調　查　報　告

壹、案　　由：據悉，由中國大陸設計製造、並以台灣大哥大自有品牌來臺銷售的白牌手機AMAZING A32，在製程中被植入惡意程式，導致資安漏洞，用戶淪為詐騙集團的人頭。國家通訊傳播委員會雖有責成台灣大哥大儘速善後補救，並要求台灣大哥大針對消費者訂出賠償標準，並限2個月內將手機召回。然經本院函查，該款售出之9萬支手機僅1萬6千多支召回，其餘手機尚在使用，顯有資安疑慮；又日後手機是否有資安疑慮？有否因應措施等，均有深入了解之必要案。

貳、調查意見：

據悉，由中國大陸設計製造、並以台灣大哥大自有品牌來臺銷售的白牌手機AMAZING A32，在製程中被植入惡意程式，導致資安漏洞，用戶淪為詐騙集團的人頭。國家通訊傳播委員會雖有責成台灣大哥大儘速善後補救，並要求台灣大哥大針對消費者訂出賠償標準，並限2個月內將手機召回。然經本院函查，該款售出之9萬支手機僅1萬6千多支召回，其餘手機尚在使用，顯有資安疑慮；又日後手機是否有資安疑慮？有否因應措施等，均有深入了解之必要案，經向通傳會調閱相關卷證資料，詳予研析，業已調查完畢，茲將調查意見臚陳如下：

一、國家通訊傳播委員會109年處理台灣大哥大AMAZING A32手機資安漏洞一案，為國內首宗手機資安召回事件，經查該會責成業者辦理之召回及矯正成效未臻理想，固係囿於該型手機生命週期較短，多數用戶已不再使用；惟事涉民眾權益，通傳會除應持續督導業者矯正之外，亦宜就本案所凸顯國內尚未針對手機資安

問題訂定矯正措施之執行程序、監督作業或結案準則等問題，參考國際經驗妥予評估，以強化行政行為之明確性與一致性。

(一)本案始末概要

1、109年10月12日通傳會獲報，內容為內政部警政署刑事警察局「大陸代工手機銷臺灣暗藏惡意程式竊資料」報告，指出台灣大哥大股份有限公司（以下簡稱台灣大哥大)自有品牌「AMAZING A32」手機預載惡意程式。

2、基於偵查不公開原則，該會當時並未對外發布相關訊息，惟旋即展開行政調查，於109年10月12日即請財團法人電信技術中心(下稱電信技術中心)檢測案關AMAZING A32型號手機及另外兩款台灣大哥大自有廠牌A55、A57型號之手機，且檢測對象擴及所有內建APP，不限刑事警察局所指特定APP。電信技術中心於109年10月26日提供AMAZING A32手機出廠版(VI.3版)及更新韌體後之版本(VI.8版)資安檢測結果，報告指出，該款手機出廠版(VI.3版)確有將資訊回傳至阿里雲，VI.8版則沒有。另A55、A57兩款手機皆無類似AMAZING A32回傳訊息之情事。

3、行政院旋於109年11月4日由沈副院長召開手機資安檢測及驗證研商會議，會中決議:

（1）電信業者自有廠牌手機在大陸製造者，申請硬體型式認證時，需檢附符合台灣資通標準協會(TAICS)手機內建軟體資安產業標準證明文件；並切結手機發生資安事件之善後措施。

（2）通傳會年度手機資安抽測納入大陸白牌手機。

（3）抽測結果發布時，應輔以實際遭駭案例，讓民眾有感。

4、109年11月12日通傳會至台灣大哥大進行行政檢查。

5、109年12月30日內政部警政署刑事警察局以刑打詐字第1094800726號函請台灣大哥大全面召回已發售之「TWM AMAZING A32」智慧型手機，並副知通傳會。

6、109年12月31日請台灣大哥大至通傳會說明後續善後措施及多元召回方案等規劃。

7、110年1月6日通傳會對外發布新聞稿說明本案，台灣大哥大亦同步於其網站發布新聞稿及力平國際股份有限公司（以下簡稱力平國際）聲明稿，並於網站公布AMAZING A32手機召回專區。（註：力平國際為台灣大哥大之合作廠商，負責AMAZING A32手機之生產製造）

8、110年1月13日通傳會第946次委員會議依據消費者保護法第7、8、9、36、38條規定，決議命台灣大哥大及力平國際提出召回計畫、賠償計畫及未來預防之改善計畫，並於處分送達之日起2個月內依上述召回、賠償計畫完成召回、賠償及善後處理作業；前揭召回計畫內容須包含資訊周知大眾措施、多元通知消費者措施、客服人員資訊佈達與協助受理之教育規劃、有效激勵消費者逕洽召回措施等，其賠償計畫並應就因該商品造成消費者受檢警調傳喚或其他損害之情形，區分類型說明處理方式。

9、110年1月21日通傳會函請台灣大哥大將所有自有廠牌手機全數辦理資安檢測，亦請各電信業者盤點發售過之智慧型手機，並請業者持續維護是類手機內建軟體資安防護，後續通傳會將持續追蹤各業者盤點及送測情形。

(二)依據內政部警政署刑事警察局提供情資，其推測案關手機製程被暗中植入惡意程式，手機成品由台灣大哥大冠名授權品牌來臺銷售，國人購買並使用手機時，詐騙集團可利用該手機門號向遊戲公司申請遊戲帳號，遊戲公司傳送遊戲認證碼簡訊到該門號時，簡訊同時回傳給詐騙集團並申辦完成遊戲帳號（即人頭遊戲帳號)後自動刪除；嗣詐騙集團騙取遊戲點數，以海外IP位址將點數儲值至該人頭遊戲帳號內，使不知情的手機使用者變成詐騙集團的人頭。

(三)本案矯正及召回方案及處理情形

1、根據通傳會提供資料，案關業者提報之「AMAZING A32」行動電信終端設備召回、賠償、未來預防之改善計畫，其對民眾因此事件而權益受損，提供以下補償措施摘錄如下:

（1）手機軟體升級。

（2）針對無意願繼續使用AMAZING A32手機之用戶，提供更換其他手機(或補貼高階手機)或補償用戶1,000元折抵金,並給予申辦其他資費專案再1,000元之帳單折抵。

（3）針對受檢調傳喚之用戶群，提供法律協助、來回車資及其他合理補償(個案認定)。

2、本案AMAZING A32於109年7月下架前總計共售出9萬餘支，次據台灣大哥大提供之資料，該手機出售9萬4千餘支中，約有6萬1千餘支係原搭配台灣大哥大門號售出、約2萬6千餘支係搭配其他業者門號售出，另有6千餘支係空機出售。

3、據媒體[1]引述通傳會翁柏宗主任委員說明，該款手

[1] 林上祚。110年1月6日。台灣大9萬多支中國製手機藏惡意程式　國家通訊傳播委員會翁柏

機當初在綁約時並非「零元手機」，當時的單機價1,990元。

4、經通傳會統計，自109年10月8日至110年3月29日期間，曾有使用紀錄AMAZING A32手機約有2.1萬支，經該會統計至110年3月29日態樣如下表1:

表1.通傳會掌握本案AMAZING A32手機使用情形。

（通傳會提供）

態樣	數量
A32軟體升級	5,291
手機回收(含續約/單機回收/維修換機/個案處理)	7,284
自行換機或不再使用手機	5,999
總數	18,574

5、依國內5家行動通信業者統計，於110年8月11日至8月17日有使用紀錄之AMAZING A32用戶尚有6,166戶，對照累積軟體升級之數量6,281支（部分用戶可能軟體升級後不再使用，因此較前揭使用中數量多），推估多數仍使用AMAZING A32用戶應已完成軟體升級。

6、另通傳會持續就申訴管道檢視AMAZING A32相關申訴案件，自110年5月後AMAZING A32手機相關申訴案件數已顯著下降（6月-8月合計2件），所有申訴案件均要求台灣大哥大積極與用戶協商及妥處。

7、小結

（1）以本案手機銷售9萬餘支計算，目前矯正及召回比率僅約19%(1.8萬/9萬)，成效顯不理想，即以尚在使用之手機2.1萬計算,矯正及召回比率85.7%，亦難稱圓滿。

宗罕見道歉要求召回。新新聞報導。

（2）次查，本案手機銷售價格帶偏低，屬入門款手機，生命週期較短，且107年4月上市迄110年10月為止，已逾3.5年，爰通傳會所指110年3月尚在使用之手機數量僅2.1萬支，僅占總銷售量之23%，尚非無憑。

（3）根據澳洲競爭和消費者委員會(ACCC: Australian Competition and Consumer Commission)2006年曾針對商品召回進行研究[2]顯示，召回公告發布後的前8週是最重要的時期，因在召回活動的前6-8週內，有超過80%的商品可能被退回。由此推測，本案發布召回迄今已逾10個月，相關措施之邊際效應已降低，難有顯著成效，然而事涉民眾權益，通傳會仍應持續督導業者矯正。

(四)次查，針對本院函詢矯正及召回措施之認可及結案標準，通傳會僅說明將「行政指導該公司須持續處理AMAZING A32手機相關申訴，爰未來任何有關AMAZING A32手機之申訴，台灣大哥大均應協助消費者妥處」等語，無法具體說明；足以凸顯本案作為國內首宗手機資安召回事件，權責機關尚未建立相關準則以供各方遵循，而使相關行政措施具備明確性及一致性，有待通傳會研謀評估。

1、根據經濟部標準檢驗局107年委託財團法人台灣經濟研究院研究之「推動我國不安全消費性商品風險評估及矯正措施之研究」，已指出我國不安全消費性商品矯正措施推動之法制面與實務面問題，內容摘錄如下：

（1）法制面

[2] 資料來源：https://www.accc.gov.au/media-release/check-your-home-for-recalled-products

〈1〉缺乏矯正措施(含召回之完整執行程序與細項規範依據我國現行不安全商品之相關法律規範,商品檢驗法於矯正措施部分主要以「限期回收或改正」為主；而消費者保護法所規範之矯正措施則含括限期改善、回收或銷燬及令經銷商停售下架或其他必要措施。

〈2〉然而，不論是商品檢驗法或消費者保護法**皆未明定矯正措施之執行程序與監督作業**，在缺乏法源依據及標準作業程序的情形下，標準檢驗局雖要求報驗義務人填具「回收改正計畫及報告」,但實質上缺乏法規範效力，**主管機關無法進行實質審查及後續監督，且結案程序亦尚待建立。**

（2）實務面

〈1〉未能依據商品風險程度決定矯正措施之適用範圍與強度:現行我國主管機關針對不安全消費性商品之監督及管理，未能針對不安全商品確切可能產生何種程度之危害風險，據以要求業者採取「合乎比例」之矯正措施。

〈2〉業者所提「召回計畫」之規劃內容與能力決定召回之成效。…然而，召回措施之成效，可能取決於召回企業之規劃能力與決心，特別是台灣以中小企業為主，對於商品召回作業可能較為陌生，若採取的召回方式對消費者而言感到相當繁瑣與不便，或無任何激勵誘因時，或發布召回通知的管道太狹隘，致召回成效不佳，可能使得產品事故事件持續發生或擴大，影響消費者安全及權益。

〈3〉對客戶或商品銷售資訊之掌握度不足：若可掌握購買商品之消費者資料程度越高，則召

回之成效越大，但往往通路商與品牌商無法全面掌握購買商品之客戶資訊。…易言之，由於製造商、品牌商與通路商之間，於某些環節上無法確實落實記錄商品之流向，造成訊息銜接的不連貫與斷裂，也導致後續無法全面掌握產品銷售對象與相關資訊，是以無法達到相當成效之召回率。

2、承上，該研究案雖然指出「由於消費性商品種類繁多且商品特性不同，主管機關應依個案逐一討論與判斷，而非以一體適用之標準來監督，因此毋須以法律明定結案依據」，然而各主要國家仍有建立召回結案之認定準則如下表2:

表2.各主要國家召回結案認定準則

國家	**召回結案之認定準則**
英國	● 產品已不再市面上流通。 ● 已實現不安全產品的預期最終結果(改正或處置)。 ● 所有切實可行的行動，無論是短期還是長期，都是為了防止事故再次發生。 ● 與行業貿易機構、標準機構、監管機構、MSA以及消防和救援服務等公共機構提出了更廣泛的行業問題。 ● 與他人的所有溝通(監管機構、客戶、消費者、供應鏈等)都是及時有效的。 ● 監測回報程度、並考量與溝通管道、時間和溝通性質之關聯。 ● 已向所有PSIP參與者提供反饋。
美國	● 當公司要求結案時，委員會的實地調查員可對公司開展召回收尾檢查。屆時，該工作人員將審查對產品業主發出的通知數量、被退回或糾正的產品數量以及召回開始後是否曾發生涉及召回產品的事件或傷亡。

加拿大	● 審查整個召回過程，確保召回矯正措施計畫已經實施。 ● 評估供應鏈客戶反饋(通知所有供應鏈客戶、回覆的供應鏈客戶數量、供應鏈客戶銷毀，退回和/或矯正的單位數量)。 ● 評估消費者信息反饋(已聯繫貴公司的消費者數量、消費者如何了解召回情況、退回、更換、退還和/或提供維修包的單位數量)。 ● 審查事故數據(若召回後仍在加拿大發生事故事件可能表示召回無效)。
澳洲	● 供應商採取了所有合理措施以有效減緩不安全產品造成的風險後，召回案件便可結束。 ● 供應商的總結報告應包括： ■ 確認出貨的總數量，以及最終自消費者及供應鏈取回的產品數量。 ■ 國內供應鏈所有實體都已收到召回通知的證據。 ■ 溝通策略的相關資訊，包括任何與該策略有效性相關的資料(例：網頁的瀏覽人數)。 ■ 供應商採取了哪些行動，釐清或改正產品安全性危害的起因，包括任何肇因分析的結果、該瑕疵是否為設計、測試、製造、包裝、運送所造成、或者有其他瑕疵、以及供應商採取什麼步驟彌補瑕疵。 ■ 與該產品相關的任何已知傷害或事件之細節。 ■ 關於受影響產品所收到的投訴或詢問件數；這些投訴的性質為何。 ■ 被召回產品的銷毀或改正方法相關資訊，包括不安全產品已被銷毀或改正的證據。
日本	● 考量當時市場上剩餘的產品事故發生率、或產品事故發生時的危害，配合殘留風險的大小，來研究今後應如何應對、以及應對時應投入多少經營資源。倘若剩餘風險無法被社會大眾所接受，則須判斷持續積極召回。

中國大陸	● 已達召回目標。 ● 高度確信大部分受影響之消費者皆已收到召回通知，並有機會適切決定所應採取之行動。 ● 未再接獲受傷或生病之通報。 ● 就產品種類與風險而言，已達適當之退回還率。 ● 主管機關同意負責召回之供應者已採取合理與適切之步驟通知受影響之消費者，並已提供機會使其採取建議的行動。
(資料來源：標準檢驗局「推動我國不安全消費性商品風險評估及矯正措施之研究」委託研究案)	

3、對此，通傳會則說明：

（1）本案係因使用AMAZING A32手機有資安疑慮致消費者權益受損，爰以仍在使用中之AMAZING A32手機（2.1萬）為母數，作為妥處之主要目標。另外，手機淘汰不再使用之原因很多，例如超過一般使用年限[3](AMAZING A32手機於2018年上市)、損壞或換新機等；通傳會已責成台灣大哥大透過公告等方式周知大眾，並行政指導該公司須持續處理AMAZING A32手機相關申訴，爰未來任何有關AMAZING A32手機之申訴，台灣大哥大均應協助消費者妥處，方能完整維護消費者權益。

（2）本案係電信事業自有品牌手機之資安疑慮，爰通傳會審酌台灣大哥大電信營運商之身分，而由消費者資訊揭露情形、整體商品回收狀況、消費者申訴反映等方面對該公司進行要求，與之「推動我國不安全消費性商品風險評估及矯

[3] 參照知名手機評測網站GSMArena所作民調統計，超過7成網友表示手機不會使用超過3年，https://www.gsmarena.com/weekly_poll_how_long_will_you_keep_your_phonenews-44070.php

正措施之研究」中其他國家做法大致類似，倘未來電信事業自有品牌手機有類似本案情事，通傳會將參考本案經驗要求之；惟倘非電信事業自有品牌之手機致生消費者損害情事，則應由手機廠商按一般商品召回作業辦理。

二、通傳會推動「智慧型手機系統內建軟體資安測試規範」，為避免構成技術性貿易障礙而採自願送測方式辦理，廠商配合度偏低，然該會於108、109年主動針對銷售量較高、自有廠牌及中國廠牌手機共抽測25款並發布檢測報告，尚值肯認；惟觀察前開檢測結果推測，市面上超過九成之智慧型手機款式均有資安風險，值得通傳會繼續擴大辦理及加強宣導，俾強化民眾使用智慧型手機之資安意識。

(一)「智慧型手機系統內建軟體資安測試規範」簡介：

1、通傳會為推動智慧型手機系統內建軟體資安檢測，參考國際、區域組織（如OWASP、ENISA)及歐美等國（如NIST、FCC、Ofcom等）對連網設備的資安防護建議，於106年3月3日公告「智慧型手機系統內建軟體資通安全檢測技術規範」，以作為我國資安檢測實驗室檢測之依據。其檢測層別包含資料層、應用程式層、通訊協定層、作業系統層、硬體層等五層，各層分別包含多項檢測項目如下表3，該技術規範將通過檢測之智慧型手機內建軟體資通安全等及區分為初級、中級及高級3種。

表3.「智慧型手機系統內建軟體資通安全檢測技術規範」之檢測層及檢測項目。

（通傳會提供）

層別	檢測項目
資料層	資料使用授權、資料儲存保護、資料遺失保護

表3.「智慧型手機系統內建軟體資通安全檢測技術規範」之檢測層及檢測項目。

（通傳會提供）

層別	檢測項目
應用程式層	程式身分辨識、程式信任來源、程式執行授權、程式執行安全
通訊協定層	協定使用授權、協定傳輸保護、協定執行安全
作業系統層	系統操作授權、系統身分辨識安全、系統執行安全
硬體層	金鑰管理保護、演算法強度要求

2、取得初級認證之智慧型手機，表示已具備防護個人隱私等敏感性資料之能力；取得中級認證者，除敏感性資料外，對於其他資料之使用、儲存及傳輸，也提供了安全防護機制；取得高級認證者，則表示提供核心底層資訊不被竄改或被不正當擷取之能力。手機製造商等申請者可依手機的市場定位及資安防護強度等需求，自行規劃需申請之系統內建軟體資安檢測及認證等級。

3、協調台灣資通產業標準協會（TAICS）訂定公布「智慧型手機系統內建軟體資安測試規範」：為擴大推動成效及其手機資安防護落實於設計階段，通傳會於108年與TAICS合作，共同推動手機內建軟體資安產業標準，俾廠商及政府採購時有所依循。**TAICS已於109年7月10日公告「智慧型手機系統內建軟體資安標準」，其係以通傳會「智慧型手機系內建軟體資通安全檢測技術規範」為基礎**，並納入最新資安防護議題。檢測安全構面包含應用程式層、通訊協定層、作業系統層、硬體層等四項如下表4。其測試項目及測試方式分別經該會查復在案。

表4. 「智慧型手機系統內建軟體資通安全檢測技術規範」檢測層及安全測試項目　　（通傳會提供）	
安全構面	安全測試項目
應用程式層	程式資料使用授權測試、程式資料儲存保護測試、資料遺失保護測試、程式身分辨識測試、程式信任來源測試、程式執行授權測試、程式執行安全測試
通訊協定層安全測試	協定使用授權測試、協定傳輸保護測試、協定執行安全測試
作業系統層安全測試	系統操作授權測試、系統身分辨識測試、系統執行安全測試、傳輸保護測試
硬體層安全測試	實體安全測試、金鑰管理保護測試、演算法強度要求測試

(二)「智慧型手機系統內建軟體資安測試」(Embedded Software on Smartphone Systems，ESS)推動情形：

1、根據通傳會查復資料，近5年通過審驗手機達848款，然而依據中華民國資訊安全學會公告之「智慧型手機系統內建軟體資通安全(ESS)」檢測通過名錄僅19款手機，檢測覆蓋率顯然偏低。

2、對此，通傳會說明如下:

（1）通傳會為建立ESS認驗證體系，經蒐集歐美等先進國家對於民間一般物聯網及資通設備之強制性規範僅止於電氣安全、電磁相容及通信介面，尚無涉及資通安全，例如美國目前與資通設備有關之資安法規為物聯網資安改進法（IoT Cybersecurity Improvement Act of 2020)而美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST)及美國行政管理和預算局（Office of Management and Budget,OMB)推動之物聯

網資安尚不及於民間產品（如手機），歐盟則為資通安全法（Cybersecurity Act on EU 2019)其歐盟網路安全機構(European UnionAgency for Network and Information Security, ENISA)建立之資通訊產品、服務及程序範圍概括一般資通訊設備，**係屬自願性資通安全認證框架**，然未特別針對智慧型手機訂定規範。

（2）依上觀之，在歐美等國並未針對ESS訂定強制資安要求規範情形下，**如我國強制推行ESS認證，將導致歐美等國智慧型手機產品無法順利進口及銷售，造成技術性貿易障礙議題**，爰現階段通傳會建立ESS認驗證體系亦比照歐美等國採自願性資通安全認證框架方式推動。

（3）該會為推廣ESS之檢測與驗證，已協調台灣資通產業標準協會(TAICS)於109年7月公告「智慧型手機系統內建軟體資安測試規範」（下稱ESS測試規範），並已有5家檢測實驗室（名錄詳見https:ess.org.tw/esslab_cert_list.html）通過財團法人全國認證基金會(TAF)認證俾供業界自主送測；惟因手機生命週期短，資安檢測費用昂貴、所需時程較長（例如單款手機通過最基本之1級資安檢測約需新臺幣315,000元，共有18個檢測項目需時20人天），且手機軟體版本更新頻繁，須就更新部分重新檢測認證，爰業界基於成本及產品快速上市等考量，送測意願普遍不高。

（4）通傳會為帶動手機製造商主動辦理ESS檢測，俾於手機設計、生產階段即加強其資安防護規劃，係透過逐年編列資安相關計畫之執行預

算，補助通傳會所屬財團法人電信技術中心，自ESS測試規範中針對應用軟體及通訊協定應有之個資保護及加密機制，參考開放網路軟體安全計畫（Open Web Application Security Project, OWASP)之行動應用安全驗證標準(Mobile Application Security Verification Standard, MASVS)**挑選10個最基本之測項**，於每年下半年針對台灣電信產業發展協會統計電信業者上半年銷售量較高之10款智慧型手機辦理抽測作業，另於每年上半年則抽測前年度下半年銷售量較高之電信業者自有廠牌及高資安風險地區製造(如大陸廠牌）共5款手機。

(三)次查，該會於108、109年主動針對銷售量較高、自有廠牌及中國廠牌手機，以基本檢測項目共抽測25款並發布檢測報告如下，由兩年檢測報告顯示，僅有APPLE廠牌手機2款均於第一次初測即通過資安檢測，其餘23款手機均無法通過第一次初測，而需經複測後始能通過，整體檢測通過率僅8%；由此推測，市面上超過9成手機款式，連僅屬基本項目之測項均無法通過初測，值得通傳會進一步擴大辦理並加強宣導，俾強化民眾使用智慧型手機之資安意識。

1、通傳會於108年試行市售手機資安抽測作業，並委託經財團法人全國認證基金會（TAF）認可之測試實驗室-財團法人電信技術中心（TTC）針對電信業者108年第1季銷售量較高之10款不同品牌智慧型手機進行測試。

（1）相關測試項目係自通傳會公告之「智慧型手機系統內建軟體資通安全檢測技術規範」擇定，

確認待測手機內建軟體無下列情事：

〈1〉未將敏感性資料（如：個人資料）加密或儲存於作業系統保護區。

〈2〉無線傳輸敏感性資料時，未使用加密傳輸。

〈3〉內建軟體之交談識別碼遭重送攻擊。

〈4〉與付費功能伺服器間傳輸，未使用安全之加密演算法。

〈5〉初次存取使用者綁定裝置之帳戶，未先認證使用者身分及權限。

〈6〉內建軟體未具備處理資料隱碼攻擊字串之能力。

〈7〉內建軟體未具備處理延伸標記語言攻擊字串之能力。

〈8〉內建軟體與伺服器溝通之帳號、密碼及金鑰以明文方式存於執行檔。

〈9〉內建軟體預設開啟不必要之權限，或系統預設開啟不必要之網路連接埠。

〈10〉系統更新時以明文方式傳輸。

（2）該會於109年5月8日發布抽測結果，10款手機，經完成初測、改善及複測後，9款通過測試，另1款於結果發布後隔週完成改善。結果如下:

〈1〉初測即通過：APPLE iPhone XR。

〈2〉第1次複測後通過：經2個月改善期後，HTC U12、三星GALAXY A7 2018、NOKIA 8.1、SONY XPERIA L2、ASUS ZENFONE MAX M1、SUGAR P1、華為Y9 2019等7款。

〈3〉第2次複測後通過：OPPO AX5。

〈4〉結果發布後完成改善：紅米NOTE 6 PRO。

2、通傳會持續於109年辦理市售手機資安抽測作業，在109年下半年至110年第1季針對台灣電信

產業發展協會統計109年上半年銷售量較高且未取得資安認證之10款不同廠牌智慧型手機，以及3款電信事業自有廠牌與2款大陸廠牌手機，並委託經財團法人全國認證基金會（TAF）認可之測試實驗室-財團法人電信技術中心（TTC）進行手機系統內建軟體之資通安全檢測。

（1）本次檢測係針對應用軟體及通訊協定應有之個資保護及加密機制，從台灣資通產業標準協會（TAICS）於109年7月公告之「智慧型手機系統內建軟體資安測試規範」中跨級別挑選10個基本項目進行檢測，主要包括：

〈1〉內建軟體應將帳號、通行碼或金鑰儲存於作業系統保護區內或以加密方式儲存

〈2〉內建軟體應避免交談識別碼遭重送攻擊

〈3〉與付費功能伺服器間傳輸，應使用安全之加密演算法

〈4〉不可於執行期間將敏感性資料儲存於系統日誌檔案

〈5〉存取敏感性資料前，應取得使用者同意。

（2）通傳會已於110年7月7日發布抽測結果，14款通過檢測之手機如下：

〈1〉初測（110年1月）通過：APPLE iPhone 11。

〈2〉複測（110年4月）後通過：初測未通過，經手機製造商積極配合改善後複測通過，包括SONY XPERIA 5、三星GALAXY A20、HTC DESIRE 19S、ASUS ZENFONE MAX M2、台灣大哥大A55及A57、SUGAR C13、紅米REDMI NOTE 8T、華為Y9 PRIME 2019、OPPO A9 2020、Koobee S16、REALME XT、VIVO Y12等13款。

3、通傳會就上開檢測檢結果補充說明如下：

（1）該會係於108年度開始辦理ESS抽測作業，經108年及109年兩次抽測結果，有多達23款手機均未通過初測，為敦促受測手機製造商加強其手機資安防護，通傳會於完成初測後均先函送檢測報告予該手機製造商，俾其瞭解受測手機之資安問題及未通過測試主要原因，以利改善手機設計、製程之資安防護作法。

（2）另部分手機之系統內建軟體係由第三方App製造者(如Google)所提供，本作法除可藉由協調未通過檢測手機之製造商積極改善其所設計App之資安防護，亦可促使製造商協調第三方App提供者改善其軟體設計資安要求,並敦促發布各款手機之更新版本，使該等手機通過複測，以確保消費者權益。

（3）經觀察108年度未通過初測手機之平均改善時間約3個月(第1次複測、第2次複測)、109年度約2個月(複測),可見109年度手機製造商之改善時間大幅減少,顯見通傳會推動ESS抽測作業已逐漸促使手機製造商改善其內部軟體設計開發之資安標準作業程序,在提升ESS防護有一定效益。爰建議仍維持現行做法，持續以抽測方式輔導手機製造商重視企業形象及完善ESS防護作為。

參、處理辦法：

一、調查意見一至二，函請國家通訊傳播委員會確實檢討改進見復。

二、檢附派查函及相關附件，送請交通及採購委員會處理。

調查委員：蔡崇義

田秋堇

中　華　民　國　110　年　12　月　9　日