞挖掘及通報，雙方在公平透明的機制下攜手合作，協助及早發現產品潛在資安弱點，降低政府機關軟體應用環境之整體風險，並由資安院(紫隊)，審核通報結果與賞金判定，維護判定公正與一致性，並維持網路連通性與測試場域穩定，確保活動順利運作。

本活動由數位發展部資通安全署指導，資安院統籌規劃與執行，建立安全且可控管之漏洞通報與修補機制。透過紅隊、藍隊及紫隊之三方協作，確保產品安全與使用者信任、提升供應鏈資安治理能力，並作為政府推動產品資安與供應鏈安全管理之重要實務基礎。

2. 活動期程

本活動自 115 年 6 月 30 日公告起展開，依序分為藍隊報名、作業整備、紅隊報名及正式活動四個階段，以確保流程完整並維持活動品質。本活動預計自 115 年 7 月起於 TWCERT/CC 網站公告受理報名，並依序辦理報名、審查、作業整備、正式活動及成果彙整等作業。實際期程得由資安院視作業情形調整，並以活動網頁正式公告內容為準。

階段	預計期間	主要內容
活動公告	115 年 6 月 30 日	資安院公告第二屆活動資訊，並受理藍隊廠商報名
藍隊報名	115 年 7 月 1 日至 8 月 31 日	藍隊應於期限內完成報名文件繳交，並提供受測標的、測試方式、獎金設定及聯絡窗口等資料
藍隊資格審查與標的確認	115 年 7 月 1 日至 9 月 7 日	資安院辦理藍隊報名文件審查，確認參與資格、受測標的、測試範圍、場域需求、獎金配置及相關配合作業
活動獎金與參與標的公告	115 年 8 月 31 日至 9 月 1 日	• 公告活動獎金池總額 • 實際公告內容得依藍隊公開意願及保密規範調整
活動作業整備	115 年 7 月 1 日至 8 月 31 日	• 藍隊配合完成環境建置與測試、連線確認等作業 • 活動開始前各項作業就緒
紅隊報名與資格審查	115 年 9 月 1 日至 9 月 30 日	• 資安院受理紅隊資安專業人員報名 • 紅隊應於期限內完成報名文件繳交；資安院原則上於收件後 5 個工作天內通知審查結果

階段	預計期間	主要內容
正式活動期間	115 年 10 月 1 日至 11 月 30 日	• 紅隊依活動規範針對指定標的進行漏洞挖掘及通報 • 藍隊負責確認漏洞內容並配合必要技術說明 • 資安院辦理通報初審、爭議處理、漏洞等級判定及獎勵裁定等作業
成果彙整與獎金核發	活動結束後辦理	• 資安院彙整活動成果、有效漏洞件數、漏洞類型及相關統計資料 • 藍隊依資安院裁定結果辦理獎金核發 • 如涉及爭議案件者，於資安院完成最終裁定後另行辦理

備註：為確保活動品質，資安院得視報名情形、受測標的準備狀況、測試環境穩定性或其他必要因素，調整各階段時程、報名方式、公告內容及活動執行細節，並於活動網頁或以電子郵件通知相關參與者。

3. 活動目標

3.1 活動目標

本屆活動之目標如下：

- 強化政府機關及民生常用軟體之資安驗證，降低軟體供應鏈風險。
- 針對高使用、高風險及關鍵資安軟體建立實測導向之漏洞發現機制。
- 促進參與廠商建立產品安全修補、通報回應及供應鏈風險管理流程。
- 透過獎金誘因擴大資安研究人員參與，提高漏洞通報品質與實務效益。
- 累積政府常用軟體之風險樣態，作為後續採購規範、驗收要求及產品資安治理政策之參考。

3.2 目標領域

本屆活動以「軟體供應鏈安全驗證」為主軸，重點關注政府機關於日常業務、資安防護、系統維運或政策推動中經常使用之軟體產品，特別是涉及第三方元件、開源套件、更新機制或供應商維運等供應鏈環節者。本活動透過漏洞獵捕協助驗證軟體本身及其供應鏈各環節之安全性，降低因軟體弱點或供應鏈缺陷所可能造成之資通安全風險。

3.3 測試標的

本活動測試標的以「政府機關常用軟體」為主、「民生軟體」為輔，並以可提供明確測試範圍、測試環境及必要操作資訊者為優先。測試標的類型包含地端軟體、地端軟體含 Agent、SaaS 服務、APP、網站等軟體或服務型態。

藍隊應依受測標的型態，提供必要之測試環境、測試帳號、網站或系統入

口點、使用手冊、Agent 取得與安裝說明、APP 下載方式、帳號命名規則或其他足以確認測試範圍與可用性之資訊。若測試標的涉及正式環境、正式環境複製版本或環境，藍隊應事前明確說明測試邊界及可測試範圍。

本活動優先納入下列類型，惟不以此為限：

- 高使用率軟體

  政府機關廣泛部署、使用頻率高，若發生漏洞可能造成大規模影響之軟體。

- 高風險軟體

  涉及帳號權限、資料處理、遠端連線、系統管理或外部連通功能，若遭攻擊可能造成未授權存取、資料外洩或系統遭控制之軟體。

- 關鍵資安軟體

  政府機關用於資安防護、組態管理、弱點管理、端點防護、監控偵測或基準檢核之軟體，例如 VANS、GCB 等相關應用或工具。

- 供應鏈關聯軟體

  涉及第三方元件、開源套件、更新機制、外掛模組或供應商維運服務之軟體，且其弱點可能影響政府機關資通系統安全者。

3.4 獎金池說明

本活動獎勵分為「單一漏洞獎金」與「資安院加碼獎勵／排名獎勵」二類。

單一漏洞獎金係針對經資安院裁定為有效之漏洞通報，依漏洞嚴重程度、可利用性、影響範圍及是否具供應鏈風險等因素核定，由藍隊依本辦法規

定及活動公告之獎金標準辦理核發。

資安院加碼獎勵／排名獎勵，係為鼓勵紅隊提升漏洞挖掘品質與參與度，由資安院依紅隊有效漏洞通報之 CVSS v4.0 累計分數進行排名核定。相關獎勵名額、金額及核發條件，依活動公告或資安院正式通知內容辦理。

所有漏洞通報須經資安院審查與裁定為有效漏洞後，始具獎勵資格。資安院得視活動募集情形、參與廠商數量、測試標的範圍及實際通報成果，調整各類標的之獎金配置與核發方式，並以活動公告或正式通知內容為準。

4. 參與對象

本活動參與者分為紅隊、藍隊及紫隊三大角色。紅隊為資安研究人員及具漏洞挖掘能力之資安專業人員；藍隊則為政府機關常用或民生軟體之提供者、開發商、維運商或相關責任單位，負責提供測試標的資訊、協助漏洞確認及後續修補作業；紫隊為資安院，負責審核通報結果與賞金判定，維護判定公正與一致性，並維護網路連通性與測試場域穩定，確保活動順利運作。透過紅、藍、紫三方協同合作，得以及早發現並修補產品漏洞，強化我國產品資安防護。

4.1 紅隊

紅隊研究員主要由資安研究人員及具備漏洞挖掘能力的專業人士組成，採自願性參與方式。紅隊負責針對受測標的進行漏洞測試與通報，並依計畫規範獲得獎勵。

4.1.1 參與資格

- 須具中華民國國籍。
- 須遵守本活動之測試範圍與相關規範。
- 須遵守利益迴避原則：紅隊研究員或其所屬團隊如曾參與受測標的(產品)之設計、開發或防禦部署，致與該受測標的具利益衝突之虞者，應主動迴避，不得對該標的進行漏洞挖掘或通報。
- 未滿 18 歲者需經法定代理人同意並共同簽署相關文件。
- 參加者若經查核涉及下列情事，資安院得隨時取消其參與資格並得由藍隊追回獎勵與獎金：

  – 違反本活動相關規範。

– 違反本活動利益迴避原則，包括未依規定主動揭露或申請迴避者。

– 曾因內亂罪、外患罪、國家安全法、反滲透法、國家情報工作法、國家機密保護法等罪，經法院判決有罪或尚在通緝中。

– 未經授權，與外國情治單位或大陸、香港、澳門官方機構有聯繫接觸紀錄。

– 曾受外國或敵對勢力利誘、脅迫，從事不利國家安全或重大利益之行為。

– 曾因洩密罪或違反安全保密規定，經法院判決或受行政處分。

4.1.2 參與證明

為鼓勵紅隊研究員加入本次活動，若紅隊研究者有需求者，可向資安院索取參與證明或成果證明。

4.2 藍隊

藍隊為政府機關常用或民生軟體之提供者及維運責任單位，應配合提供受測標的資訊、測試範圍、必要環境及漏洞確認窗口，並於活動期間協助進行漏洞確認、申訴、修補建議回應及獎金核發等作業，並確保產品於活動期間正常運作。透過參與漏洞獵捕，廠商能提前掌握產品資安風險，展現品牌對安全的承諾，並逐步建立資安治理機制。

4.2.1 參與資格

- 藍隊成員為本活動測試標的之軟體提供者、開發商、維運商、代理商或其他經資安院認定與測試標的具管理、維護或修補責任之單位。
- 須為本國以政府機關常用軟體為主、以民生為輔，並優先關注高使用、

高風險及關鍵資安軟體。

- 須遵守本活動規範，並依規定完成漏洞確認並進行修補。

4.2.2 參與證明

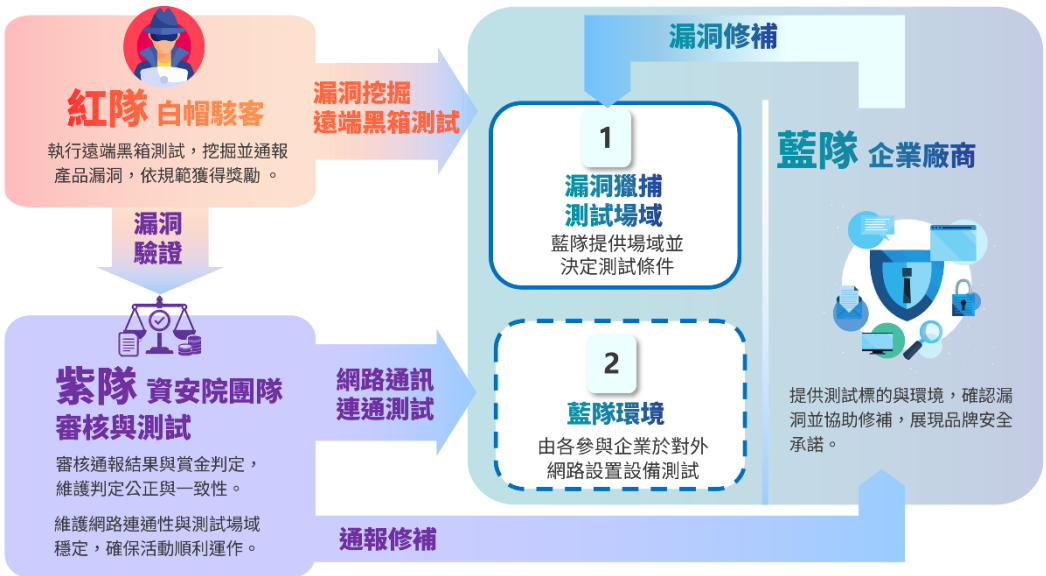
為鼓勵與感謝廠商(藍隊)提供產品與測試環境加入本次活動，資安院將提供廠商活動參與證明，以感謝廠商重視產品資安與共同為降低軟體供應鏈風險付出之努力。

5. 活動辦法與相關流程規範

本活動之執行流程由多方角色共同參與，透過明確分工確保活動順利推進。主要參與角色如下：

- 紅隊(漏洞挖掘團隊)：負責執行遠端黑箱測試，挖掘並通報產品潛在漏洞。另依據說明需要，於本文件中將使用「紅隊」、「通報者」或「漏洞挖掘者」代表此角色。
- 藍隊(民間企業)：提供受測標的與必要測試環境，並確認紅隊所通報之漏洞。另依據說明需要，於本文件將使用「藍隊」、「廠商」或「標的提供者」代表此角色。
- 紫隊(資安院審核及測試團隊)：負責審核、裁定通報結果與獎勵歸屬，確保判定之公正與一致性；以及負責進行網路通訊與連通性測試，確保受測標的與測試場域可用、穩定，協助活動順利運作。另依據說明需要，於本文件亦將以「紫隊」或「主辦方」代表此角色。

各角色於活動中之互動與責任分工如下圖所示：



本圖示意紅隊透過遠端測試進行漏洞挖掘，通報後交由藍隊確認，紫隊則負責審核與最終裁定。

5.1 時程規範

本活動規範所稱日(天)數，依以下方式計算：

- 除另有說明外，係以工作天計算。
- 以日曆天計算者，工作天、依行政院人事行政總處所公告認定之放假日及全國性選舉投票日及行政院所屬中央各業務主管機關公告應全國放假之日，均應計入；惟活動開始前未可得知之放假日(如颱風假)，不予計入。

5.2 報名流程

本活動採報名制，由資安院公告活動資訊後，參與者須於期限內下載並填寫報名文件，完成後寄送至指定信箱(bounty@nics.nat.gov.tw)。資安院將進行文件審查，必要時得通知補正；參與者需能於報名截止日前完成補正並經審查通過，始視為完成報名程序。

5.2.1 報名公告與文件下載

本活動資訊將公告於資安院(https://www.nics.nat.gov.tw/)網站，並同步於TWCERT/CC(https://www.twcert.org.tw/)網站提供報名文件下載(如報名表、個人資料使用同意書、保密協議書等文件)。

5.2.2 報名文件繳交

- 紅隊：於報名期限內，將「報名表暨保密協議書與個人資料同意書」，寄至活動信箱(bounty@nics.nat.gov.tw)。

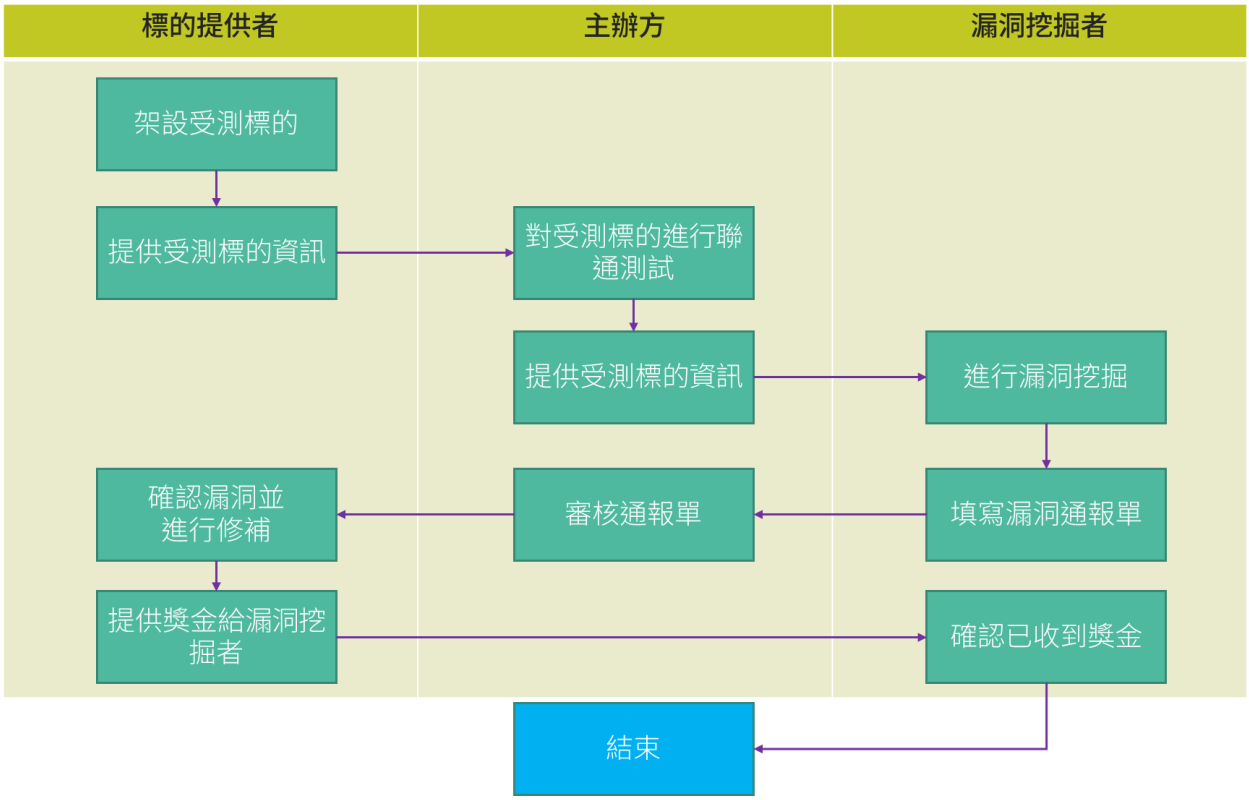
- 藍隊：於報名期限內，將「報名表暨保密協議書」寄至活動信箱(bounty@nics.nat.gov.tw)。
- 文件若不完整，資安院得通知補正；參與者需能於報名截止日前完成補正，始得視為有效。

5.2.3 報名文件審查與通知

- 資安院於收件後進行報名文件審查，原則上於 5 個工作天內以電子郵件回覆收件狀況；惟實際回覆時間，得由資安院視個案情形裁量決定。
- 經資安院審查通過並以電子郵件通知後，始視為完成報名程序。
- 活動相關資訊(含漏洞挖掘受測標的)將於正式活動開始前，由資安院以電子郵件通知合格參與者，其不對外公開。

5.3 漏洞挖掘流程

本活動之漏洞測試由藍隊廠商提供受測標的，資安院於測試開始前進行環境檢測及連通性確認，以確保測試場域之可用性與穩定性。紅隊研究員須透過「TWCERT/CC 漏洞獵捕活動資訊網頁面」(活動開始另行以電子郵件通知)取得最新標的資訊後進行測試。紅隊僅得於規定期間內依本活動規範執行遠端黑箱測試，對指定標的進行漏洞挖掘，並應避免任何破壞性行為。測試過程中，若受測標的出現重大異常或中斷，藍隊應提供必要之技術支援，以確保活動能順利進行。



5.3.1 受測標的提供

參與本活動之廠商請提供欲受測之軟體產品做為「受測標的」，提供方式有以下 2 種。

1. 廠商自行維護：將受測標的連接至藍隊自行維護之外網，供紅隊可遠端針對受測標的進行漏洞挖掘作業，並請廠商於計畫期間持續維持受測標的之可用性。

2. 資安院維護：若藍隊無法自行設置網路供紅隊進行測試，可選擇將受測標的建置於資安院所選定之場域，並由場域提供對外連線方式供漏洞挖掘者進行檢測，若受測標的出現嚴重異常狀態，需請標的提供者給予必要之技術支援。資安院完成受測標的設置後，將提供相關 IP/Port 資訊予標的提供者，以利確認其標的連線情形。廠商應提供足以驗證漏洞之測試環境、測試帳號、必要文

件、API 或操作說明，實際由廠商自行依風險評估結果決定是否要用正式環境參與活動。

2 種標的提供方式皆應保持其受測標的之正常運作，以利漏洞挖掘者可於活動期間持續作業。標的提供者應於收到漏洞通報書後，確認漏洞之有效性，並依漏洞裁判書結果進行漏洞挖掘獎勵與獎金發放作業(依第 5.6 規定辦理)。

有關廠商於活動中之配合作業項目如下：

1. 於活動前選定本次受測標的，並提供其名稱、型號及連線方式或 IP 位址予資安院。
2. 廠商得自行遴選公司產品作為受測標的，所提供之受測標的應具備可連線之實測環境，以利測試驗證及提升漏洞挖掘效益，由資安院依活動目標、標的風險及場域量能審查確認。
3. 於漏洞挖掘執行期間，持續確保受測標的之可用性，若接獲通知受測標的已無法正常連線或執行功能，應即協助進行故障排除以利漏洞挖掘作業持續進行。
4. 收到資安院提供之漏洞通報書後，於 5 日工作日內進行漏洞確認，若針對漏洞判定有疑慮，填復漏洞申訴書後提供資安院進行裁定。
5. 完成漏洞通報審核後並於本活動結束後 30~45 日工作日內，依照資安院提供之通報者資訊頒發對應獎金給通報者，並保留匯款紀錄。

5.3.2 受測標的資訊提供

為確保漏洞獵捕活動能順利進行，藍隊需於活動開始前完成受測標的之準備與資訊提供，每家廠商受測標的以 3 組為限，並於活動全程維持標的之可用性。標的撤除或中斷僅得於特定情況下進行，以維護測試之公平性與連續性。

- 藍隊應於活動前提供本次計畫受測標的，並至 TWCERT/CC 漏洞獵捕活動資訊網頁面(活動開始另行以電子郵件通知)填寫標的名稱、型號及連線方式或 IP 位址等資訊。
- 藍隊完成系統整備後，須通知資安院進行複核，以確認受測標的之可用性與穩定性。
- 配合事項：
  - 受測標的應於整個活動期間維持可用，僅於產品遭遇重大影響(如服務重大中斷、產品安全性嚴重受損等)，或藍隊設定之獎金總額已達上限時，方得撤下並停止測試。
  - 資安院將不定期檢查並確認受測標的之連線狀態，若發現異常，得要求藍隊立即處置並回報。

5.3.3 受測標的資訊取得

藍隊應於活動期間持續更新標的資訊；紅隊則應透過 TWCERT/CC 漏洞獵捕活動資訊網頁面(活動開始另行以電子郵件通知)登入並下載最新版資訊，作為測試依據。

5.3.4 漏洞挖掘測試

紅隊應依活動規範執行遠端黑箱測試，測試範圍僅限於本活動所指定之受測標的。

測試結果應以可重現、可驗證之漏洞為限，並須於活動結束前完成通報。有關漏洞認定排除項目，將依本活動「5.4.5 裁定與結果之漏洞認定標準」辦理。若經查違反規定，資安院得取消其參與資格並追回已發放之獎勵與獎金。

紫隊將於漏洞挖掘過程中持續監測網路連線狀態，以確保標的可用性。

5.4 漏洞通報流程

紅隊完成漏洞測試後，應依活動規範填寫漏洞通報書，並以報名成功信件所提供之約定密碼加密，於期限內寄至活動信箱(bounty@nics.nat.gov.tw)。資安院將進行初審，如有缺漏得通知補正，補正次數以 2 次為限。通過初審後，其漏洞通報書將轉交藍隊確認，藍隊如有爭議得提出漏洞申訴，申訴次數以 2 次為限，最終結果以資安院裁定為準。

5.4.1 漏洞通報書下載與填寫要求

紅隊須透過 TWCERT/CC 平台下載官方制式漏洞通報書範本，並依範本格式完整填寫。

通報書內容至少包含：

- 基本資料：通報者基本資料。
- 使用 IP：漏洞測試來源 IP。
- 漏洞說明：成因、影響程度及建議 CVSS v4.0 基礎評分(CVSS-B)。
- 利用步驟：詳細操作步驟，附必要截圖作為證據，以證明漏洞具可重現性及可驗證性。

- 使用工具(含 AI 工具)：列出所用工具。
- 修補建議：提供可行修補方式或風險緩解措施。
- 修補複測：通報者得依意願選擇是否協助藍隊進行修補後之複測。

紅隊於測試及通報過程中，應遵守最小揭露原則，僅得取得足以證明漏洞存在之最小必要資料，不得大量查詢、匯出、下載、保存、複製、使用或散布受測標的內之資料、個人資料、營業秘密或其他機敏資訊。

5.4.2 通報書送交

- 完成通報書後，須以 PGP 加密或約定密碼(隨附於報名成功信件中)加密後寄送至指定信箱(bounty@nics.nat.gov.tw)。
- 信件大小超過 20MB 者，請分次寄送。
- 信件主旨須註明：「【產品資安漏洞獵捕活動】OO 產品漏洞通報／OO 產品漏洞申訴」。

5.4.3 初審與補正

- 資安院於收件後進行初審，若通報內容有缺漏、證據不足或格式不符者，得通知紅隊於 5 個工作天內完成補正。
- 補正次數以 2 次為限，逾期未補正、未依要求補正或經 2 次補正後仍未符合審查需求者，視為放棄該次通報，資安院得不予受理或終止審查。

5.4.4 藍隊確認與申訴

- 通過初審之通報書，將由資安院轉交廠商確認，並以報名成功通知信中所提供之約定密碼進行加密後傳遞。
- 藍隊須於收到通報書後 5 個工作天內回覆是否同意漏洞內容；如對漏洞

有效性、影響範圍、嚴重程度或重複通報等事項有疑義，得提出漏洞申訴書。

- 藍隊申訴次數以 2 次為限；逾期未回覆或未於期限內提出申訴者，資安院得依現有通報資料進行審查與裁定。

5.4.5 裁定與結果

- 資安院(裁判團隊)將依漏洞通報書、補正資料、藍隊確認結果及申訴資料，進行漏洞有效性、嚴重程度及獎勵資格之最終判定。
- 資安院(裁判團隊)裁定結果以漏洞裁判書形式提供，並作為獎勵核發及後續處理之依據。紅、藍雙方均不得對最終裁定結果提出異議。
- 漏洞認定標準：本活動之漏洞認定，係以紅隊所提交之通報書內容為基礎，由藍隊進行確認，並由資安院(裁判團隊)進行最終裁定。為確保漏洞獎勵之公正性，本章節將針對不列入認定範圍之類型漏洞進行說明，不予認定之漏洞類型亦不得作為獎勵。

5.4.6 認定原則

- 僅限本活動指定之受測標的。
- 漏洞須具可重現性、可驗證性，且對產品或使用者安全有實質影響。
- 不具實際安全風險或僅屬資訊建議者，不予認定。
- 涉及系統資源耗盡、服務異常或可用性影響之漏洞，須以非破壞性方式證明其可利用性；是否納入認定範圍，由資安院視個案情形裁定。

5.4.7 不予認定之漏洞類型

以下情形不屬於本活動認定範圍：

- 針對標的進行破壞性測試行為：如刪除設定檔，格式化、覆蓋、加密伺服器檔案，對資料庫進行破壞。
- 社交工程(如釣魚、詐騙手法)。
- 實體安全(需取得實體存取權限)。
- 未使用之套件弱點。
- Self-XSS(僅影響自身)。
- 需中間人攻擊或實體存取始能利用之漏洞。
- 頻寬消耗型或資源消耗型之 DoS/DDoS 攻擊手法。
- 安全影響輕微的資訊洩漏(如路徑、目錄、日誌等)。
- Cookie 缺少安全標頭。
- 僅透過自動化工具掃描，未經驗證可利用性之漏洞。

前項涉及 DoS/DDoS 或資源耗盡之情形，如屬可重現且可驗證之產品設計缺陷，並可證明對受測標的安全性或可用性具有實質影響者，資安院得視個案情形裁定是否納入漏洞認定範圍。

5.4.8 漏洞爭議裁定

漏洞認定最終結果，由資安院(裁判團隊)裁定，並以漏洞裁判書為憑，紅、藍雙方均不得對最終裁定提出異議。

5.4.9 測試規範與違規處理

紅隊研究員應於活動期間內，依資安院公告之測試範圍、指定標的及活動規範進行漏洞挖掘，不得逾越授權範圍或從事可能造成系統、資料、服務

或第三方權益受損之行為。

紅隊研究員不得從事下列行為：

- 對非本活動公告之標的、系統、網域、IP、API 或第三方服務進行測試。
- 進行 DoS／DDoS、壓力測試、暴力破解、大量掃描或其他可能造成服務中斷、效能異常之測試行為。若紅隊認為受測標的存在可造成服務中斷或資源耗盡之產品設計缺陷，應以最小影響方式提出可重現之技術說明與驗證證據，不得實際造成受測標的服務中斷、效能重大異常或資料損害。
- 刪除、竄改、加密、覆蓋、下載或大量擷取受測標的內之資料、設定檔、日誌、資料庫內容或其他資訊。
- 植入惡意程式、後門、持久化機制、勒索軟體、挖礦程式或其他非必要測試程式。
- 進行社交工程、釣魚、實體入侵、供應鏈攻擊、內部人員誘導或其他非技術性攻擊手法。
- 未經許可取得、保存、散布或揭露個人資料、營業秘密、機敏資訊、漏洞細節或測試結果。
- 嚴禁將包含客戶個資、原始碼或內部機密的真實資料，直接輸入或匯入公共 AI 模型進行分析或產生測試腳本。
- 將測試帳號、標的資訊、連線資訊、漏洞通報內容或活動相關資料提供予非本活動參與人員。
- 其他經資安院認定違反活動目的、測試範圍、保密義務或可能影響活動

公平性與安全性之行為。

測試過程中，如紅隊研究員意外取得個人資料、營業秘密、機敏資訊或非測試所必要之資料，應立即停止相關測試行為，不得保存、複製、使用或對外揭露，並應立即通報資安院，由資安院協調後續處置。

紅隊研究員如違反本活動測試規範，或其測試行為造成受測標的服務中斷、資料毀損、機敏資訊外洩、第三方系統受影響、藍隊營運受損或其他重大風險者，資安院得視情節採取下列措施：

- 要求立即停止測試行為。
- 取消該漏洞通報之審查或獎勵資格。
- 暫停或取消紅隊研究員之活動資格。
- 追回已發放或待發放之獎勵與獎金。
- 限制其參與後續相關活動。
- 如涉及違法或損害賠償責任，得依法辦理。

5.4.10 AI 工具的使用規範

紅隊研究員得使用 AI 工具輔助漏洞分析、程式碼檢視、測試步驟整理或通報文件撰寫；惟 AI 工具僅得作為輔助工具，不得取代實際測試、漏洞驗證及通報者之專業判斷。

紅隊研究員如使用 AI 工具，應於漏洞通報書「使用工具」欄位中載明，並遵守下列規範：

- 不得將受測標的之連線資訊、帳號密碼、原始碼、系統設定、漏洞細節、測試結果、個人資料、營業秘密或其他機敏資訊輸入公開或未經授

權之 AI 工具。

- 不得僅以 AI 工具產出內容作為漏洞通報依據；通報內容應經實際測試確認，並具備可重現、可驗證之技術證據。
- 不得使用 AI 工具產生、改寫或執行惡意程式、後門、持久化機制、勒索軟體、挖礦程式或其他超出本活動測試目的之程式碼。
- 不得利用 AI 工具進行大量自動化掃描、暴力破解、繞過限制、規避偵測或其他可能影響受測標的穩定性與安全性之行為。
- 如使用 AI 工具協助產生測試程式、指令或分析內容，紅隊研究員應自行確認其合法性、安全性及正確性，並對使用結果負責。

紅隊研究員如因使用 AI 工具造成機敏資訊外洩、測試範圍逾越、受測標的異常、第三方權益受損，或提交未經驗證之錯誤通報者，資安院得視情節取消該通報之審查或獎勵資格，並得暫停或取消其活動參與資格；如涉及違法或損害賠償責任，得依法辦理。

5.5 漏洞修補

漏洞修補與產品版本更新責任仍歸屬藍隊廠商。藍隊得依其內部資源與產品生命週期及漏洞風險程度，辦理後續修補及版本更新作業。資安院得視個案情形追蹤漏洞修補進度與 CVE 申請進度，並協助紅隊與藍隊就修補狀況、公開時程及必要資訊進行溝通協調。建議藍隊善用本活動成果，逐步建立產品資安治理、漏洞通報回應及修補管理流程。若藍隊於修補完成後希望進行複測，資安院得協助聯繫原通報者；是否協助複測，依紅隊意願及雙方後續安排辦理。

5.6 獎勵與獎金核發

本活動採用多元獎勵機制，鼓勵紅隊積極挖掘並通報具實質影響之漏洞。所有通報須經資安院裁定為有效漏洞，方具獎勵資格。獎勵內容包含單一漏洞獎金、資安院加碼獎勵／排名獎勵、漏洞獎金名人堂及 CVE 編號申請機會，以協助通報者建立專業形象並提升技術能見度。單一漏洞獎金由藍隊負責核發，並應於規定期限內完成支付；資安院加碼獎勵／排名獎勵由資安院另對漏洞發現 CVSS v4.0 累計分數最高前三名之紅隊研究員核發獎金，或資安院依活動公告及本辦法規定另行辦理。前述獎勵得併同領取，惟仍須符合各該獎勵之核發條件。

5.6.1 獎金說明

藍隊得設定活動總獎金上限，當該標的獎金累計達總上限時，資安院得公告該標的停止受理新通報或停止漏洞挖掘；已受理之通報案件，仍依本辦法進行審查與裁定。

5.6.1.1 單一漏洞獎金

- 單一漏洞獎金依漏洞嚴重程度 CVSS v4.0 基礎評分(CVSS-B)分級，藍隊於活動前須確認獎金基準，並於活動結束後依資安院裁定結果辦理支付。
- 獎金分級共分為 4 級，每個漏洞之分級標準與參考獎金如下表所示。

– 嚴重等級(CVSS v4.0：9.0~10.0 分)：新臺幣 100,000 元

– 高等級(CVSS v4.0：7.0~8.9 分)：新臺幣 30,000 元

– 中等級(CVSS v4.0：4.0~6.9 分)：新臺幣 10,000 元

– 低等級(CVSS v4.0：1.0~3.9 分)：新臺幣 3,000 元

- 紅隊通報漏洞經資安院裁定為有效漏洞者，依 CVSS v4.0 分級及本活動公告之獎金標準核發單一漏洞獎金。
- 藍隊須於活動結束後 30~45 個日曆日內，且最遲不得逾 115 年 12 月 31 日完成單一漏洞獎金支付，並保留匯款紀錄，以供資安院確認獎金已交付通報者。
- 如涉及爭議案件，則於資安院最終裁定確認後，依裁定結果另行辦理獎金支付。
- 若藍隊未依規定期限支付獎金，資安院得取消其後續參與資格。

5.6.1.2 資安院加碼獎勵／排名獎勵

- 資安院得依活動成果，針對有效漏洞通報成果表現優異之紅隊研究員，另行提供加碼獎勵或排名獎勵。
- 排名獎勵之計算，原則上以紅隊研究員經裁定為有效漏洞之 CVSS v4.0 分數累計結果為依據；如分數相同，資安院得綜合考量漏洞嚴重程度、通報品質、影響範圍、通報時間及是否具供應鏈風險等因素決定排序。
- 紅隊研究員如有違反本活動規範、保密義務、測試範圍或其他經資安院認定不適宜領獎之情形，資安院得取消其加碼獎勵／排名獎勵資格。
- 加碼獎勵／排名獎勵之名額、金額、計算方式、核發條件及核發時程，依活動公告或資安院正式通知內容辦理。
- 加碼獎勵／排名獎勵得與單一漏洞獎金併同領取；惟同一通報案件是否另有其他獎勵，仍以資安院公告或最終裁定結果為準。

5.6.1.3 稅務及其他事項

- 獎金金額新臺幣 1,001 元(含)以上者須列入個人綜合所得申報；得獎獎金在新臺幣 20,001 元(含)以上者，依法扣繳 10%所得稅。
- 獎金發放涉及稅務、匯款、收據或其他行政作業者，由實際核發單位依相關法令及行政程序辦理。

5.6.2 漏洞獎金名人堂

紅隊優秀成員將登錄於活動「名人堂」頁面，顯示其漏洞通報成就與專長技能，作為資安圈能見度與信譽的重要里程碑。

5.6.3 CVE 編號申請

- 通報者所回報之漏洞，經廠商同意公開相關漏洞資訊者，得透過資安院協助依本活動規範申請 CVE 編號。獲得 CVE 編號後，通報者將被登錄為正式漏洞發現人，並得選擇姓名公開或匿名，有助於提升技術聲譽與專業能見度。
- 惟有下列情形之一者，不得申請 CVE 編號：廠商不同意公開該漏洞資訊，或漏洞於修補完成前公開可能造成安全風險者。前述情形經廠商完成修補並同意公開後，通報者得繼續申請 CVE 編號。

5.6.4 領獎原則

本活動之獎勵與獎金發放，依下列原則辦理。

- 獎金僅頒發給第一個有效通報該漏洞的通報者。
- CVE 共同發現者列名僅作為技術歸屬與公開紀錄之用，並不影響本活動獎金僅頒發給第一位有效通報者之原則。
- 漏洞須符合「可驗證、可重現、可利用」的原則，且必須在活動範圍內。
- 同一漏洞之後續重複通報，不再額外發放獎金。
- 若通報內容屬於針對同一標的之連續攻擊行為，資安院得將其視為同一筆紀錄合併審查，並以首次有效通報者為準。
- 漏洞通報書需於活動限制期間內完成補正，並經資安院審核確認其漏洞通報有效性。
- 若經資安院裁定為有效漏洞之通報者(以下簡稱有效通報者)，即具領獎資格。資安院將通知藍隊並提供有效通報者之聯絡資訊(姓名、電子郵件、電話)，用於後續獎金支付與聯繫事宜。獎金發放相關作業(包含銀

行帳號取得、收據開立、稅務文件提供)由有效通報者與藍隊雙方直接辦理。

6. 資訊保密與公開原則

6.1 保密義務

- 參與本活動之紅隊、藍隊及資安院，均須簽署保密協議書，確保於活動過程中取得之所有資訊(含產品資料、測試環境、通報內容、技術細節等)僅限於本活動範圍內使用。
- 未經資安院與相關廠商同意，參與者不得對外揭露或散布漏洞資訊、測試結果或其他相關資料。
- 違反保密義務者，資安院得取消其參與資格、追回獎勵與獎金，並保留追究法律責任之權利。
- 資安院於活動規劃與執行過程中，對於藍隊所提供之產品資訊、紅隊通報內容，亦負有保密責任。所有資訊僅限於本活動範圍內使用，不得作為其他研究、商業或非授權用途。

6.2 公開原則

- 本活動之參與廠商可選擇以公開或匿名方式參加，資安院將尊重廠商選擇，不強制揭露廠商名稱。
- 活動成果報告將以整體統計或匿名化方式呈現，不會揭露特定廠商之測試結果或漏洞細節。
- 資安院僅於必要時，對外公布經確認之重大成果(如總通報數量、漏洞類型分布)，並確保不涉及個別廠商之專有資訊。
- 所有公開資訊將經資安院審核後發布，以避免未經授權之漏洞細節外洩。廠商名稱、LOGO、參與本活動之事實或對廠商具正面效益且不涉及漏洞細節、活動結果之資訊(如於記者會、活動網站、宣傳素材中之露

出)；選擇公開參加之廠商，資安院得逕行運用，無須就個別項目逐一徵詢同意；廠商如有特定項目不願揭露，得事前與資安院溝通後排除之。

6.3 漏洞 CVE 編號申請原則

- 若紅隊欲申請 CVE 編號，須經藍隊同意公開相關漏洞資訊，並應配合漏洞修補進度及公開時程辦理。
- 資安院得視個案情形，協助追蹤漏洞修補進度與 CVE 編號申請進度，並協調紅隊與藍隊確認公開內容、揭露範圍及申請時程。
- 獲得 CVE 編號後，紅隊可選擇姓名公開或匿名，以提升專業能見度，同時兼顧資訊保護。
- 若同一漏洞經多人於活動期間內獨立發現，資安院得協助將所有有效發現者列為該 CVE 編號之共同發現者，並於公開資訊中註明。

7. 法律遵循與安全港

7.1 法律遵循

- 參與者於活動期間，應遵守中華民國相關法令及本活動規範。
- 任何超出本活動範圍之外之行為，均不在活動保障範圍內，若涉及違法，參與者應自行負責，並可能被要求退還已獲獎勵或獎金，同時喪失未來參與相關計畫之資格。
- 紅隊須確認其所使用之工具、程式碼或其他技術，不得侵害第三方之智慧財產權或違反其他法律規範。

7.2 安全港條款

- 紅隊於遵守本活動規範之前提下，於活動期間內針對公告指定標的所進行之測試行為，資安院及藍隊認定其屬於授權行為，不構成《中華民國刑法》或其他適用之電腦法規所稱之「無故入侵他人之電腦或其相關設備」。
- 安全港保障範圍僅限於：本活動公告之受測標的、本活動允許之測試方法。
- 若紅隊超出範圍進行測試，或對非指定標的系統進行操作，則不在安全港保障之內，並可能涉及法律責任。
- 若紅隊因依本活動規範進行測試而遭第三方(含司法單位)提起法律行動，資安院及藍隊將採取適當行動說明該行為係在本活動授權範圍內進行。
- 若紅隊對測試行為是否屬於安全港保障範圍存有疑義，應於執行前向資安院確認。

- 若本活動之安全港條款與藍隊其他使用條款或政策有所衝突，本安全港條款優先適用。
- 本安全港條款並不適用於非本活動藍隊之第三方，若紅隊的測試行為涉及第三方之基礎設施，如網路、系統、資訊、應用程式、產品或服務等，仍可能面臨第三方提起法律行動。

7.3 保密與責任限制

- 所有參與者須簽署保密協議書，活動過程中取得之資料僅限於本活動使用，不得對外揭露。
- 若紅隊依本活動規範進行測試時，無意中未經授權存取個人資料、商業機密或其他敏感資訊，應立即停止任何可能導致進一步存取前述資訊之行為，告知資安院與藍隊已存取之資料，並立即自系統中移除該資訊，不得保存、使用或對外揭露相關資訊。
- 資安院僅負責活動規劃、平台協助及裁定，惟不承擔因漏洞利用、測試行為或工具使用所導致之任何損害責任。
- 藍隊提供受測標的，對於紅隊測試環境以外之影響不承擔責任。
- 紅隊須自行承擔因測試工具或操作所生之風險，不得因此向資安院或藍隊請求補償。

7.4 智慧財產權與揭露權

7.4.1 智慧財產權

- 紅隊提交之漏洞報告、技術細節及相關通報資料，其使用、保存、公開及揭露，應依本活動規範、保密協議及藍隊同意辦理。未經資安院及藍隊同意，紅隊不得自行公開、揭露或另作本活動以外之用途。

- 紅隊自行開發或使用之程式碼、工具或其他技術成果，除另有約定外，仍由紅隊自行保有；惟紅隊應自行確認其使用未侵害第三方智慧財產權，亦不得違反本活動測試範圍、保密義務或相關法令。

7.4.2 揭露權

- 漏洞資訊之公開、使用及揭露，應依本活動規範、保密協議、藍隊同意及紫隊審核結果辦理，並由藍隊、紅隊與紫隊協調公開方式、揭露範圍及時程。
- 若紅隊欲就通報之漏洞申請 CVE 編號，須先取得藍隊同意公開相關漏洞資訊，並配合紫隊與藍隊協調申請方式、公開內容及揭露時程。

7.5 辦法效力

- 本辦法經資安院公告後施行，適用於本活動之全體參與者。
- 參與者報名並經審查通過，即視為同意遵守本辦法之全部內容。

7.6 修正權限

本辦法如有未盡事宜，資安院得依實際需要進行補充或修正，並另行公告。修正後之內容，與原辦法具有同等效力。

7.7 優先適用

- 本辦法如與其他文件有所衝突，以本辦法為準。
- 本辦法如與現行法令牴觸，應依相關法令辦理。

7.8 緊急狀況

如遇不可抗力之事故或其他緊急狀況，資安院得單方面調整或終止活動，並公告於活動網頁，參與者同意將自行主動閱讀，資安院將不另行個別通

知參與者。

7.9 解釋權利

有關本活動內容及規則，資安院保有最終解釋權利。

7.10 爭端之解決與管轄法院

因本活動所生之任何爭議，雙方應依誠信原則協商解決；如協商不成，須進入訴訟程序者，雙方同意以臺灣臺北地方法院為第一審管轄法院。

8. 附件

相關參考文件：

– (紅隊)報名表暨保密協議書與個人資料同意書

– (藍隊)報名表暨保密協議書

– 法定代理人同意書