第 4 次行動應用 App 基本資安檢測實驗室能力試驗活動

簡章

公告日期：民國 107 年 10 月 05 日

壹、目的

為瞭解國內檢測實驗室之行動應用 App 基本資安檢測能力，「行動應用資安制度推動委員會」(以下稱本委員會)特舉辦「行動應用 App 基本資安檢測能力試驗活動」(以下稱本活動)。本活動目的在於讓參與檢測實驗室，瞭解本身資訊安全檢測能力並提供與其他檢測實驗室相互比對的機會，以加強檢測實驗室出具檢測報告的品質保證與管制，比對結果亦可作為改善措施之參考依據。檢測實驗室藉本活動除提升行動應用 App 資安檢測能力水準之外，並期望維持國內檢測實驗室檢測能力之一致性。

經濟部工業局認可財團法人全國認證基金會(Taiwan Accreditation Foundation，以下稱 TAF)為辦理「行動應用 App 基本資安檢測實驗室」(以下稱實驗室)之認證機構。為確認實驗室之技術能力與一致性，TAF 已於民國 104 年 12 月 11 日公告「行動應用 App 基本資安檢測實驗室認證服務計畫」，並說明參與該服務計畫之實驗室須參加行動應用 App 基本資安檢測相關能力試驗活動，做為申請成為行動應用 App 基本資安檢測制度的認可實驗室之佐證資料。

貳、報名期程、方式及收費

一、 報名期程

報名時間自民國 107 年 10 月 08 日至 107 年 11 月 02 日止。

二、 報名方式

(一) 於本委員會網址：http://www.mas.org.tw 下載「第 4 次行動應用 App 基本資安檢測能力試驗活動報名表」 (以下稱報名表)及「第 4 次行動應用 App 基本資安檢測能力試驗活動保密承諾書」(以下稱保密承諾書)，詳實填寫報名表正本一式 2 份及保密承諾書正本 1 份，並以掛號信寄回本委員會。

(二) 經本委員會秘書組審核報名表及保密承諾書無誤後，將以掛號信

寄回本委員會用印之報名表正本1份，視為完成報名程序。

(三) 聯絡窗口：

行動應用資安制度推動委員會聯絡人

藍小姐　ccisapa01@gmail.com/07-525-0558

(四) 郵寄地址：80499 高雄郵政 59-26 號信箱

「行動應用資安制度推動委員會秘書組（能力試驗活動申請件）」收

三、 收費

民國 107 年度不收取活動費用，後續年度收費標準另行公告。

參、能力試驗作業

本活動由本委員會設計並提供待測盲樣件，交付參與實驗室執行測試與評估，由各參與實驗室提供行動應用 App 基本資安檢測報告。本委員會依據所提供之報告，評估參與實驗室之行動應用 App 基本資安檢測能力。

一、 自我評估

(一) 本委員會提供1個測試樣本及參考答案，該測試樣本提供參加能力試驗之實驗室，可於參與本活動前，先行針對測試樣本，進行行動應用 App 資安檢測能力自我評估。

(二) 開放測試期間：民國 107 年 11 月 05 日至 107 年 11 月 09 日止。

二、 正式試驗

(一) 待測盲樣件寄送與執行時程

1. 本活動舉辦期間：民國 107 年 11 月 05 日至 107 年 11 月 23 日止。
2. 本委員會於盲樣待測件寄送前1個工作天將以 e-mail 通知報名表中所填之聯絡窗口，並將盲樣待測件以光碟片形式，採雙掛號寄送至報名表中所填之待測件寄送地址。實驗室收到盲樣待測件後請立即以 e-mail 通知本委員會聯絡窗口，若未通知本委員會，盲樣待測件收到日期則認定為雙掛號寄交日期。若實驗

室於本委員會 e-mail 通知後 3 個工作天未收到盲樣待測件，請與本委員會窗口聯繫。

3. 實驗室請務必於收到光碟片後 1 個工作天內，進行盲樣待測件安裝並執行，此即為啟用時間點。若實驗室未於前述時間內完成安裝及執行，則啟用時間點將以實驗室收到盲樣待測件之日期與時間認定。
4. 本委員會於盲樣待測件啟用後，將另行以 e-mail 通知實驗室聯絡窗口檢測報告電子檔交付截止期限。
5. 實驗室於啟用時間點起算 5 個工作天內，須完成盲樣待測件之資安檢測，並以 e-mail 提交加密之行動應用 App 基本資安檢測報告電子檔予本委員會，加密所使用之密碼請實驗室聯絡窗口以電話告知本委員會聯絡窗口。
6. 正式提交檢測報告日期以 e-mail 寄送日期為準，實驗室於 e-mail 提交檢測報告電子檔後，仍須以掛號信寄送檢測報告紙本 1 份予本委員會聯絡窗口，未於 5 個工作天內寄達檢測報告紙本予本委員會，則認定為未能符合參與本活動之要求。
7. 本委員會預計將於民國 107 年 11 月 30 日前，寄送能力試驗評估結果予參與本活動之實驗室，若能力試驗評估結果通知時間有異動，將另行以 e-mail 通知實驗室聯絡窗口。

(二) 檢測要求與說明

1. 本活動以「行動應用 App 基本資安檢測基準 V3.0」(以下稱檢測基準 V3.0)為評鑑範圍，實際須檢測之基準項目共計 62 項，請參照「結果摘要表」中所列之基準項目，參與實驗室須對盲樣待測件進行 62 項基準項目完整檢測評估，並盡可能檢測出所有問題，及填寫「結果摘要表」及完成檢測報告。
2. 實驗室應確實依其檢測程序與方法，對盲樣待測件進行檢測與記錄。
3. 參與實驗室應於檢測報告中，針對所檢測出不符合檢測基準

V2.1 事項，應列出該不符合事項之基準判定依據、檢測所使用工具與方法、檢測情境說明，並檢附如 Log 原始檔、畫面截圖等相關佐證資料。

4. 預設問題樣態可能因各基準項目考慮之面向不同，而有於各項基準中重複引用作為判定依據之可能，實驗室須整體考量。亦即：

   (1) 單一檢測基準之判定需多個預設問題樣態始能進行判定。

   (2) 同一預設問題樣態可做為多個基準項目判定之依據。

5. 檢測範圍僅限盲樣待測件本身及其與伺服端相關之互動，以工具或人工檢測伺服端問題、盲樣待測件本身品質及功能相關之問題(如閃退、不穩定等)，均不列入檢測報告內容之評估範圍。
6. 用以判定不符合基準之佐證資料應為直接可證明之檢測發現，並以呈述事實方式撰寫檢測報告，避免使用疑似或推論等臆測用語。
7. 實驗室之檢測報告原則上依實驗室自有之報告格式製作，唯必須包含檢測基準 V3.0 中「附錄三、行動應用 App 基本資安檢測報告參考格式 」內之所有內容，且須檢附「結果摘要表」。
8. 由於待測件為盲樣，故部份須配合其他條件(如：上架商店網頁內之資訊、「行動應用 App 基本資安調查表」中宣告內容等) 始可判定之基準項目，其結果得以「不適用」表示，但須敘明不適用之原因。

(三) 評價方式

本委員會將依實驗室所提交之「結果摘要表」為本活動之評估項目，並以檢測報告為佐證資料，以評估參與實驗室對行動應用 App 資安漏洞之檢測能力。

1. 若實驗室檢測出之資安漏洞數，大於(或等於) 該盲樣待測件 App 原先設計之漏洞數之 80%，認定為「滿意」。
2. 若實驗室檢測出之資安漏洞數，介於該盲樣待測件 App 原先設

計之漏洞數之 80%至 60%(或等於)之間，認定為「有疑問」。

3. 若實驗室檢測出之資安漏洞數，小於盲樣待測件 App 原先設計之漏洞數之 60%，認定為「不滿意」。

4. 經本委員會判定，實驗室誤判之資安漏洞(該盲樣待測件 App 並無此漏洞)，不能列入檢測出之資安漏洞數中。

5. 實驗室檢測出之資安漏洞，非屬該盲樣待測件 App 設計之漏洞，但經本委員會判定屬資安漏洞，則仍列入檢測出之資安漏洞數中。

6. 實驗室檢測出之資安漏洞數結果，評價最高以 100%計算。

三、 注意事項

(一) 本活動辦理過程，實驗室之資訊均以保密方式處理，惟當法規主管機構或認證機構查核時，本委員會將配合提供參與本活動之實驗室相關資訊，以供查核使用，若實驗室拒絕此要求請勿報名。

(二) 本委員會將確保參加本活動之實驗室，其能力試驗評估結果不外洩，僅作於本活動之目的使用，不做其他用途及不當應用。

(三) 若對能力試驗評估結果有異議時，請於能力試驗結果通知後 20 個工作天，向本委員會聯絡窗口提出書面評估結果申訴表(不提供現場申訴及現場說明)，每家參加能力試驗活動廠商申訴以 1 次為限，本委員會於收到評估結果申訴表後 10 個工作天回復申訴問題，若因申訴造成實驗室能力試驗評估結果有異動將併評估結果申訴表回復時一併通知。

(四) 本委員會為秉持公平原則，實驗室於評估結果申訴表中所填寫之申訴內容，以所交付檢測報告內容之補充說明為原則，額外提出之事證將不予接受，建議實驗室應於檢測報告中盡量提供完整佐證資料。

(五) 建議實驗室能力試驗評估結果為「不滿意」時，待實驗室精進檢測工具、方法等技術，參加下次能力試驗活動後再申請 TAF 認證。

(六) 為配合實驗室能力試驗結果之改善計畫，本委員會將於能力試驗評估結果通知後，統一開放5個工作天供實驗室改善測試使用，本委員會將 e-mail 通知聯絡窗口開放時間。

(七) 當本委員會有具體事證，足以證實實驗室有串通、委外檢測或偽造結果之事實，得以取消實驗室參與本活動之資格及能力試驗活動評估結果。

(八) 相關最新消息將不定期公布於本委員會網站。

第 4 次行動應用 App 基本資安檢測能力試驗活動

報名表

申請日期：○年○月○日

法人/機構名稱			
代表人/負責人			
實驗室名稱			
實驗室地址			
待測件寄送地址			
Apple ID			
實驗室 Public IP(不限 1 個)			
聯絡窗口姓名		電話/分機	
聯絡窗口行動電話		聯絡窗口 e-mail	
法人/機構印鑑章		代表人/負責人簽章	

＊報名廠商恪遵行動應用資安制度推動委員會公告之第 4 次行動應用 App 基本資安檢測能力試驗活動簡章相關規定，並接受能力試驗評估結果。

＊本報名表經雙方簽章後，視同完成能力試驗活動報名。

識別代號：＿＿＿＿＿＿＿＿　審核通過日期：＿＿＿＿＿＿＿＿

行動應用資安制度推動委員會(簽章)：＿＿＿＿＿＿＿＿

註：完成報名者，本表影本可為向 TAF 申請「行動應用 App 基本資安檢測實驗室」認證之佐證資料，待收到「行動應用資安制度推動委員會」能力試驗評估結果後補予 TAF。

第 4 次行動應用 App 基本資安檢測能力試驗活動

保密承諾書

○○○○有限公司（以下簡稱甲方）為向行動應用資安制度推動委員會(以下簡稱乙方)申請行動應用 App 基本資安檢測實驗室能力試驗活動，由乙方提供待測盲樣件（以下簡稱盲樣 App）予甲方執行實作檢測使用，以利甲方做為向財團法人全國認證基金會（以下簡稱 TAF）申請成為行動應用 App 基本資安檢測認可實驗室之佐證資料。為確保乙方所交付盲樣 App 及其資訊之機密性，甲方同意恪遵下列各項規定：

第一條 盲樣 App 僅授權甲方於本次能力試驗活動及 TAF 現場評鑑展示使用，於 TAF 認證服務結束後甲方應進行銷毀，甲方並須對盲樣 App 及其所有資訊負保密責任，不得揭露與任何第三人，或為其本身或他人之利益而使用。

第二條 甲方同意因職務需要必須使用或知悉前項保密資訊之員工，應負責使其員工遵守本承諾書之保密義務。

第三條 甲方違反本承諾書之約定或有任何因可歸責於甲方之事由，致使乙方所提供盲樣 App 資訊之公開或洩漏者，除應由甲方負擔一切法律上責任外，並應對因此造成之一切損害賠償乙方。

此致

行動應用資安制度推動委員會

立書人

甲方：○○○○有限公司
負責人姓名：○○○○
地址：○○○○
電話：○○○○

中　華　民　國　　１　０　７　　年　○　　月　○　　日