104 年委託研究報告

104 年手機系統內建軟體資安檢測計畫委託研究案期末報告書

計畫委託機關：國家通訊傳播委員會

中華民國 105 年 06 月

104 年委託研究報告
PG10407-0033

104 年手機系統內建軟體資安檢測計畫委託研究案

期末報告書

受委託單位

中華民國資訊軟體協會

計畫主持人

喻維貞

協同主持人

鍾榮翰

研究人員

楊蕙如、蔡志明、洪光鈞、葉錫勳、姚人鳳

本報告不必然代表國家通訊傳播委員會意見

中華民國 105 年 06 月

目　次

表　次 III

圖　次 V

提　要 VII

壹、 專案概述 1

一、 專案名稱 1

二、 專案目標 1

三、 專案研究範圍 1

四、 期末交付項目 1

貳、 期末報告 3

一、 蒐集及研析國際智慧型手機行動裝置資通安全檢測發展現況 3

二、 研提智慧型手機資安風險評估報告 22

三、 研提我國智慧型手機系統內建軟體資通安全檢測技術規範草案 41

四、 研提第三方檢測實驗室認可規定修訂草案 69

五、 評估技術規範草案可行性 77

六、 辦理座談會 107

七、 辦理說明會 112

八、 智慧型手機之安全宣導資料 123

九、 本案與性別相關之統計及分析 130

十、 專案工作會議 133

參、 後續規範推動建議 135

一、 短期：自願性與半強制性推動規範藉以宣示國家政策 135

二、 中期：因應趨勢調整規範並結合政府採購擴大檢測需求 137

三、 長期：修訂法規並推動強制性要求落實資安檢測..... 138
四、 計畫研究期間相關問題討論與可行性作法建議..... 139

肆、 附件..... 142
一、 國際智慧型手機行動裝置資通安全相關研析報告..... 142
二、 智慧型手機資安風險評估報告..... 142
三、 智慧型手機系統內建軟體資通安全檢測技術規範草案..... 142
四、 資通設備資通安全檢測實驗室管理作業要點修正草案..... 142
五、 所測暢銷市售手機資安檢測結果..... 142
六、 座談會會議紀錄、簽到表及研析意見..... 142
七、 所辦說明會之紀錄及研析意見..... 142
八、 智慧型手機之安全使用宣導資料..... 142
九、 專案工作會議會議紀錄..... 142
十、 手機內建軟體資安認證安全標章(電子檔)..... 142

表　次

表 1　期末交付項目對照表 2
表 2　國際間智慧型手機行動裝置資通安全相關文獻整理表 3
表 3　各國規範綜合研析比較表 6
表 4　國際組織與各國規範所公告之相關技術細節彙整對應表 10
表 5　共通準則硬體安全深度彙整分析表 19
表 6　行動裝置 10 大風險 30
表 7　智慧型手機風險評估矩陣表 34
表 8　國際標準行動裝置層級 43
表 9　資料型別分類表 48
表 10　資料型別與個人資料保護法之對照 49
表 11　檢測項目說明 51
表 12　檢測項目與檢測細項對應表 52
表 13　本規範與「行動應用 APP 基本資安檢測規範」之差異 58
表 14　檢測項目與各規範對應關係 63
表 15　智慧型手持式行動臺安全檢測實驗室管理要點訂定重點摘錄 71
表 16　智慧型手持式行動臺安全檢測實驗室(試辦期)資格重點摘錄 75
表 17　2011~2014 年智慧型手機作業系統市占率變化 77
表 18　專案測試標的 78
表 19　第一版規範之檢測結果系統比較 80
表 20　測項 D.2.1.B 之試測結果 93
表 21　測項 A.2.1.B 之試測結果 94
表 22　測項 P.2.1.B 之試測結果 95
表 23　檢測細項(期末審查版) 96
表 24　檢測細項(期後修調版) 100
表 25　檢測項目之檢測時間(必測項) 104
表 26　檢測項目之檢測時間(選測項) 105

表 27　檢測工時平均估計表.....106
表 28　測試層別與級別檢測時間.....106
表 29　檢測費用計算基準建議.....107
表 30　推廣說明會場次資訊.....112
表 31　說明會議程資訊.....113
表 32　出席人員公司性質與性別統計分析表.....116
表 33　與會人員產業與職位類別分析表.....120
表 34　政策是否強制性調查分析表.....121
表 35　與會者申請檢測實驗室意願調查分析表.....121
表 36　常見攻擊手法彙整表.....124
表 37　使用者指引參考表.....128
表 38　計畫內會議各類職位男女人數分析表.....131

圖　次

圖 1　預先定義值矩陣範例(一)..... 24
圖 2　預先定義值矩陣範例(二)..... 25
圖 3　依風險之量測排序威脅之範例..... 26
圖 4　行動裝置 10 大風險..... 29
圖 5　智慧型手機風險評估框架..... 33
圖 6　技術規範研究流程..... 42
圖 7　行動裝置架構圖..... 43
圖 8　安全等級..... 45
圖 9　規範檢測架構..... 47
圖 10　本規範與國際/國內規範之差異 67
圖 11　安全標章(彩色版)..... 69
圖 12　安全標章(黑白版)..... 69
圖 13　檢測實驗室分類圖..... 70
圖 14　台灣智慧行動手機廠牌排名..... 78
圖 15　檢測層別與測試項目..... 92
圖 16　各手機試測結果統計比較..... 93
圖 17　敏感性資料以明文方式儲存於非作業系統保護區圖示 94
圖 18　伺服器有效憑證過期圖示..... 95
圖 19　定位資訊明文傳輸圖示..... 95
圖 20　說明會現況..... 114
圖 21　出席人員公司性質分析圖..... 116
圖 22　出席人員性別分析圖..... 117
圖 23　問卷內容..... 119
圖 24　申請檢測實驗室類型分析圖..... 122
圖 25　各安全等級適宜之檢測時間調查結果..... 123
圖 26　智慧型手機使用需求狀況分析..... 130

圖 27　計畫內會議出席男女比例.....131
圖 28　計畫內會議各類職位男女比例分析.....132
圖 29　技術規範推動規劃.....135
圖 30　短期規範推動時程規劃.....136

提　要

關鍵詞：資通安全、智慧型手機、內建軟體、技術規範

一、研究緣起

隨著智慧型手機硬體及軟體技術日趨進步成熟，手機廠商、行動通信業者及軟體廠商為了提升市場競爭力及市佔率，積極開發與民眾日常活動相關的各種應用，民眾在使用各類應用時，使用者大多需要輸入一些個人資料，因此智慧型手機資安風險已成為消費者保護新興課題。

然而，對於智慧型手機資訊安全要求，目前國際間並無統一檢測標準，且歐美等先進國家亦無手機資安檢測的強制性規範。因此須蒐集智慧型手機行動裝置資通安全相關檢測發展現況，研訂手機系統內建軟體資安檢測相關機制，作為我國建立手機資安檢測環境及相關機制之參考。

二、研究目標

藉由蒐集國際智慧型手機行動裝置資通安全檢測發展資料，並召開有關機關、產業界、檢測機構及專家學者座談會，廣泛徵求各界意見，提出適合我國智慧型手機系統內建軟體資通安全檢測技術規範及檢測實驗室認可規定等，以完備智慧型手機資通安全檢測及認證機制，加強民眾個資及隱私之防護。

三、重要發現

(一)蒐集及研析國際智慧型手機行動裝置資通安全檢測發展現況

本計畫整理國際組織、美國、歐盟、中國、英國、日本、新加坡及韓國共 8 個國家/組織所制定政策之相關內容，研析各國相關之發布文件共 30 份。比較個規範內容之差異，作為後續研擬資通安全檢測技術規範及檢測實驗室認可規定之參考，研擬文件如下表，詳細內容請參閱附件 1。

(二)研提智慧型手機資安風險評估報告

參考國際之智慧型手機資安相關評估文件,針對智慧型手機之韌體、作業系統及出廠時內建應用軟體等風險，提出智慧型手機資安風險評估報告，內容包括資安風險評估方法、流程、範圍、面向、等級及結果等。詳細內容請參閱附件 2

(三)研提智慧型手機系統內建軟體資通安全檢測技術規範草案

參酌國際作法及考量我國產業環境，研析智慧型手機系統內建軟體資通安全包括韌體、作業系統及出廠時內建應用軟體等，進一步研提我國智慧型手機系統內建軟體資通安全檢測技術規範草案，完整規範草案內容請參考附件 3。

(四)研提第三方檢測實驗室認可規定修訂草案

為使智慧型手機系統內建軟體資通安全檢測技術規範於未來落實檢測時，能確保資通安全品質，故修訂資通設備資通安全檢測實驗室管理作業要點，內容包括下列項目，完整規範草案內容請參考附件 4。

- 實驗室應具備之檢測能力
- 實驗室人員(含技術主管、品質主管、報告簽署人)具備之資格
- 實驗室申請書(含檢測範圍與檢附文件)
- 檢測實驗室認可證書
- 檢測費用
- 其他相關規定

(五)評估技術規範草案可行性

選擇至少 5 款暢銷市售手機，進行資安檢測，以評估手機系統內建軟體資安檢測技術規範草案之可行性。經過手機測試結果修調規範內容，並評估檢測所需時間完整評估結果內容請參考附件 5。

(六)規範座談會

辦理三場座談會，促使本計畫提出之手機系統內建軟體資安檢測技術規範符合國內市場需求。

(七)規範推廣說明會

為推動手機系統內建軟體資安檢測技術規範，辦理推廣說明會向手機通訊商與檢測實驗室業者說明規範內容與通過審驗之優點。

(八)提出智慧型手機之安全使用宣導資料

為加強智慧型手機之安全使用宣導，編撰智慧型手機之安全使用資料，以提供民眾有關手機資安應具備資安意識資料。完整規範草案內容請參考附件 8。

四、主要建議事項

由於目前國際間多數國家未強制性規定手機上市前須經資訊安全檢測，僅部分國際品牌手機業者以自主檢測方式宣稱手機安全性，然其檢測方式與檢測標準並未有統一規範，對於消費者來說無法明確判斷。為配合國家政策並維護消費者權益，本計畫研究團隊建議規範後續推動方向如下：

(一)短期：自願性與半強制性推動規範藉以宣示國家政策

1. 推動實驗室具備檢測能力
2. 通訊業者綁約手機應送測
3. 鼓勵手機原廠自願性檢測

(二)中期：因應趨勢調整規範並結合政府採購擴大檢測需求

1. 因應發展趨勢更新檢測項目
2. 搭政府採購要求手機安全
3. 宣導檢測安全標章重要性

(三)長期：修訂法規並推動強制性要求落實資安檢測

1. 修訂法規推動強制性要求
2. 民間維護並控管安全標章

Abstract

Keyword：information security、smartphone、default applications、security criteria

1 The origin of Research

Since the application and the market of smartphone becomes maturity. The phone manufacturers, operators and software vendors are aggressively to design and develop the application to immersed into people's life to increase the competitiveness and market share. When people use these applications, most of the application will ask them to input personal information, and that's why the security risk of smartphone becomes a new objective to protect it.

However, there is no international standards for the information security of smartphone. Even in Europe or USA, they do not have the mandatory criteria to test it. Above all, we have to collect the related standards or criteria in the world to design and define the related policy for embedded applications of smartphone. It will be helpful for government to reference to define the policy for smartphone security criteria.

2 Objective

We have to collect the security criteria of smartphone and call the conference to collect the comments from organizations, industries, test labs and specialist. The comments will help to establish the security criteria to fit the security testing requirement of embedded applications of smartphone and regulation of test labs. It will not only enhance the security test technologies and certification mechanism but also protect the personal information and privacy for people.

3 Results

3.1 Collect and analysis the criteria of smartphone in the world

In this project, we collect the criteria and policies from international organization, USA, EU, China, UK, Japan, Singapore and Korea. We analysis the related 30 documents and compare them to each other as the reference base for designing and defining the security criteria. The detail information could be found in Appendix 1.

3.2 Propose the report of the security risk for smartphone

We study the related documents as below and propose a risk report for smartphone including firmware, operating system and embedded applications. The report will cover the evaluation methods, workflow, coverage, aspect, security level and results. The detail information could be found in Appendix 2.

3.3 Propose the draft security criteria of embedded applications for smartphone

Base on the mechanism of the other organizations or countries and the industry environment of Taiwan. We propose a draft criteria of embedded applications for smartphone including firmware, operating system and embedded applications. The detail information could be found in Appendix 3.

3.4 Propose drift criteria for the third party certification lab

There are two types of certification lab which are Type 1 and Type 2 certification lab classified by testing areas. Type 1 lab have to provide the service to test Basic and Medium level test items. Type 2 lab have to provide the service to test High level test items. The criteria is designed by

referencing the rule of Test Lab Criteria of Information and Communication Appliance and The Promotion Process of Certification Lab Validation for Mobile App Basic Self-Test v1.0 to promote the certification lab validation criteria. The content is as figure 1 and the detail information could be found in Appendix 4.

3.5 Evaluate the feasibility of criteria

We test 6 sample smartphones. Four of them are using Android system and the other as using iOS and Windows system. We test them by the 36 test items in the criteria and have a detail report be documented in Appendix 5.

3.6 Hold the conference of embedded applications of smartphone to discuss and promote security criteria

We hold three conferences to collect the comments for the criteria of embedded application of smartphone from specialist and professors. Besides that, we also hold two conferences to explain and promote the criteria.

3.7 Propose the promotion plan of how to use the smartphone securely

We propose a guideline for how to use the smartphone securely to let people know the importance of information security and concept of how to use smartphone correctly. We explain the complicated subjects understandable to let people understand it completely. The detail information could be found in Appendix 8.

4 Suggestion for promotion

Since most of the countries does not define the security criteria to be the mandatory test before selling the smartphone. There is only some vendors claims they have pass the security tests through self-testing, but actually there’s no standard for it. It will not easy for consumers to judge the result. In

order to match the national policy and consumers' right, our strategy of the criteria is as below.

4.1 Short term: Call for volunteer and helf-mandatory to promote the criteria and declare national policy.

- Push lab's certification ability.
- The contracted smartphone should be certificated.
- Call for volunteers from smartphone vandors to apply the certification.

4.2 Mid-term: Revise the criteria base on the trend and extend the test requirement by folling the governement purchasing.

- Revise the criteria by developing trend.
- Suggest government to purchase secue smartphone.
- Promote the imprtantance of security certificaiton.

4.3 Long term: Revise the laws and regulations to push the criteria as the mandatory test.

- Revise the laws and regurlations to push the criteria as the mandatory test.
- Matain the certification by non-government organization.

壹、專案概述

一、專案名稱

「手機系統內建軟體資安檢測計畫委託研究計畫」委託研究案

二、專案目標

藉由蒐集國際智慧型手機行動裝置資通安全檢測發展資料，並召開有關機關、產業界、檢測機構及專家學者座談會，廣泛徵求各界意見，提出適合我國智慧型手機系統內建軟體資通安全檢測技術規範(以下簡稱本規範)及檢測實驗室認可規定等，以完備智慧型手機資通安全檢測及認證機制，加強民眾個資及隱私之防護。

三、專案研究範圍

(一)蒐集及研析國際智慧型手機行動裝置資通安全檢測發展現況。

(二)參酌國際作法及考量我國產業環境，研提我國智慧型手機系統內建軟體資通安全檢測技術規範草案，並透過檢測作業確保規範之可行性。

(三)研提第三方檢測實驗室認可規定修訂草案。

(四)研提智慧型手機資安風險評估報告及智慧型手機之安全使用宣導資料。

(五)辦理座談會廣泛徵詢各界對智慧型手機系統內建軟體資通安全檢測技術規範草案，確保規範內容符合國內需求。

(六)辦理我國智慧型手機系統內建軟體資通安全檢測技術規範相關推廣活動。

四、期末交付項目

自契約生效次工作日起至 105 年 03 月 03 日前提出期末報告中文版

本 14 份，期末報告書應包含下列項目，本會已完成並列於對照頁內：

表1　期末交付項目對照表

項次	工作內容	執行成果	對照頁碼
1	蒐集及研析國際智慧型手機行動裝置資通安全檢測發展現況	已完成國際智慧型手機行動裝置資通安全相關研析報告。	P.3~20 附件 1
2	研提智慧型手機資安風險評估報告	已完成智慧型手機資安風險評估報告。	P.21~39 附件 2
3	研提智慧型手機系統內建軟體資通安全檢測技術規範草案	已完成智慧型手機系統內建軟體資通安全檢測技術規範草案。	P40~67 附件 3
4	研提第三方檢測實驗室認可規定修訂草案	已完成資通設備資通安全檢測實驗室管理作業要點修正草案。	P.68~75 附件 4
5	評估技術規範草案可行性	已完成所測暢銷市售手機資安檢測結果分析。	P.76~101 附件 5
6	辦理 3 場次座談會	已完成，並提供會議紀錄及研析意見。	P.102~106 附件 6
7	辦理 2 場次說明會	已完成，並提供會議紀錄及研析意見。	P.107~117 附件 7
8	提出智慧型手機之安全宣導資料	已完成智慧型手機之安全使用宣導資料。	P.118~124 附件 8
9	提出本案與性別相關之統計及分析	已完成性別相關之統計及分析	P.125~127
10	專案工作會議	已召開 9 場專案工作會議	P.128~129 附件 9

貳、期末報告

一、蒐集及研析國際智慧型手機行動裝置資通安全檢測發展現況

隨著智慧型手機軟、硬體技術一日千里，且功能日趨多元化與複雜化，為了解國際間因應智慧型行動裝置資訊安全問題，本計畫整理國際組織、美國、歐盟、中國、英國、日本、新加坡及韓國共 8 個國家/組織所制定政策之相關內容，各國相關之發布文件共 30 份彙整如下表，且提供對應之說明如後，以作為後續研擬資通安全檢測技術規範及檢測實驗室認可規定之參考，詳細研究報告請參考附件 1。

表2　國際間智慧型手機行動裝置資通安全相關文獻整理表

編號	地區	發布單位	相關發布文件
1	國際組織	A. OWASP(Open Web Application Security Project)	1. OWASP Mobile Security Project - Top Ten Mobile Risks(2014)
2	美國	A. U.S. Chief Information Officer and the Federal CIO Council	1. Government Mobile and Wireless Security Baseline(2013/5)
		B. National Institute of Standards and Technology(NIST)	1. SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations(2013/4) 2. SP-800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise(2013/6) 3. SP 800-142, Practical Combinatorial Testing(2010/10) 4. SP 800-164, DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices(2012/10) 5. SP 800-163,Vetting the Security of Mobile Applications (2015/1)
		C. Department of	1. Cyber Threats to Mobile

編號	地區	發布單位	相關發布文件
		Homeland Security(DHS) (US-CERT)	Phones(2011)
		D. Department of Defense(DoD)	1. Commercial Mobile Device Implementation Plan(2013) 2. Mobile Device Strategy(2012) 3. Mobile Operating System Security Requirements Guide Version 1, Release 3 (2013/6)(DISA)
		E. Federal Communications Commission (FCC)	1. Ten Steps to Smartphone Security(2012/12) 2. Ten Steps to Smartphone Security (Android)(2012/12) 3. Ten Steps to Smartphone Security (iOS)(2012/12) 4. Ten Steps to Smartphone Security (Windows Phone)(2012/12) 5. Ten Steps to Smartphone Security (BlackBerry)(2012/12)
		F. National Security Agency(NSA)	1. Mobility Security Guide v2.3(2013/11) 2. Security Requirements for Mobile Operating Systems v1.0 (2013/1) (NIAP)
3	歐盟	A. European Union Agency for Network and Information Security (ENISA)	1. Smartphone secure development guidelines for app developers(2011/11) 2. Top Ten Smartphone Risks(2014)參考到 Smartphones：Information security risks, opportunities and recommendations for users(2010/12)
		B. European Commission	1. Opinion 02/2013 on apps on smart devices(2013/02)

編號	地區	發布單位	相關發布文件
4	中國	A. 工業和資訊化部	1. YD/T 2407-2013 移動智慧終端機安全能力技術要求(2013/4) 2. YD/T2408-2013 移動智慧終端機安全能力測試方法(2013/4)
5	英國	A. Communications-Electronics Security Group(CESG)	1. End User Device Strategy：Security Framework & Controls(2013/2)(ERG)
		B. Information Commissioner's Office (ICO)	1. Personal information online small business checklist
		C. Office of Communication(Ofcom)	1. Safer smartphones–keeping your device secure(2013/10)
6	日本	A. Japan Smartphone Security Forum (JSSEC)	1. Security Guideline for using Smartphones and Tablets(2011/12)
		B. Information-technology Promotion Agency (IPA)	2. 10 Major Security Threats (2013/3)
7	新加坡	A. Monetary Authority of Singapore	1. Technology Risk Management Guidelines(2013/6)
8	韓國	A. Korea Communications Commission	1. KCC announces 'Comprehensive Plans for Smart Mobile Security'(2010/12)

本計畫首先依據各標準發布之目的，將其區分為下列幾種類型，各類型依據其強制性及影響範圍由高至低依序說明如下：

(一)全國強制性之標準規範

國家政府以立法方式，由政府單位把關，強制要求規範所涵蓋之對象遵守，建立條列式的測試項目作為判定之依據。

目前中國大陸是唯一全國強制性規範實施的國家，對欲連上網路之行動裝置，要求需符合最高安全標準。

(二)政府組織內部規範

基於保護國家安全的立場，針對一般的政府單位訂定通用的遵循規範，以及特定的政府單位針對其特殊性質予以強化之規範，後者通常使用在與國家安全相關之政府單位。

(三)組織與企業指引

提供政府組織與企業內部在導入行動裝置與方案之參考，在以資訊安全為考量之前提，協助導入單位透過定義與評估風險、建立框架、參照現有 ISO 標準，以此建立安全的行動裝置作業環境。

(四)使用者/開發者指引

提供一般使用者/開發者強化對於行動裝置使用或程式開發之參考，或，通常以宣導加強安全觀念並輔以簡易的操作設定或觀念說明。

(五)風險評估

主要提供目前行動裝置安全問題之統計與客觀評估。通常被前述四項用來做為設計防禦重點的參考依據。

依據上述分類說明中，本計畫將所收集標準依據同質性加以分類並針對互異之處加以彙整說明如下。

表3　各國規範綜合研析比較表

編號	地區	發布單位	相關發布文件	類型	分類/分層	檢驗分級
1	國際組織	OWASP	1. OWASP Mobile Security Project - Top Ten Mobile Risks (2014)	風險評估	6 類威脅, 10 項弱點	無
2	美國	Federal CIO	1. Government Mobile and Wireless Security	組織與企業指引	4 類威脅 (其中包含	無

編號	地區	發布單位	相關發布文件	類型	分類/分層	檢驗分級
		Council	Baseline(2013/5)		2 類屬於基礎設施受到之威脅)	
		NIST	1. SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations(2013/4)	組織與企業指引	3 種初始化控制等級, 4 種優先等級	無
			2. SP-800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise(2013/6)	組織與企業指引	無	無
			3. SP 800-142, Practical Combinatorial Testing(2010/10)	使用者/開發者指引	無	無
			4. SP 800-164, DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices(2012/10)	組織與企業指引	使用者端裝置 5 層架構	無
			5. SP 800-163,Vetting the Security of Mobile Applications (2015/1)	組織與企業指引	7 種威脅類別 4 類威脅等級	無
		DHS, US-CERT	1. Cyber Threats to Mobile Phones(2011)	使用者/開發者指引	無	無
		DoD	1. Commercial Mobile Device Implementation Plan(2013)	組織與企業指引	無	無
			2. Mobile Device Strategy(2012)	組織與企業指引	無	無

編號	地區	發布單位	相關發布文件	類型	分類/分層	檢驗分級
			3. Mobile Operating System Security Requirements Guide Version 1, Release 3 (2013/6)(DISA)	政府組織內部規範	無	無
		FCC	1. Ten Steps to Smartphone Security(2012/12)	使用者/開發者指引	無	無
			2. Ten Steps to Smartphone Security (Android)(2012/12)		無	無
			3. Ten Steps to Smartphone Security (iOS)(2012/12)		無	無
			4. Ten Steps to Smartphone Security (Windows Phone)(2012/12)		無	無
			5. Ten Steps to Smartphone Security (BlackBerry)(2012/12)		無	無
		NSA	1. Mobility Security Guide v2.3(2013/11)	政府組織內部規範	無	無
			2. Security Requirements for Mobile Operating Systems v1.0 (2013/1) (NIAP)	政府組織內部規範	無	依據 ISO 15408 安全評估共通準則 (Common Criteria) 之分級標準

編號	地區	發布單位	相關發布文件	類型	分類/分層	檢驗分級
3	歐盟	ENISA	1. Smartphone secure development guidelines for app developers(2011/11)	使用者/開發者指引	無	無
			2. Top Ten Smartphone Risks(2014)	使用者/開發者指引	無	無
		EC	1. Opinion 02/2013 on apps on smart devices(2013/02)	使用者/開發者指引	無	無
4	中國	工業和資訊化部	1. YD/T 2407-2013 移動智慧終端機安全能力技術要求(2013/4)	全國強制性之標準規範	使用者端裝置 5 層架構	5 級安全能力，5 級安全功能
			2. YD/T2408-2013 移動智慧終端機安全能力測試方法(2013/4)		無	無
5	英國	CESG	1. End User Device Strategy：Security Framework & Controls(2013/2) (ERG)	政府組織內部規範	12 項安全控制領域	無
		ICO	1. Personal information online small business checklist	使用者/開發者指引	無	無
		Ofcom	1. Safer smartphones–keeping your device secure(2013/10)	使用者/開發者指引	無	無
6	日本	JSSEC	1. Security Guideline for using Smartphones and Tablets(2011/12)	使用者/開發者指引	無	無
		IPA	1. 10 Major Security Threats (2013/3)	風險評估	無	無

編號	地區	發布單位	相關發布文件	類型	分類/分層	檢驗分級
7	新加坡	MAS	1. Technology Risk Management Guidelines(2013/6)	組織與企業指引	無	無
8	韓國	KCC	1. KCC announces 'Comprehensive Plans for Smart Mobile Security'(2010/12)	使用者/開發者指引	無	無

本計畫依據國際組織與各國規範所公告之相關技術細節，進行深入的研究分析並彙整如下，以作為後續檢測項目撰擬參考。

表4　國際組織與各國規範所公告之相關技術細節彙整對應表

類別	技術細節內容
資料授權、儲存與保護	● **OWASP Mobile Top 10 Risk** ➢ M2：應避免使用 NSUserDefaults 的儲存敏感資訊，例如:避免使用 NSManagedObject 所有資料將儲存在未加密的資料庫文件中。 ➢ M2：機密資訊的儲存或暫存有必要考慮使用一個標準的加密函式庫，如 CommonCrypto。但對於特殊敏感的資訊應用，則可考慮使用白箱加密，以避免數位簽名在通用加密函式庫中被找到而造成洩漏。 ➢ M2：Android 可用“setStorageEncryption”以強制加密本地端文件的儲存。而對於 SD 卡儲存某些安全函式可以透過 javax.crypto 中的函式庫實現。 ➢ M2：儲存敏感訊息時，完全依賴於編碼加密或解密密鑰，應考慮提供操作系統預設加密機制外的附加加密。

類別	技術細節內容
	➢ M5：當行動裝置軟體之資料需要從行動裝置匯出時，則該資料需要用使用者金鑰進行加密，以確保僅持正確金鑰者方可存取該資料。 ● **NIST SP 800-164** ➢ 受保護的儲存裝置：保護儲存在設備上資料的機密性和完整性，並當使用中的資料發生未授權的應用程式試圖存取被保護的項目時，應撤銷其存取權限。 ➢ 避免當行動裝置遭竊而導致機敏資料洩露，需要有足夠強健的 Data at Rest (DAR)機制，可參考下列標準： • NIST SP 800-111 敘述有關環境風險和注意事項兩大類設備的資訊、儲存加密技術為終端使用者設備參考指南。 • FIPS-140 敘述有關 DAR 加密保護機制之標準，並保證使用標準化和普遍接受的機制進行加密操作，以及完成獨立的驗證。 • FIPS-199 為了有效的應用基於策略的受保護的儲存媒體，資訊的所有者需要明確定義出資料的保護需求和政策。其中資訊將被進行機密等級分類，並依據使用分類的標準作為處理的依據。 • NIST SP800-60 用以協助對應資訊安全類別，關於醫療資訊、財務或個人資訊之保護，則可進一步參考 NIST SP800-122。 ➢ 加密機制的強健性由加密演算法與密鑰長度所共構，可參考下列標準： • NIST SP800-133 密鑰的生成的準則。 • NIST SP800-90A 建議透過使用確定性隨機變數產

類別	技術細節內容
	生器，來產生具有足夠熵值的隨機變數以提升安全強度。 • NIST SP800-132 建議提供密鑰導出函數，並可用於推導從密碼密鑰對資料加密之密鑰或密鑰的保護的準則。 • ISO / IEC11889 提供重點服務保護加載密鑰用於確保機密性和完整性。此服務可以實現為一個純粹基於軟體服務或與硬體支援的可信平台模組。 • NIST SP800-88rev1，提供媒體清除原則，確立了消除數據的三種方法，以提供不同級別的保護。 ● **NIST SP 800-163** ➢ 啟用已獲得使用者授權功能：應用程式必須描述所有工作、按鈕，選項和其他介面連接所必需的作業並得到使用者確認。 ➢ 避免啟用未授權功能：權限可能透過隱式授予，使應用程式能在未經使用者同意的前提下，擅自使用相關功能。 ➢ 限制權限：應用程式應該只有最小的必要權限，且應避免與使用者授權聲明不一致。需要被加以考量應用程式所獲取權限的如下： • File input/output (I/O) and removable storage • Privileged commands • APIs ➢ 測試應用程式更新：應用程式的新版本都必須經過測試，以確定任何可能產生的新弱點。 ➢ 避免應用程式共謀：避免應用程式可能透過彼此之間

類別	技術細節內容
	的資訊交換，而獲得原本未被使用者授權資料之取得。 ➢ 保護敏感資料：應導入被證明足夠強健的加密機制(參考經 FIPS 140-2 驗證核可之加密機制)，以保護所蒐集/儲存/傳輸敏感資料的機密性和完整性。在隱私處理時也需要被考慮如位置數據、車載攝影照片，及設備身分的應用程式等，也需要被加以保護避免洩露。 ● **YD/T 2408-2013** ➢ 4.6.3 用戶資料的加密儲存：未經授權的軟體無法存取加密儲存區之電話簿資料。 ➢ 4.6.5.1 用戶資料遠端鎖定：受測之行動裝置經鎖定後，在尚未解鎖前，行動裝置持有者無法進行操作。 ➢ 4.6.5.2 用戶資料遠端刪除：受測之行動裝置資料經刪除後，用戶資料無法再被讀取。 ➢ 4.6.6.1 用戶資料的本地備份：透過備份功能進行使用者電話簿、簡訊、多媒體簡訊、郵件與多媒體資料之備份，並產生相關提示。
傳輸協定與保護	● **OWASP Mobile Top 10 Risk** ➢ M2：強制用戶使用標準的 Web API 或登錄方案（通過 HTTPS）進行身分驗證。 ➢ M2：應用程式可應用 SSL / TLS 傳輸機敏資訊，網路會談層或其他敏感數據傳輸到後端 API 或 Web 服務通道之加密保護。 ➢ M3：考慮未來安全弱點發生在 SSL 執行發現的情況下，額外提供數據加密將提供資料保密有效的二次防禦。較新的威脅允許攻擊者在資料通過行動裝置 SSL 庫加密之前截取行動裝置內傳輸中的敏感資訊，並竊

類別	技術細節內容
	聽網路流量後發送到目標伺服器。 ➢ M3：使用 SSL/TLS 傳輸時，應避免網路會談層的混雜，進而造成使用者 session ID 的洩露。 ➢ M6：不應使用被證明有明顯弱點的演算法與通訊協定，例如:RC2, MD4, MD5, SHA1。 ● **NIST SP 800-164** ➢ 透過建立身分，產生連線、維護、共享、蒐集、宣告及處理六個方面已完成整個管理的生命週期。 ➢ 發出服務請求的一方，應對遠端的裝置進行評估，並參與設備上的軟體所使用的通訊協定,以保證機密性、完整性及簽章的正確性，並完成設備驗證。 ● **NIST SP 800-163** ➢ 未加密通訊：當應用程式之間進行內部通訊，則將可能讓應用程式收集額外資訊，並注入惡意資訊。而當使用在對外通訊時(Data network, Wi-Fi, Bluetooth, NFC, etc.)則可能招致中間人攻擊之威脅。 ● **YD/T 2408-2013** ➢ 4.4.1.1.1 藍牙接口開啟/關閉之開關 ➢ 4.4.1.1.2 藍牙接口開啟之受控機制 ➢ 4.4.1.1.3 NFC 接口開啟/關閉之開關 ➢ 4.4.1.1.4 NFC 接口開啟之受控機制 ➢ 4.4.1.2 藍牙配對連接的受控機制 ➢ 4.4.1.3.1 藍牙接口連接狀態顯示 ➢ 4.4.1.3.2 NFC 接口連接提示 ➢ 4.4.1.4.1 藍牙接口數據傳輸受控機制 ➢ 4.4.1.4.2 NFC 接口數據傳輸受控機制

類別	技術細節內容
	➢ 4.4.2.1 有線外圍接口連接建立確認機制：在未發出提示，並獲得使用者授權之前，行動裝置資料無法被存取，僅能進入充電模式。
應用程式執行與安全	● **OWASP Mobile Top 10 Risk** ➢ M5：確保所有身分驗證請求都需要在伺服器端進行。一旦驗證成功，資料將被載入到行動裝置。以確保資料只在認證成功後才可使用。 ➢ M5：如果需要的數據的客戶端儲存時，資料將需要被安全地從使用者之登錄憑證所得之加密密鑰進行加密。 ➢ M2：資料庫應考慮使用 SQLcipher 進行資料加密 ➢ M2:對於存儲在 keychain 的項目應利用安全的 API 加以保護。 ➢ M3：使用受信任的 CA 提供商簽署的證書及要求 SSL 驗證程序的完整。避免使用自簽憑證，作為安全應用程序的一部分 ➢ M3：唯有在確認金鑰使用受信任且有效憑證，並且與伺服器的確認身分後才可建立安全連線。 ➢ M3：在 Android 系統上，移除開發期間所有可能允許應用程序接受所有憑證，如 org.apache.http.conn.ssl.AllowAllHostnameVerifier 或 SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER。如果使用延伸 SSLSocketFactory 的類別，則應確保 checkServer Trusted 方法正確的被實作，使伺服器能有效核對憑證之正確性。

類別	技術細節內容
	➢ M3：在 iOS 系統使用 CFNetwork 時，可以考慮使用安全傳輸 API 來指定受信任的客戶端憑證。幾乎在所有情況下，使用 NSStream 通訊連結 SECURITYLEVEL 的 TLSv1 應使用具備更高標準的密碼強度。以確保（NSURL 或包裝）NSURL 通訊不允許自簽或無效憑證，如 NSURL 類方法 setAllowsAnyHTTPSCertificate。 ➢ M10：行動裝置應用程式在編譯時應針對其完整性檢測，須能夠發現程式碼被新增或修改。應用程式必須能在執行時對完整性衝突做出反應。 ➢ M7：避免行動裝置應用程式遭注入威脅，伺服器應該對下列可能的注入威脅，做適當的處理，包含: SQLite Injection, JavaScript Injection, Local File Inclusion, XML Injection, Format String Injection, Classic C Attacks, Intent Injection/Fuzzing。
系統執行與安全	● **OWASP Mobile Top 10 Risk** ➢ M9：行動裝置應該具備適當的超時保護，以避免未經授權的惡意存取。良好的超時週期根據應用程式的安全敏感性、既有的風險狀況等有很大的不同，建議的方針是： • 15 分鐘的高安全性應用 • 30 分鐘中等安全應用 • 1 小時低安全應用 ➢ M5：行動裝置應用程式中之持久性認證功能，用戶密碼不應該在裝置上儲存。 ➢ M5：理想情況下，行動裝置應用程式應使用能夠讓用戶自行撤銷已安裝特定於裝置之憑證，以確保可避免

類別	技術細節內容
	裝置被盜或遺失時，遭到未經授權的存取。 ➢ M8：避免使用不合時宜的 handleOpenURL 方法處理 URL 的呼叫；應採用 openURL: sourceApplication: annotation 這類的方式與透過安全參數驗證受信任的應用程式白名單。 ➢ M6：避免使用行動裝置應用程式內建加密程序，以防止攻擊者透過逆向工程或繞道的方式,取得機敏資料。 ● **NIST SP 800-164** ➢ 隔離並防止在同一設備上的應用程式和資訊意外交互存取。 ➢ 參考 NIST SP800-88rev1 媒體清除原則，以提供不同級別的保護。 ● **YD/T 2408-2013** ➢ 4.6.1.1 開機密碼保護：行動裝置開啟身分認證功能，以確保唯有持正確密碼方可令行動裝置開機。 ➢ 4.6.1.2 開機後鎖定狀態的密碼保護：行動裝置開啟身分認證功能，以確保唯有持正確密碼方可使用行動裝置。

資料來源： 本計畫彙整

另就本研究案中，我們可瞭解美國於 NIST Special Publication 800-164 規範中，將行動裝置基本架構分為硬體、韌體、作業系統、應用程式及資訊內容，特別針對手機硬體的密碼模組功能的區塊的檢測措施與管理辦法，可參考 NIST「聯邦資訊處理標準」FIPS-140-2 標準來加強手機密碼模組安全功能。而密碼模組是指由硬體、軟體及韌體組合成的模組，用來實現密碼邏輯、程序及密碼演算法。目前對密碼模組檢驗的國家有美國、加拿大與英國，其他國家則將其

納入資訊安全的領域中。在共同準則(Common Criteria, CC)安全評估的保護剖繪(protection profile, PP)中，密碼模組有些也會要求通過 FIPS 140-2 的驗證，所以共同準則安全評估與密碼模組安全需求兩者有互補關係，依據不同的檢測概念執行各自的產品檢驗。

目前由美國及加拿大訂定密碼模組驗證的相關標準，即 FIPS 140-2。美國 NIST 於 1994 年 1 月 11 日公布「密碼模組安全需求規範 FIPS 140-1」，將密碼模組產品安全等級分為四級，於 1994 年 6 月 30 日正式生效。同時美國 NIST 與加拿大通訊安全組織 (Communication Security Establishment, CSE)於 1995 年 7 月 17 日共同宣佈了美國/加拿大「密碼模組核可計畫」(Cryptographic Module Validation Program, CMVP)。美國聯邦政府規定 1997 年 6 月 30 日後採購的密碼模組產品必須通過 CMVP FIPS 140-1 測試；加拿大政府雖然沒有強制規定，但是強烈建議政府採購的密碼模組產品要通過 CMVP FIPS 140-1 測試。NIST/CSE 於 2001 年 5 月 25 日公布 FIPS 140-2，為 FIPS 140-1 的修訂版，並宣布於 2002 年 5 月 25 日正式生效。從 2002 年 5 月 26 日之後，美國聯邦政府與加拿大政府只准購買通過 CMVP FIPS 140-2 測試通過的密碼模組產品。

就上述密碼模組檢驗從提出申請至取得美國 NIST 發證，最快時間約 8 個月，因此許多資通訊系統廠商，都會要求密碼模組設計與研發商，於開發期間就提出認證申請工作，待取得認證後，再將該通過認證之密碼模組整合至資通訊產品，以宣告產品符合國際安全標準。另外，2015 年第 16 屆國際共同準則研討會（ICCC）中，由韓國國家安全研究院(NSRI) Keunwoo Rhee 先生提到，為了解決行動裝置安全議題，韓國從 2014 年 8 月起集結產官學各單位人馬針對行動裝置安全議題進行討論，以共同準則(Common Criteria, CC)架構並列出行動裝置安全功能要求，包含資料保護、身分認證、安全管理、存取控管、可信賴路徑，以及延伸定義組件平台與應用管理

保護。本計畫依據 Common Cretia 最近一版公告的行動裝置基礎保護規範(Mobile Device Fundamentals Protection Profile, MDFPP)，有關硬體安全技術資訊彙整如下表所示。

表5　共通準則硬體安全深度彙整分析表

序號	項目	技術要求與檢測說明
1	受信任的傳輸通道	行動裝置能提供建立與通訊目標之可信任安全連線，且在傳輸期間對通訊資料加以保護，傳輸過程應符合 IEEE、RFC 發佈之信任通道建立標準。相關參考標準如下列所示： IEEE 802.11-2012, IEEE 802.11ac-2013 IEEE 802.1X, RFC 5280, 2560, 5759
2	開機自我測試	行動裝置開機過程，需通過所有與密碼有關之功能及系統軟體完整性檢測。
3	連續認證失敗次數監測	應具備正整數次之驗證錯誤計數機制，當嘗試錯誤超過門檻值，需抹除受應保護之資訊。
4	金鑰管理	加密金鑰及通訊密鑰之產生、交換、合併與銷毀。 應符合 NIST、ANSI 及 IEEE 發佈之金鑰使用及管理標準。相關參考標準如下列所示: ANSI X9.31-1998, IEEE 802.11-2012, IEEE 802.11ac-2013, IEEE 802.1X, NIST SP 800-38A, 38C~F, 56A~B, 57, 90B
5	金鑰儲存保護	所有的儲存於行動裝置之金鑰，都需要對其機密性與完整性，透過金鑰額外保護。故行動裝置應具備適當之機制，以對存放於行動裝置之金鑰保證其機密性與完整性。

序號	項目	技術要求與檢測說明
6	金鑰傳輸保護	行動裝置之金鑰應具備適當的存放與管理機制，且明文金鑰不得存放於非揮發性之記憶體、不得用任何方式匯出或直接對外傳輸。
7	演算法要求	行動裝置使用之加/解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發佈之金鑰演算法標準。相關參考標準如下列所示: ANSI X9.31-1998, IEEE 802.11-2012 IEEE 802.11ac-2013, IEEE 802.1X NIST SP 800-38A, 38C~F, 56A~B, 57, 90B
8	產生初始化向量	行動裝置所有使用之加密模式，應各自對其初使化向量產生要求。因此加密模式應符合 NIST 發佈之初始化向量要求。相關參考標準如下列所示: NIST SP 800-38A, 38C~F, 56A~B, 57, 90B
9	產生隨機位元	金鑰使用之亂數以確定性方式產生隨機位元。 符合 NIST、ANSI 發佈之隨機位元產生規範要求。相關參考標準如下列所示:ANSI X9.31-1998, NIST SP 800-38A, 38C~F, 56A~B, 57, 90B

資料來源： 本計畫彙整

反觀國內手機資安檢測也會遭遇到測試時程與晶片掌握度等問題，就研究團隊了解目前國內手機業者亦向各專業廠商採購硬體零件進行組裝，硬體(例如：手機晶片)相關安全性，實掌握在該硬體製造商而非手機原廠中。若強制要求進行硬體晶片的安全檢測工作，除產品認證須耗費較長時間，同時也影響產品上市時間，也降低廠商送檢驗意願，而失去安全檢測的目的。因此建議參考國際手機資安的檢測管理模式，由主管機關將晶片硬體功能檢測獨立並訂定相關

檢測規範，並利用手機產品的分層架構特性及對應的檢測要求規範做法，以提升國內手機資安檢測規範實施的可行性。

另加上目前收集到的規範多數均以使用者資料安全以及行動裝置應用程式為主要考量，因此本計畫藉由上述條件歸納彙整出 10 份主要標準，作為後續規範與檢測執行之主要參考依據，藉此提升整體與全面性考量。

基於風險評估與使用者指引之各規範共通性內容加以歸納，可明確得出以下結論：首先透過資料收集與分析，事先評估所可能遭遇之風險。其次是將各種風險依據智慧型行動裝置之特性，進行適當之分級分類(例如：YD/T 2407-2013、YD/T 2408-2013 及 SP800-164)以達到風險管理之目的，以及參考規範中對於分級分類後進一步深化訂定檢測內容。最後，則是依據各企業/政府組織內部的資訊安全政策(例如：美國國防部、美國國家安全局)或規範安全評估，進行實作及預防資訊安全風險之相關管制措施，以期達到全面性的防護成效。詳細各國分析請參閱附件 1。

二、研提智慧型手機資安風險評估報告

參考國際之智慧型手機資安相關評估文件，針對智慧型手機之韌體、作業系統及出廠時內建應用軟體等風險，提出智慧型手機資安風險評估報告，內容包括資安風險評估方法、流程、範圍、面向、等級及結果等。

(一)安全目標

行動裝置需要支援多元的安全目標，典型的作法是整合許多的安全功能在裝置裡，通常的安全目標如下：

機密性：確保傳輸或是儲存的資料，不會遭到未獲授權者的讀取。

完整性：偵測傳輸或是儲存的資料，遭到故意或是非故意的改變。

可用性：確保使用者可以利用行動裝置，在需要時存取所需資源。

(二)風險之定義

風險的定義，參考 ISO 31000:2009 係指：對於組織目標之不確定影響(effect of uncertainty on objectives)。所謂影響：係指對於預期結果的誤差，包括正向與負向的結果。

另參考 ISO/IEC 27000:2009 係指：事故發生的潛在可能性及其後果。

(三)風險評鑑技術與方法

ISO 31010:2009 風險管理—風險評鑑技術(Risk management -- Risk assessment techniques)提供系統化的風險評鑑方法選擇及應用的指引文件，詳細內容詳見附件 2。

CNS/ISO/IEC 27005：2011 之附錄 E 建議之二項資訊安全風險評鑑作法，摘述如後：

1.高階風險評鑑作法

高階風險評鑑允許定義行動之優先順序及時間表，基於各種理由例如：預算，單位可能無法同時實作所有的控制措施，故應將最關鍵之風險優先處理。高階風險評鑑作業之優點如下：

- 一開始採用較簡單之作法，容易獲得風險評鑑參與人員之接受。
- 可做為良好之輔助規劃，以建構資訊安全之策略藍圖。
- 可將資源及預算運用於最有利之處。

惟由於初始採用高階風險評鑑，潛在地存在評鑑結果較不精確，可能未識別某些營運過程或系統，可視需要針對高安全等級之資產，進行詳細風險評鑑作業。

2.詳細風險評鑑作法

詳細風險評鑑對於資產進行深度之識別與鑑別作業，並針對資產詳細列出其可能面臨之威脅與可能存在之脆弱性，以做為評鑑其風險與風險處理方法之依據。

詳細風險評鑑作法可以是定量或是定性的方法，或是二者之結合。宜根據資產之價值，或需被保護之特性，以評鑑威脅發生之可能性。CNS/ISO/IEC 27005 於該文件之附錄 E 中，列舉了符合 ISO 31010 所示之後果可能性矩陣(Consequence/probability matrix)法之實務範例，但不以此為限。

3.預先定義值之矩陣

預先定義值矩陣主要考量資產之價值、威脅發生之可能性及脆弱性被利用之程度，以排序待因應之風險，範例詳見圖 1 所示，摘述說明如後：

	發生可能性－威脅	低			中			高		
	易被利用	低	中	高	低	中	高	低	中	高
資產價值	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

資料來源： CNS 27005

圖1　預先定義值矩陣範例(一)

(1)資產價值

依據資產之建置成本或是置換成本加以估價，再轉換成相同性尺度。

資產之價值可以經由與資料擁有者之晤談，依據不利之營運後果可合理預期發生之最壞情境加以估計，可以參考「資訊系統分類分級鑑別機制」的作法，例如對於資料保護受到損害或是影響業務運作之情境，經訪談後設定置換成本，資產安全等級區分為普、中、高三級，可以再轉換成相同性尺度，細分為0~4之五等級區分，以表示資產之價值，另實務當中對於資訊資產之衡量，亦會採用評估「機密性C」、「完整性I」與「可用性A」之組合[CIA]加以衡量。

部分單位會將資產價值之[CIA]組合表示成以下二種模式：

A.資產價值[CIA]＝C + I + A

B.資產價值[CIA]＝C x I x A

(若採用相乘之方式，建議將以上所述之相同性尺度修訂為1~5等級區分，以避免相乘之後，產生資產價值為0之情形)

不論採用相加或是相乘之計算模式，經轉換成相同性尺度之後，所代表之意義均是排序後之結果，代表因應風險的優先順序，至於要採用相加或是相乘的方法，可以視需求與尺度範圍而定，並無優劣之分。

(2)發生可能性—威脅。

將威脅發生之可能性，區分為低、中、高三級。

(3)脆弱性易被利用之程度。

再將威脅利用脆弱性之容易程度，區分為低、中、高三級。

經由以上方法識別風險之相關量測組合，尺度由 0~8，填入於矩陣之內。

另一範例顯示類似之矩陣，分析營運衝擊之程度，另考量事故情境發生之可能性，以排序風險處理之優先順序。

	事故情境之可能性	非常低 (非常不可能)	低 (不可能)	中 (有可能)	高 (可能)	非常高 (經常)
營運衝擊	非常低	0	1	2	3	4
	低	1	2	3	4	5
	中	2	3	4	5	6
	高	3	4	5	6	7
	非常高	4	5	6	7	8

資料來源： CNS 27005

圖2　預先定義值矩陣範例(二)

縱軸將營運衝擊程度由非常低至非常高，區分為 5 個尺度，分別為 0~4。

橫軸將事故情境之可能性由非常低至非常高，區分為五個尺

度，分別為 0~4。再將兩軸之尺度值相加，產生 0~8 尺度，詳見圖 2 所示。

以上範例所列示之 0~8 尺度，可以再簡化成為整體風險等級，例如：

A.低風險：0~2。

B.中風險：3~5。

C.高風險：6~8。

4.依風險之量測排序威脅

本方法將後果(資產價值)之因素與威脅發生之可能性(將脆弱性層面納入考量)相關聯，詳見圖 3 所示。

威脅描述詞 (a)	後果(資產) 值 (b)	威脅發生 可能性 (c)	風險量測 (d)	威脅排序 (e)
威脅 A	5	2	10	2
威脅 B	2	4	8	3
威脅 C	3	5	15	1
威脅 D	1	3	3	5
威脅 E	4	1	4	4
威脅 F	2	4	8	3

資料來源： CNS 27005

圖3　依風險之量測排序威脅之範例

(1)首先依據預先定義之尺度，範例中採用的是 1~5，評估各受威脅資產之後果(資產價值) (b 欄位)。

(2)同樣依預先定義之尺度 1~5，評估各威脅發生之可能性(c 欄

位)。

(3)藉由相乘(bxc)計算風險之量測。

(4)最後再依風險相關之量測順序排序威脅(e 欄位)。

(四)行動裝置風險評估流程

參酌以上風險評鑑技術所描述之高階風險評鑑作法及詳細風險評鑑作法，以下各列舉國際規範中所適用之行動裝置風險評鑑作法，摘述如後：

1.NIST 行動裝置安全管理參考指引

美國國家標準局 NIST SP 800-124r1「機關行動裝置安全管理參考指引」(Guidelines for Managing the Security of Mobile Devices in the Enterprise)，當前行動裝置主要資安風險來源列舉七大面向，並建議在設計與建置行動裝置之安全控制措施時，須針對行動裝置以及經由行動裝置接取的資源，發展系統威脅模型(threat models)。

威脅模型包括確認利益相關的資源、威脅與漏洞以及這些資源的安全管控，然後進行成功攻擊與影響的量化工作，藉以分析相關資訊，以作為安全管控的改進或強化的決策參考。威脅模型幫助組織確認安全要項，以協助設計行動裝置的解決方案，期所有管控均能符合相關的安全要求。

NIST 在該指引中提出了七項：行動裝置的高階威脅與弱點(High-Level Threats and Vulnerabilities)，依據風險評鑑方法之區分，屬於「高階風險評鑑作法」。

(1)欠缺實體安全保護(Lack of Physical Security Controls)

(2)使用不可信任之行動裝置(Use of Untrusted Mobile Devices)

(3)使用不可信任之網路(Use of Untrusted Networks)

(4)使用不可信任之軟體(Use of Untrusted Applications)

(5)與其他系統之交互作用(Interaction with Other Systems)

(6)使用不可信任之內容(Use of Untrusted Content)

(7)使用定位服務(Use of Location Services)

2.OWASP 行動安全專案(Mobile Security Project)

開放網路軟體安全計畫，簡稱 OWASP(Open Web Application Security Project)是一個開放社群、非營利性組織，全球目前有 82 個分會，其主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善應用程式的安全性。美國聯邦貿易委員會(FTC)更強烈建議所有企業務必遵循 OWASP 所發布的十大網路弱點防護守則，美國國防部亦將此守則列為最佳實務。此網站每年度收集之資料分析相關行動裝置 APPs 之風險與威脅並公告，目前已知歐盟在 2011 年 11 月所發表的 Smartphones secure development guidelines for app developers 文件中，亦參考此資料做為制定指引之基礎。

(1)OWASP 行動應用威脅模型(Mobile Application Threat Model)

因應雲端技術快速的發展，不論是使用者或應用程式開發者，資訊的操作模式已逐漸地從主機平台移至可攜式行動裝置或智慧型手機，即使平台不同，既然是由人所開發的應用程式，必定會產生一定程度的弱點風險。

OWASP 採用行動應用威脅模型(Mobile Application Threat Model)作為詳細風險評鑑作法之依據，研究方法將行動裝置遭受的威脅分成 6 大分類，分別為：

- 詐欺(Spoofing)
- 拒絕/否認(Repudiation)
- 阻斷服務(Denial of Service)
- 篡改(Tampering)
- 資訊洩漏(Information Disclosure)
- 提升權限(Elevation of Privilege)

3.行動裝置 10 大風險

OWASP 再將上述分類依照風險所造成嚴重性衝擊(例如：機密性、完整性、可用性)加以定出行動裝置十大風險。概略說明如下：

資料來源： OWASP Top Ten Mobile Risks 2014

圖4　行動裝置 10 大風險

表6　行動裝置 10 大風險

編號	風險名稱	內容	建議作法
M1	伺服器端的控制薄弱	主要是說明 Mobile 的弱點並不只單存在於 Mobile 端，所開發的 APP 應用程式或雲端系統的程式亦有可能存在弱點，例如：OWASP Cloud Top 10。	人員於伺服器端開發應用程式時，應避免產生 OWASP Web Top 10 或 OWASP Cloud Top 10 相關弱點
M2	不安全的資料儲存	意指敏感性資料未受到適當的保護，一般常見如敏感性資料未加密，或是一些不常用到的暫存資料可能含有敏感訊息，可能會造成機密性資料損失、憑證外洩、侵犯隱私權等衝擊。	只儲存必要資訊，不將敏感資料存放於開放式的儲存媒體，採用安全的檔案加密應用程式介面，設定檔案的讀取與寫入設定權限等。
M3	傳輸層保護不足	可攜式行動裝置於傳輸機敏性資料時，很常發生未加密情況，可能會造成駭客使用中間人攻擊(Man-in-the middle attacks)，從中竄改或竊取封包資料，進而造成機敏資料的洩漏。	程式開發者應確保所有敏感性資料有採用加密方式進行傳輸，若只採用明文方式傳遞，攻擊者可輕易透過網路監聽方式(Sniffer)竊取機敏性資料。
M4	非故意的資料外洩	可攜式行動裝置中的第三方應用程式可能會自動幫使用者儲存一些敏感性資訊，一但攻擊者成功取得行動裝置權限時，將會侵犯使用者隱私，甚至導致資料洩漏情形。	一些較敏感性的資料應避免自動儲存於可攜式行動裝置內，檢查部分應用程式是否會儲存敏感性資訊，建議加以手動移除，或是選擇不自動儲存功能。
M5	粗糙的授權與認證	部分可攜式行動裝置的網頁應用程式僅採用永不變的數值來執行身分驗證與授權階	使用嚴謹的身分驗證與授權(例如：雙因素認證)，避免使用可攜式行

編號	風險名稱	內容	建議作法
		段	動裝置的硬體 ID 標籤或永不變的 ID 識別碼做為身分驗證的因素
M6	加密失效	所謂加密失效分為兩種情況，一種是使用強健的加密演算法卻遭到破解，另一種為使用過於簡單的加密演算法遭到破解。前者要實現的困難度較高，後者則是相當常見。	開發應用程式建議使用強健的加密演算法，並不斷進行反覆測試，直到應用程式開發完成時，仍需執行嚴格的挑戰測試(Battle-Tested)。
M7	客戶端注入	Injection 攻擊即使從傳統電腦轉移到了可攜式行動裝置上的網頁應用程式，若網頁應用程式存有 Injection 弱點，攻擊者仍可利用 SQL Injection 或 XSS 攻擊手法來提升可攜式行動裝置的權限，或是利用網路盜打市話(Toll Fraud)的情況發生。	網頁應用程式傳遞參數給雲端資料庫的內容，需過濾不受信任或不應該接受的內容，例如：SQL 執行語法、特殊字元等，同樣可採用 prepared statement 功能進行過濾。
M8	不受信任的輸入	在各種可攜式行動裝置的平台均會發生，應用程式可能經由惡意攻擊者精心設計，或是應用程式遭攻擊者透過 Client Side Injection 攻擊方式來消耗可攜式行動裝置的硬體資源或提升權限情形。	每個應用程式在設計時應注意身分認證與授權的問題，以確保可攜式行動裝置需經過使用者的身分驗證後才允許執行特殊的行為或功能。
M9	不適當的會話處理	可攜式行動裝置的應用程式 session 過期時間，一般而言會設定的比較長，原因是對使用者方便存取或使用。	若需要提高安全性，相對其軟硬體設計(演算法或操作方式)的複雜度亦會增高，只要 session 值的過期時間應設定在一個可接受範圍內，就

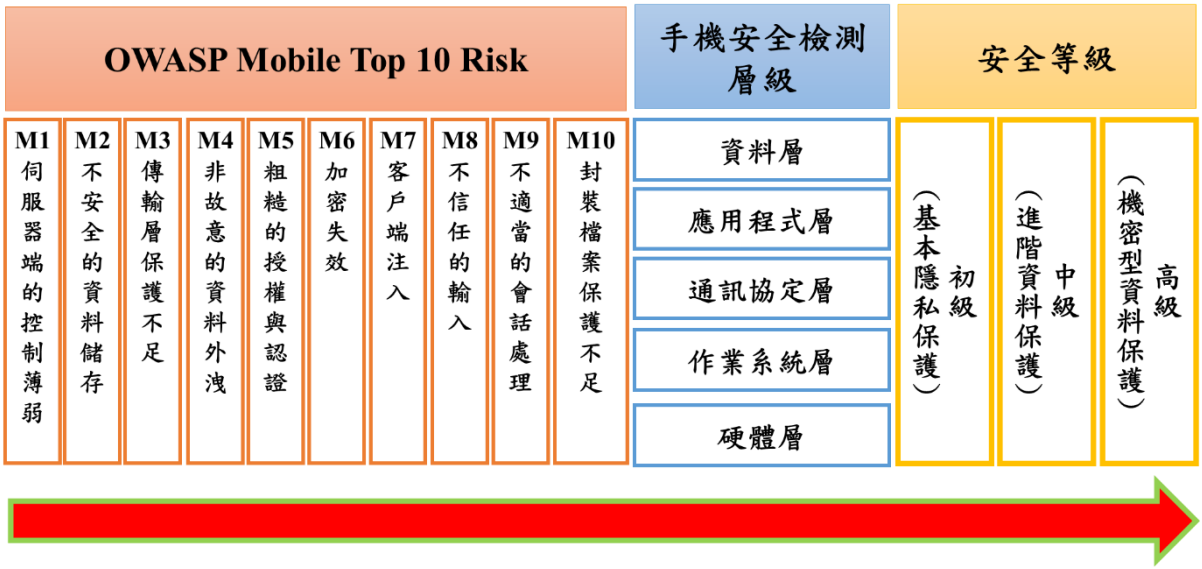
編號	風險名稱	內容	建議作法
			無需擔心讓使用者太頻繁的重新驗證。
M10	封裝檔案保護不足	此弱點的洩漏方式，乃是指應用程式原始碼中，把輸入或輸出的相關參數直接寫入在程式碼當中，因此只要攻擊者能夠取得應用程式的原始碼，若原始程式碼內容含有敏感資訊，可能會造成企業敏感性資料洩漏情況。	程式開發者應避免將敏感資訊寫入於原始程式碼中

資料來源： OWASP

(五)智慧型手機風險評估框架

本案遵循高階風險評鑑作法，並參考 OWASP Mobile Top 10 Risk，作為風險評鑑之威脅分析依據，以評估智慧型手機在資料層、應用程式層、通信協定層、作業系統層及硬體層，作為智慧型手機風險評估框架，評估當「機密性」、「完整性」及「可用性」喪失，可能造成之衝擊程度，區分為以下三級：

- 初級：基本隱私保護
- 中級：進階資料保護
- 高級：機密型資料保護



資料來源：本計畫彙整

圖5　智慧型手機風險評估框架

(六)檢測單元區分

依據國際間對智慧型手機安全之分層概念，本規範將智慧型手機安全區分為資料層、應用程式層、通訊協定層、作業系統層及硬體層五個層別，主要考量不同層別可能面臨的資訊安全風險有所不同，並對各層別訂定技術要求。智慧型手機通過所屬技術要求之檢測項目，即表示達到該檢測安全需求與安全期望。

(七)安全等級

依據上述風險評估方法，將智慧型手機內建軟體檢測區分 3 個等級，分別定義為：

1.初級-基本隱私保護：智慧型手機提供個人使用者隱私相關的資料安全，包含手機安全性功能和個人資料相關保護，如蒐集個人資料的行為必須明確告知使用者。

2.中級-進階資料保護：智慧型手機提供完整資料保護機制，包含使用中、儲存及傳輸中的資料，確保所有資料在各狀態下可被

安全使用。

3.高級-機密型資料保護：智慧型手機須確保核心底層不被竄改或被不正當的獲取資訊。

(八)智慧型手機風險評估矩陣

綜上所述之風險評估框架，彙整智慧型手機風險評估矩陣，以供後續檢測規範發展之要件。

表7　智慧型手機風險評估矩陣表

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
M4：Unintended Data Leakage(非故意的資料洩漏)	D.1	D.1.1.B	資料使用授權	手機系統內建軟體於存取敏感性資料前，應取得使用者同意	初
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	D.1	D.1.2.M(+)	資料使用授權	手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。	中
M2：Insecure Data Storage(不安全的資料儲存)	D.2	D.2.1.B	資料儲存保護	手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。	初
M2：Insecure Data Storage(不安全的資料儲存)	D.2	D.2.2.M(+)	資料儲存保護	手機系統內建軟體於儲存敏感性資料時提供資料加密功能，以避免遭不正當方式取得敏感性資料。	中

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
M2：Insecure Data Storage(不安全的資料儲存)	D.2	D.2.3.M(+)	資料儲存保護	手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於程式碼中，以避免遭不正當的方式存取。	中
M2：Insecure Data Storage(不安全的資料儲存)	D.3	D.3.1.B	資料遺失保護	手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，讓使用者可在遠端啟動鎖定。	初
M2：Insecure Data Storage(不安全的資料儲存)	D.3	D.3.2.B	資料遺失保護	手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，讓使用者可在遠端移除資料。	初
M2：Insecure Data Storage(不安全的資料儲存)	D.3	D.3.3.B	資料遺失保護	手機系統應提供資訊備份功能。	初
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.1	A.1.1.B	程式身分辨識	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。	初
M5：Poor Authorization and Authentication(不	A.2	A.2.1.B	程式信任來源	手機系統內建軟體具備付費服務時，應使用有效期間之伺服器憑	初

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
安全的授權與鑑別)				證，以避免使用過期的憑證。(A.2.1.B(+)適用無圖示軟體)	
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.2	A.2.2.B	程式信任來源	手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。	初
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.3	A.3.1.B	程式執行授權	手機系統內建軟體在使用付費服務前，應提示並取得使用者同意後才可執行。	初
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.3	A.3.2.B	程式執行授權	手機系統內建軟體應僅使用其所需之權限，且權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。	初
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	A.3	A.3.3.M	程式執行授權	手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路服務連接埠(本地服務)」相符。(A.3.3.M(+)適用無圖示軟體)	中
M5：Poor Authorization and Authentication(不	A.3	A.3.4.M(+)	程式執行授權	手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。	中

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
安全的授權與鑑別)					
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.3	A.3.5.M(+)	程式執行授權	手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。	中
M7：Client Side Injection(使用者端注入)	A.4	A.4.1.B	程式執行安全	手機系統內建軟體應提供回報安全性問題之管道	初
M7：Client Side Injection(使用者端注入)	A.4	A.4.2.M	程式執行安全	手機系統內建軟體應具隱碼攻擊字串的處理能力。	中
M7：Client Side Injection(使用者端注入)	A.4	A.4.3.M	程式執行安全	手機系統內建軟體應具延伸標記語言攻擊字串的處理能力。	中
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	P.1	P.1.1.B	協定使用授權	手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。	初
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	P.1	P.1.2.B	協定使用授權	當手機之無線傳輸技術功能確認開啟時，應給予使用者相對應的提示狀態。	初
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	P.1	P.1.3.B	協定使用授權	手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。	初

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	P.2	P.2.1.B	協定傳輸保護	手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。(P.2.1.B(+)適用無圖示軟體)	初
M9：Improper Session Handling(不適當的通訊控制)	P.2	P.2.2.M	協定傳輸保護	手機系統內建軟體應避免交談識別碼遭重送攻擊。	中
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	P.2	P.2.3.M	協定傳輸保護	手機系統內建軟體與付費服務伺服器間之資料加密傳輸，應使用安全之加密演算法。(P.2.3.M(+)適用無圖示軟體)	中
M9：Improper Session Handling(不適當的通訊控制)	P.3	P.3.1.M	協定執行安全	手機系統內建軟體應具通訊協定內容的錯誤處理能力。	中
M4：Unintended Data Leakage(非故意的資料洩漏)	O.3	O.3.2.M	系統執行安全	手機之作業系統應具位址空間配置隨機化功能，以避免程式與參考函式在記憶體中的位址為固定值。	中
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	O.3	O.3.3.H	系統執行安全	手機之作業系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。	高

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
M4：Unintended Data Leakage(非故意的資料洩漏)	O.3	O.3.4.H	系統執行安全	手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。	高
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	O.3	O.3.5.H	系統執行安全	手機之作業系統應具備驗證錯誤計數機制，當嘗試錯誤超過門檻值，應抹除受保護之資訊。	高
M6：Broken Cryptography(不安全的加密保護)	H.1	H.1.1.H	金鑰管理保護	手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀。應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。	高
M6：Broken Cryptography(不安全的加密保護)	H.1	H.1.2.H	金鑰管理保護	手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。	高
M6：Broken Cryptography(不安全的加密保護)	H.1	H.1.3.H	金鑰管理保護	金鑰不得以明文方式存放於非揮發性之記憶體、且不得用任何方式匯出或直接對外傳輸。	高
M6：Broken Cryptography(不安全的加密保護)	H.2	H.2.1.H	演算法強度要求	手機實作之加/解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發布之金鑰演算法標準。	高

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
M6：Broken Cryptography(不安全的加密保護)	H.2	H.2.2.H	演算法強度要求	手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。	高
M6：Broken Cryptography(不安全的加密保護)	H.2	H.2.3.H	演算法強度要求	金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。	高

資料來源：本計畫彙整

其中 M1 伺服器端安全控制脆弱於本規範中並無設計檢測項目，主要考量本規範檢測範疇鎖定於整支手機的檢測，M1 主要著重於檢測伺服器端安全性問題，就目前智慧型手機系統內建軟體所連結之服務主機，其伺服器之控管實已超出手機系統內建軟體之範疇，並參考經濟部工業局於 105 年 1 月所公布之「行動應用 App 基本資安檢測基準 V2.0」最新版規範中，亦未檢測此項目，是以綜合考量下，本規範亦未納入此類型相關檢測項目，但為求整體檢測完整性，仍於 O.1.1.B 測項納入資料連結伺服器之測項，並由廠商於自我宣告表中聲明「資料連結伺服器之 IP/DN/公司主機名稱」，以為確認。

三、研提我國智慧型手機系統內建軟體資通安全檢測技術規範草案

參酌國際作法及考量我國產業環境，研析智慧型手機系統內建軟體資通安全包括韌體、作業系統及出廠時內建應用軟體等，進一步研提我國智慧型手機系統內建軟體資通安全檢測技術規範草案，完整規範草案內容請參考附件 3。

本規範主要分析當前智慧型手機安全威脅來源、風險評估、資安趨勢以及常見資安問題，並針對國際間現行管理與技術規範、資安指引、方法論或安全開發技術等資料進行評估，據此提出「智慧型手機系統內建軟體資通安全檢測技術規範草案」，內容包含安全分級、技術要求、檢測項目、檢測方法及判定標準，藉以制定出適合我國產業型態之檢測技術規範。

在分析與研究目前國際間相關手機安全檢測相關標準後，選定三個具備行動裝置完整測試框架與一個完整說明行動應用程式安全審驗之國際標準或規範，並加上美國二份重要文件，做為研擬技術規範參考依據，詳如下所列：

- OWASP Mobile Security Project
- NIST SP 800-164
- NIST SP 800-163
- ITU-T YD/T 2407-2013
- NSA-IAD
- DoD-DISA

由上述文件據以建構符合我國手機產業之技術規範測試框架；在整體技術測試框架完備後，即展開各項安全測試項目與判定標準設計，並提出安全要求等級，以做為技術規範草案內容之擬定。技術規範研

究流程詳如圖 6：

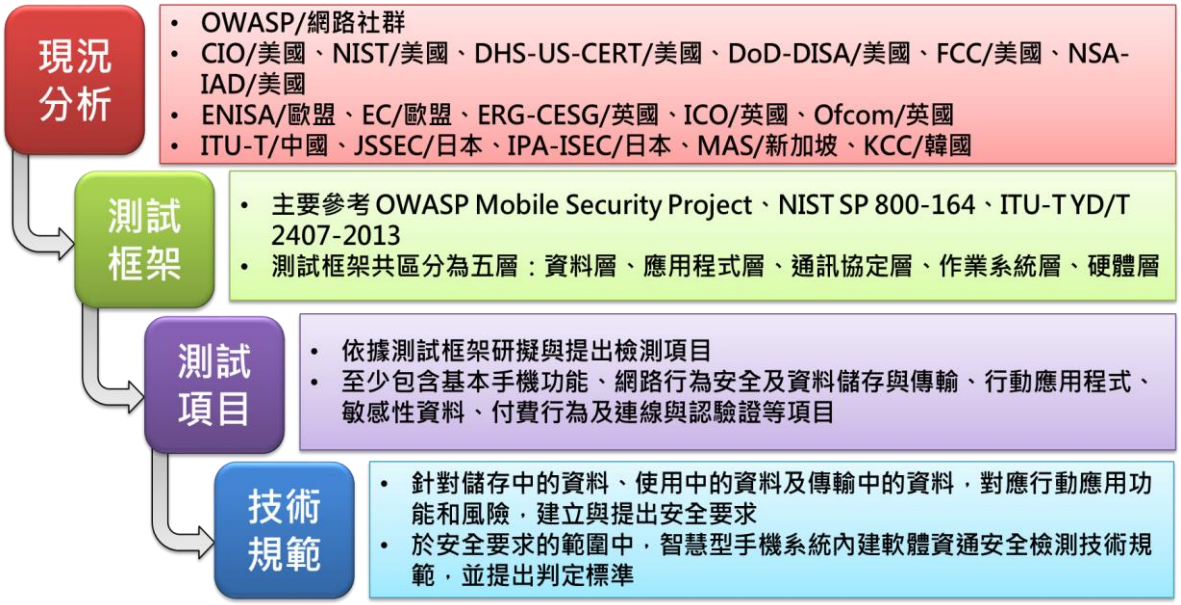


圖6　技術規範研究流程

資料來源：本計畫彙整

(一)規範架構

在技術安全檢測方面，主要針對行動裝置可能面臨的資安問題進行檢測技術規範的規劃與研擬，並參考 NIST SP 800-164「Giudelines on Hardware-Rooted Security in Mobile Devices (Draft)」中所提出行動裝置架構與安全概念，將行動裝置區分為不同層級，並依據不同層級來定義出基本的安全功能準則，依此所設計出的測試規範，將可涵蓋行動裝置上可能發生的安全問題。行動裝置架構詳如圖 7：

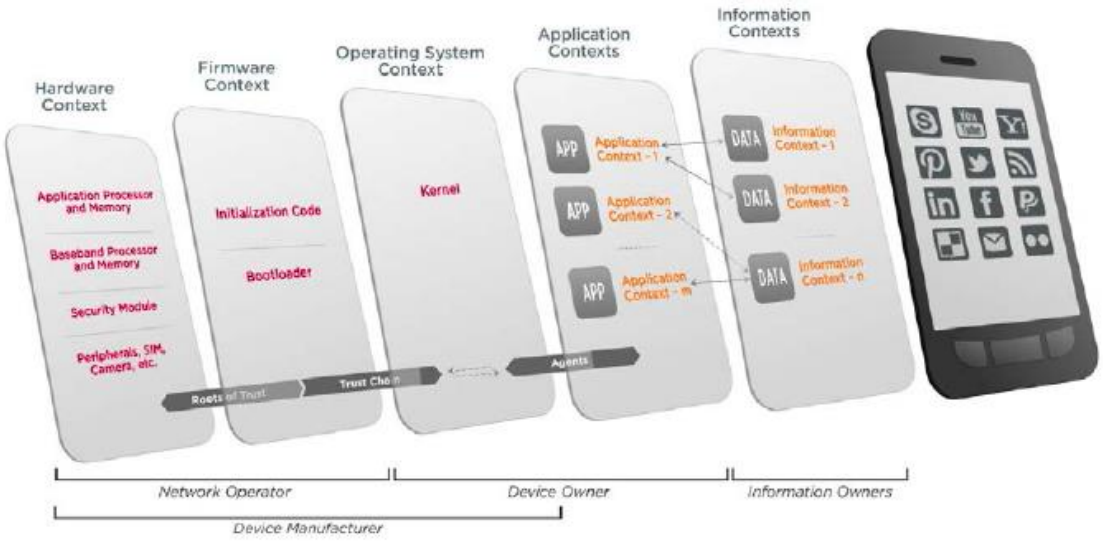


圖7　行動裝置架構圖

資料來源：NIST SP 800-164

除了參考上述 NIST SP 800-164 中的行動裝置分級外，針對內建應用軟體部分，以 NIST SP 800-163 做為參考之依據，行動應用軟體審驗程序之主要步驟及相關參與人員，是一系列以確定行動應用軟體是否符合安全需求為目的之活動，本計畫另酌參其他國際標準中所訂定行動裝置層級，歸納出行動裝置層級區分為 3-5 個層級。茲將重要國際組織與國家規範或標準對於行動裝置層級彙整之分析詳如表 7。

表8　國際標準行動裝置層級

層級/參考文件	OWASP TOP 10 Mobile Risks	NIST SP 800-164	YD/T 2407.2408-2013	NSA-IAD	DoD-DISA
1	Information/ Data	Information/Contexs	使用者資料	Information/Data	Information /Data
2	APPs	Applications Contexs	應用層	APPs	APPs

層級/參考文件	OWASP TOP 10 Mobile Risks	NIST SP 800-164	YD/T 2407.2408-2013	NSA-IAD	DoD-DISA
3	Library/ Dependencies/ Driver	OS Contexs	外圍接口	OS	OS
4	OS	Firmware Contexs	操作系統	N/A	N/A
5	Hardware	Hardware Contexs	硬體(測項另訂)	N/A	N/A

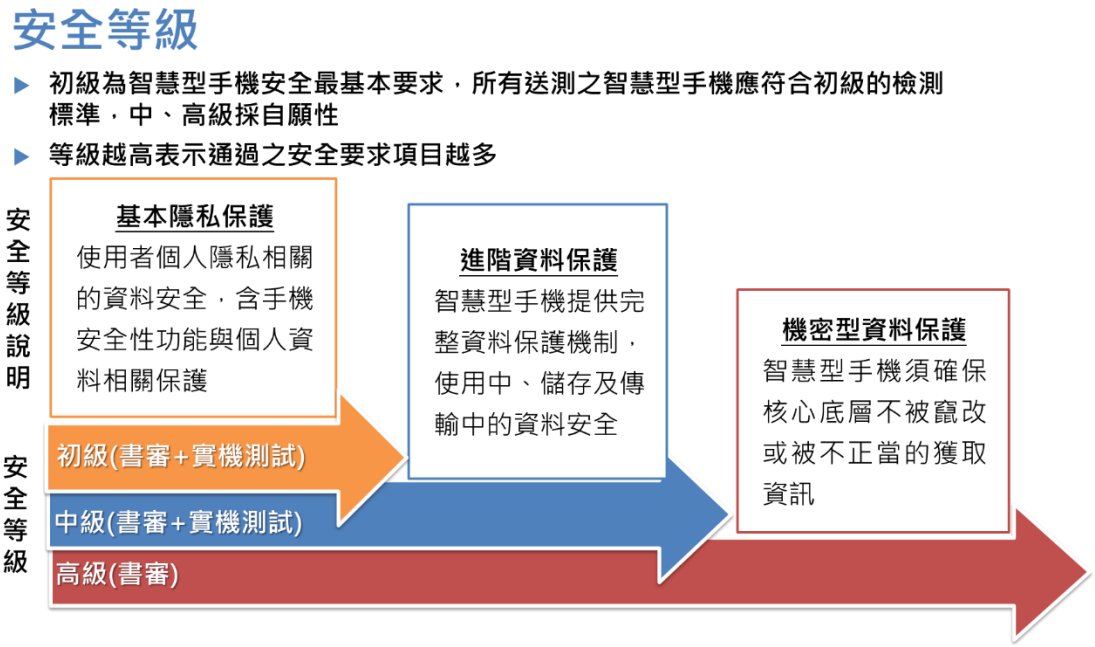
資料來源：本計畫彙整

依據研析結果可知，目前較為完整定義出行動裝置層級之標準或指引分別為 OWASP Top 10 Mobile Risks、NIST SP 800-164 以及中國大陸 YD/T 2407.2408-2013。有鑑於此，本計畫亦參照國際常見行動裝置定義的層級，將行動裝置安全架構分為資料層(Information/Data)、應用程式層(APPs)、通訊協定層(Protocol)、作業系統層(Operation System)以及硬體層(Hardware)。

(二)規範安全等級

本規範適用於智慧型手機系統及其內建軟體，以確保其符合現階段資訊安全要求。為配合不同安全需求，初期將智慧型手機系統內建軟體安全等級區分為基礎與進階 2 種，然經多次專家座談會以及與 NCC 之工作會議討論後，則最後以使用者在意之安全考量為基準，將安全等級規劃為初級、中級及高級 3 種。初級為智慧型手機基本隱私保護最低要求，中級必須符合初級所有檢測細項並新增資料進階保護之檢測細項，高級主要乃為確保智慧型手機之核心底層不會被遭到竄改或不正當地擷取資訊，因此須符合初級與

中級，並納入手機設計相關安全性文件審定之檢測細項。所有智慧型手機均應通過初級檢測項目之檢測細項，然中級與高級部分則採自願性檢測。



資料來源：本計畫彙整

圖8　安全等級

(三)檢測要求

檢測要求包括書面審視與實機測試兩個部分。書面審視主要為申請單位提供檢測申請書、廠商自我宣告表及安全功能規格表等文件，透過文件檢視以利實驗室執行檢測細項；實機測試則為檢測實驗室依據檢測細項所執行之測試。申請單位提出送測申請後，檢測實驗室應依據本規範所說明之適用範圍進行書面審視與實機測試。

1.內建軟體屬性

智慧型手機系統內建軟體(以下簡稱系統內建軟體)檢測範圍包含出廠預設、銷售商加載及無圖示軟體 3 種屬性：

(1)出廠預載軟體：智慧型手機出廠時預設搭載安裝之應用程

式，且使用者可透過圖示啟動。

(2)銷售商加載軟體：智慧型手機銷售時預設搭載或首次連結網路後自動安裝之應用程式，且使用者可透過圖示啟動。

(3)無圖示軟體：於上述兩種情況所安裝之應用程式，使用者無法透過圖示啟動，然該軟體會將資料回傳至後端伺服器。

2.檢測層別

依據國際間對智慧型手機安全之分層概念，本規範將智慧型手機區分為資料層、應用程式層、通訊協定層、作業系統層及硬體層五個層別，考量不同層別可能面臨的資訊安全風險有所不同，故對各層別訂定檢測項目。

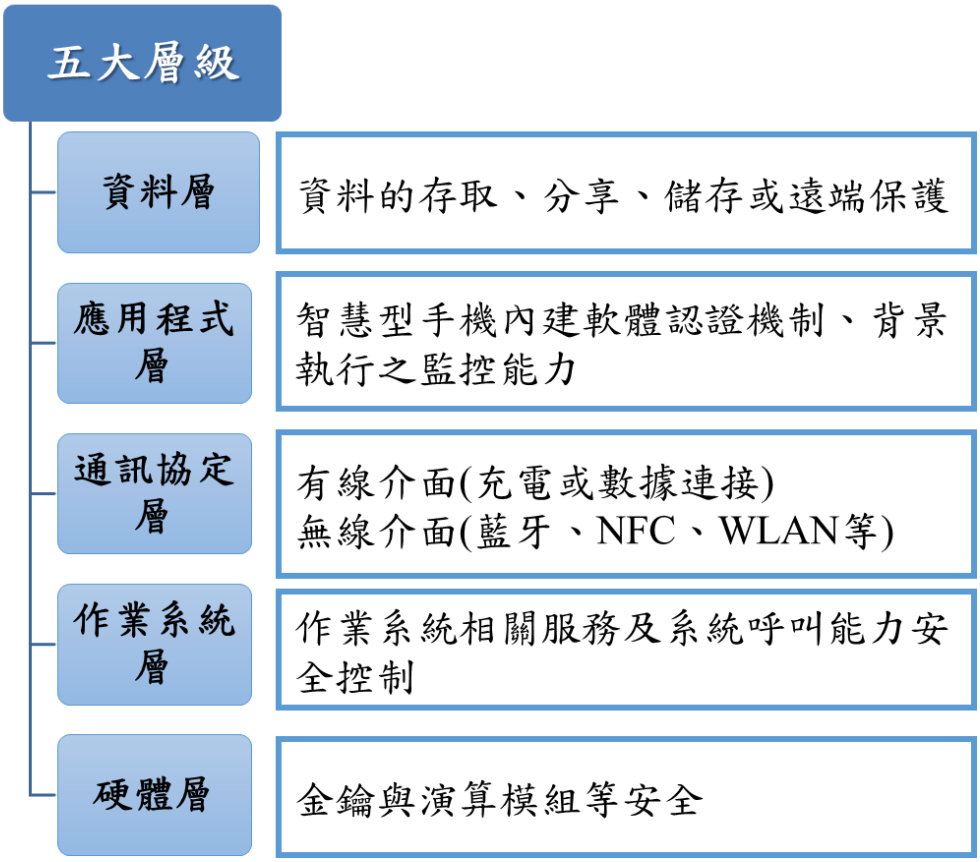
(1)資料層(Information/Data)：主要包含資料的傳送、儲存或使用等相關安全。

(2)應用程式層(APPs)：主要包含手機系統內建軟體等相關安全。

(3)通訊協定層(Protocol)：主要包含有線介面、無線介面及通訊協定等相關安全。

(4)作業系統層(Operating System)：主要包含作業系統相關服務與各硬體元件存取等相關安全。

(5)硬體層(Hardware)：主要包含金鑰與演算模組等安全。



資料來源：本計畫彙整

圖9　規範檢測架構

3.資料型別

參考個人資料保護法之定義，個人資料指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。然本計畫定義敏感性資料指個人資料或手機相關資訊遭外洩或竄改將可能導致個人或資料擁有者的權益受損。

蒐集國內外對於敏感性個資之說明，包含歐盟個資公約中解釋報告(Explanatory Report)中描述『資料之內容(contents)並不會

對個人造成傷害，只有「資料之使用情境(context)」才會對個人造成傷害，但某些特殊類型資料，其「資料之內容」卻很可能侵害個人權利或利益…』。

綜合上述，本規範依資料之敏感性與是否為使用者輸入等兩個因素，將其分成第 1 型、第 2 型、第 3 型、第 4 型，其中第 1 型與第 2 型為敏感性資料，而資料型別分類說明如表 9，另依「個人資料保護法之特定目的及個人資料之類別」擬列之識別類共有 134 類(C○○一~C一三四)，其中C○○一、C○○二、C○一二、C○三五及C○七三內容與手機系統使用相關，其餘皆不適用，因此將該識別項目與本規範定義之資料型別範例進行對照如表 10。

表9　資料型別分類表

型別	判斷標準		範例
	是否屬於敏感性資料	是否為使用者輸入	
第 1 型	是	是	1.本規範用語釋義之個人資料。 2.手機相關資訊：簡訊內容、通話錄音、裝置密碼、帳號密碼。
第 2 型	是	否	IMEI、IMSI[註]、定位資訊。
第 3 型	否	否	APPs 列表、音樂播放資訊、手機作業系統、手機型號、手機韌體版本、MCC、MNC、行動通信業者、網路傳送方式、設定檔(可蒐集但應提示，不得修改、刪除及傳輸)。
第 4 型	N/A	N/A	資料加密、協定加密、無加密但內容未知。

型別	判斷標準		範例
	是否屬於敏感性資料	是否為使用者輸入	
[註]IMEI 碼及 IMSI 碼如須與行動通信業者或手機廠商之銷售保固連結，該 IMEI 碼及 IMSI 碼才具個資識別性，但使用人與登錄人可能不同，故歸類為第 2 型。			

資料來源：本計畫彙整

表10　資料型別與個人資料保護法之對照

個人資料保護法		本規範		
代碼	範例	資料型別	範例	不適用於本規範之項目
C〇〇一辨識個人者	姓名、職稱、住址、工作地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電或其他任何可辨識資料本人者等	第1型	本規範用語釋義之個人資料。	相片
C〇〇二辨識財務者	金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、個人之其他號碼或帳戶等	第1型		
C〇一一個人描述	年齡、性別、出生年月日、出生地、國籍、聲音等	第1型		

個人資料保護法		本規範		
代碼	範例	資料型別	範例	不適用於本規範之項目
C〇一二身體描述	身高、體重、血型等	第1型		
C〇三五休閒活動及興趣	嗜好、運動及其他興趣等	第3型	APP 列表、音樂播放資訊、	
C〇七三安全細節	密碼、安全號碼與授權等級等	第1型	帳號密碼、裝置密碼	
無此類別		第2型	IMEI、IMSI、定位資訊	
無此類別		第3型	手機作業系統、手機型號、手機韌體版本、MCC、MNC、行動通信業者、網路傳送方式、設定檔	

資料來源：本計畫彙整

(四)檢測項目

本規範依據層別訂定檢測項目，檢測項目再依各檢測項目安全需求訂定檢測細項，各檢測項目與檢測細項說明如表 11、表 12，檢測項目與檢測細項之編碼原則為：層別代碼．檢測項目編號．檢測細項編號．安全等級代碼，各層別代碼依序為 D(資料層)、A(應用程式層)、P(通訊協定層)、O(作業系統層)、H(硬體層)，各安全等級之代碼依序為初級(B)、中級(M)及高級(H)；如資料層第 1 個檢測項目所屬編號為 D.1，第 1 個檢測細項為初級是以其檢測編號

則為 D.1.1.B，依此類推。若為選測項目則標示(+)，此檢測細項可由送測單位自由選擇是否檢測。

表11 檢測項目說明

層別	檢測項目	安全需求
資料層	D.1 資料使用授權	手機系統內建軟體對敏感性資料進行存取前，應取得使用者同意。
	D.2 資料儲存保護	手機系統內建軟體應將敏感性資料儲存於作業系統保護區域，並提供資料加密功能，以避免敏感性資料遭不正當方式存取。
	D.3 資料遺失保護	手機系統應提供資料保護與備份功能，以避免資料外洩和防止資料損失。
應用程式層	A.1 程式身分辨識	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。
	A.2 程式信任來源	手機系統內建軟體應確認付費功能機制與資料來源的安全。
	A.3 程式執行授權	手機系統內建軟體所執行的行為，應取得使用者同意，並與其宣告之內容相符。
	A.4 程式執行安全	手機系統內建軟體應具備惡意字串輸入時的處理能力。
通訊協定層	P.1 協定使用授權	手機與外部設備進行連接時，應給予使用者相對應的提示，並提供開啟及關閉無線傳輸技術之功能。
	P.2 協定傳輸保護	手機系統內建軟體與伺服器間之資料加密傳輸，應使用安全之加密演算法，並避免可能的傳輸攻擊。
	P.3 協定執行安全	手機系統應具備通訊協定內容的錯誤處理

層別	檢測項目	安全需求
		能力。
作業系統層	O.1 系統操作授權	手機系統所執行的行為，應取得使用者同意，必要時並提供風險提示。
	O.2 系統身分辨識	手機系統應提供安全的身分辨識及保護機制。
	O.3 系統執行安全	手機系統應具備程式執行期的記憶體保護機制，並提供安全回報之管道。
硬體層	H.1 金鑰管理保護	手機之金鑰管理，應符合金鑰使用及管理標準。
	H.2 演算法強度要求	手機實作之加密、解密及簽章演算法，應符合金鑰演算法標準與初始化向量要求。

資料來源：本計畫彙整

1.檢測細項內容

依據五大層級之各檢測項目延伸檢測細項內容，各檢測項目進一步發展相關檢測條件、檢測步驟與判斷標準，詳細內容詳見附件 3。

表12 檢測項目與檢測細項對應表

檢測項目	**檢測編號**	**檢測細項**
D.1 資料使用授權	D.1.1.B	手機系統內建軟體於存取敏感性資料前，應取得使用者同意。
	D.1.2.M(+)	手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。
D.2 資料儲存保護	D.2.1.B	手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。
	D.2.2.M(+)	手機系統內建軟體於儲存敏感性資料時應提供

檢測項目	檢測編號	檢測細項
		資料加密功能，以避免遭不正當方式取得敏感性資料。
	D.2.3.M(+)	手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。
D.3 資料遺失保護	D.3.1.B	手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。
	D.3.2.B	手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。
	D.3.3.B	手機系統應提供資料備份功能。
A.1 程式身分辨識	A.1.1.B	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。
A.2 程式信任來源	A.2.1.B	手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。
	A.2.2.B	手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。
A.3 程式執行授權	A.3.1.B	手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。
	A.3.2.B	手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。

檢測項目	檢測編號	檢測細項
	A.3.3.M	手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路連接埠(本地服務)」相符。
	A.3.4.M(+)	手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。
	A.3.5.M(+)	手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。
A.4 程式執行安全	A.4.1.B	手機系統內建軟體應提供回報安全性問題之管道。
	A.4.2.M	手機系統內建軟體應具備隱碼攻擊字串的處理能力。
	A.4.3.M	手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。
P.1 協定使用授權	P.1.1.B	手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。
	P.1.2.B	當手機之無線傳輸技術功能確認開啟時，應給予使用者相對應的提示狀態。
	P.1.3.B	手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。
P.2 協定傳輸保護	P.2.1.B	手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。
	P.2.2.M	手機系統內建軟體應避免交談識別碼遭重送攻擊。

檢測項目	檢測編號	檢測細項
	P.2.3.M	手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。
P.3 協定執行安全	P.3.1.M	手機系統應具備通訊協定內容的錯誤處理能力。
O.1 系統操作授權	O.1.1.B	手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。
	O.1.2.B	手機系統於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。
O.2 系統身分辨識	O.2.1.B	手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。
	O.2.2.B	手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。
	O.2.3.B	手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。
	O.2.4.M	手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。
O.3 系統執行安全	O.3.1.B	手機系統應提供回報安全性問題之管道。
	O.3.2.M	手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。
	O.3.3.H	手機系統應建立與通訊目標間受信任的傳輸通

檢測項目	檢測編號	檢測細項
		道，作為傳輸期間資料保護使用。
	O.3.4.H	手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。
	O.3.5.H	手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。
H.1 金鑰管理保護	H.1.1.H	手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。
	H.1.2.H	手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。
	H.1.3.H	金鑰不得以明文方式存放於非揮發性之記憶體，且不得用任何方式匯出或直接對外傳輸。
H.2 演算法強度要求	H.2.1.H	手機實作之加密、解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發布之金鑰演算法標準。
	H.2.2.H	手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。
	H.2.3.H	金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。

資料來源：本計畫彙整

2.選測項目說明

另為求檢測規範可適用於各作業平台，並且將檢測時間與檢測費用等成本建置於合理之範圍內，從目前進行實測的手機檢視，於安全等級初級者設定為基礎資料傳輸，並且適合各作業

平台，部分無法適用於各作業平台及無圖示軟體之檢測細項，則納入中級之選測項目中，送測單位自由選擇是否進行檢測。而於檢測編碼上，則由(+)標示為選擇檢測項目。(檢測項目作業系統適用性結果詳見表 12)。

(五)檢測細項參考依據對照

本國智慧型手機系統內建軟體資安檢測規範須與國際規範內容接軌，故參考國際之智慧型手機資安相關評估文件包括：中國 YD/T 2407.2408-2013、OWASP Mobile Security Project - Top Ten Mobile Risks、NIST SP800-163、NIST SP800-164 及 Samsung 於通過 CC 之 TOE 報告中，初步擬列於 CC 安全評估的保護剖繪(protection profile, PP)架構中，與手機檢測相關書審及驗證項目內容，本計畫共歸納 43 個檢測項目，資料層(Data)8 個、應用程式層(APPs) 11 個、通訊協定層(Protocol) 7 個、作業系統層(Operating System) 11 個、硬體層(Hardware) 6 個。

囿於我國相關業務分工，上架至線上市集之行動應用軟體由經濟部主管，目前已由經濟部工業局研擬「行動應用 APP 基本資安檢測規 v2.0」。手機及其出廠時已內建軟體由國家通訊傳播委員會主管，由本計畫團隊研擬「智慧型手機系統內建軟體資通安全檢測技術規範(草案)」。以智慧型手機分層架構中，二份規範皆有對應至資料層與應用程式層，因此在各專家會議中常拿來討論比較，其主要探討重點以檢測項目之訂定是否適宜、安全需求為何、廠商該如何配合、檢測實驗室該如何檢測及其判定的依據為何...等，為求國內手機相關檢測規範未來通用可能性，故將二份規範相同之處調整為相似檢測項目與方法，茲將本規範與「行動應用 APP 基本資安檢測規範」之差異比較分析詳見表 13(比較版本：工業局 v2.0、NCCv0.9 期末審查修訂版)，而各檢測項目與所參考之規範來源詳

見表 14。

表13　本規範與「行動應用 APP 基本資安檢測規範」之差異

項次	工業局(v2.0) 初級檢測項目(6 項)	NCC(v0.9)
1.	4.1.2.3.4.行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中	D.2.1.B 手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。
2.	4.1.2.3.5.敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存	D.2.2.M(+)手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。 D.2.3.M(+)手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。
3.	4.1.2.3.6.敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取	D.2.1.B 手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。
4.	4.1.2.3.7.敏感性資料應避免出現於行動應用程式之程式碼	D.2.3.M(+)手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。
5.	4.1.5.1.1.行動應用程式應避免含有惡意程式碼	無此測項 原因：因惡意程式碼會因不同檢測工具而有不同定義，造成各檢測實驗室判定標準不一，故工作會議決議不納

項次	工業局(v2.0) 初級檢測項目(6 項)	NCC(v0.9)
		入測項。
6.	4.1.5.4.1.行動應用程式應針對使用者輸入之字串，進行安全檢查	A.4.2.M 手機系統內建軟體應具備隱碼攻擊字串的處理能力。
7.	4.1.1.1.2.行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途 (工業局撰擬規範團隊表示本測項與NCC 要求之精神一致，然未檢視於 App 商店提供之相關說明，並未訂定具體檢測要求，規劃於下一版本修訂)	A.1.1.B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。 A.3.2.B 手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。
8.	4.1.1.3.1.行動應用程式開發者應提供回報安全性問題之管道	A.4.1.B 手機系統內建軟體應提供回報安全性問題之管道。 O.3.1.B 手機系統應提供回報安全性問題之管道。
9.	4.1.2.1.1.行動應用程式應於蒐集敏感性資料前，取得使用者同意	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。
10.	4.1.2.1.2.行動應用程式應提供使用者拒絕蒐集敏感性資料之權利	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。
11.	4.1.2.3.1.行動應用程式應於儲存敏感性資料前，取	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。

項次	工業局(v2.0) 初級檢測項目(6 項)	NCC(v0.9)
	得使用者同意	
12.	4.1.2.3.2.行動應用程式應提供使用者拒絕儲存敏感性資料之權利	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。
13.	4.1.2.4.1.行動應用程式透過網路傳輸敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。	P.2.1.B 手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。 P.2.3.M 手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。
14.	4.1.2.5.1.行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意	D.1.2.M(+)手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。
15.	4.1.2.5.2.行動應用程式應提供使用者拒絕分享敏感性資料之權利	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。
16.	4.1.2.5.3.行動應用程式分享敏感性資料時，應避免未授權之行動應用程式存取	此測項對使用者而言，威脅性在於行動應用程式間共享資料後，將敏感性資料傳輸至伺服器端，因此本規範中於下列測項中做檢測： P.2.1.B 手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。 P.2.3.M 手機系統內建軟體與付費功能

項次	工業局(v2.0) 初級檢測項目(6 項)	NCC(v0.9)
		伺服器間之資料加密傳輸，應使用安全之加密演算法。
17.	4.1.4.1.1.行動應用程式應有適當之身分認證機制，確認使用者身分	A.1.1.B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。
18.	4.1.4.1.2.行動應用程式應依使用者身分授權	A.1.1.B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。
19.	4.1.4.2.1.行動應用程式應避免使用具有規則性之交談識別碼	P.2.2.M 手機系統內建軟體應避免交談識別碼遭重送攻擊。
20.	4.1.4.1.2.行動應用程式應依使用者身分授權	A.2.1.B 手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。
21.	4.1.4.2.3.行動應用程式應確認伺服器憑證為可信任之憑證機構、政府機關或企業簽發	無此檢測細項 原因：「可信任」的憑證機構、政府機關或企業等，未有明確清單可引用，故實驗室無法明確判定，故不納入測項
22.	4.1.4.2.4.行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料	A.2.1.B 手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。
23.	4.1.5.1.2.行動應用程式應避免資訊安全漏洞	P.2.3.M 手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安

項次	工業局(v2.0) 初級檢測項目(6 項)	NCC(v0.9)
		全之加密演算法。
24.	4.1.5.3.1.行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本	無此檢測細項 原因：因廠商反應，實務上不會因為引用函式庫有更新就會提供對應的更新版本，而是依據更新的內容來決定，故不納入測項。
25.	4.1.5.4.2.行動應用程式應提供相關注入攻擊防護機制	A.4.2.M 手機系統內建軟體應具備隱碼攻擊字串的處理能力。 A.4.3.M 手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。
26.	4.1.3.1.1.行動應用程式應於使用付費資源前主動通知使用者	A.3.1.B 手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。
27.	4.1.3.1.2.行動應用程式應提供使用者拒絕使用付費資源之權利	A.3.1.B 手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。
28.	4.1.3.2.1.行動應用程式應於使用付費資源前進行使用者認證	A.3.1.B 手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。
29.	4.1.3.2.2.行動應用程式應記錄使用之付費資源與時間	無此檢測項目 原因：若未有紀錄功能並不會影響手機安全性，故經工作會議評估討論後決議不納入測項。

資料來源： 本計畫彙整

表14 檢測項目與各規範對應關係

檢測編號	檢測細項	各國規範					
		1	2	3	4	5	6
D.1.1.B	手機系統內建軟體於存取敏感性資料前，應取得使用者同意。	V	V	V		V	
D.1.2.M(+)	手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。	V	V			V	
D.2.1.B	手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。		V			V	
D.2.2.M(+)	手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。		V		V	V	V
D.2.3.M(+)	手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。		V		V	V	V
D.3.1.B	手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。		V	V			
D.3.2.B	手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。		V	V			
D.3.3.B	手機系統應提供資料備份功能。		V	V			
A.1.1.B	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。		V		V	V	
A.2.1.B	手機系統內建軟體具備付費功能時，應		V		V		

檢測編號	檢測細項	各國規範					
		1	2	3	4	5	6
	使用有效期間之伺服器憑證，以確保付費交易之安全。						
A.2.2.B	手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。		V		V		
A.3.1.B	手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。		V				
A.3.2.B	手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。						
A.3.3.M	手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路連接埠(本地服務)」相符。				V		
A.3.4.M(+)	手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。						
A.3.5.M(+)	手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。						
A.4.1.B	手機系統內建軟體應提供回報安全性問題之管道。		V				
A.4.2.M	手機系統內建軟體應具備隱碼攻擊字串的處理能力。		V				
A.4.3.M	手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。		V				
P.1.1.B	手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。			V			
P.1.2.B	當手機之無線傳輸技術功能確認開啟			V			

檢測編號	檢測細項	各國規範					
		1	2	3	4	5	6
	時，應給予使用者相對應的提示狀態。						
P.1.3.B	手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。			V			
P.2.1.B	手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。	V	V		V	V	V
P.2.2.M	手機系統內建軟體應避免交談識別碼遭重送攻擊。		V		V		
P.2.3.M	手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。		V		V		
P.3.1.M	手機系統應具備通訊協定內容的錯誤處理能力。						
O.1.1.B	手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。			V	V		
O.1.2.B	手機系統於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。						
O.2.1.B	手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。		V	V			
O.2.2.B	手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。					V	
O.2.3.B	手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。						

檢測編號	檢測細項	各國規範					
		1	2	3	4	5	6
O.2.4.M	手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。		V	V		V	
O.3.1.B	手機系統應提供回報安全性問題之管道。						
O.3.2.M	手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。				V		V
O.3.3.H	手機系統應建立與通訊目標間受信任的傳輸通道,作為傳輸期間資料保護使用。	CC 安全評估的保護剖繪(protection profile, PP)之手機檢測項目					
O.3.4.H	手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。						
O.3.5.H	手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。						
H.1.1.H	手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。						
H.1.2.H	手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。						
H.1.3.H	金鑰不得以明文方式存放於非揮發性之記憶體，且不得用任何方式匯出或直接對外傳輸。						
H.2.1.H	手機實作之加密、解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發布之金鑰演算法標準。						

檢測編號	檢測細項	各國規範					
		1	2	3	4	5	6
H.2.2.H	手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。						
H.2.3.H	金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。						
1.NCC-103 年手機系統內建軟體資安評估 2.工業局-行動應用 APP 基本資安規範 3.中國- YD/T 2407.2408-2013 4.OWASP TOP 10 MOBILE RISKS 5.NIST SP800-163 6.NIST SP800-164							

資料來源：本計畫彙整

資料來源：本計畫彙整

圖10　本規範與國際/國內規範之差異

(六)安全標章

1.標章設計

安全標章的設計以盾牌形象比喻安全防護意象，標章名稱定義為「資安認證 手機內建軟體」，以星星數量明顯區分初級、中級與高級 3 種安全等級差異，並印上 NCC logo 明確告知管控所屬機關，依照使用需求不同，顏色上設計彩色版與黑白版兩款，彩色版以 NCC Logo 暗紅色為主色，並搭配金框，不僅呼應 NCC Logo 顏色，更給人可靠防護的深刻印象。

2.發證編碼原則

為使標章上能明確提供檢測相關訊息，特於標章上納入 10 碼數字，以利標章管理，說明如下：

YY mm sss tt L

- YY：表年份(0-9，0-9)：西元 2007 年以 07 表示，2008 年以 08 表示…依此類推。
- mm：表設備商(A~Z，A-Z):設備商 AA，設備商 AB…依此類推。
- sss：表設備型號(0-9，0-9):型號 00，型號 01…依此類推。
- tt：表版本號碼(0-9，0-9): 版本 00，系列 01…依此類推。
- L：表安全等級(1-3)：1:普級；2:中級；3:高級。

資料來源：本計畫彙整

圖11　安全標章(彩色版)

資料來源：本計畫彙整

圖12　安全標章(黑白版)

四、研提第三方檢測實驗室認可規定修訂草案

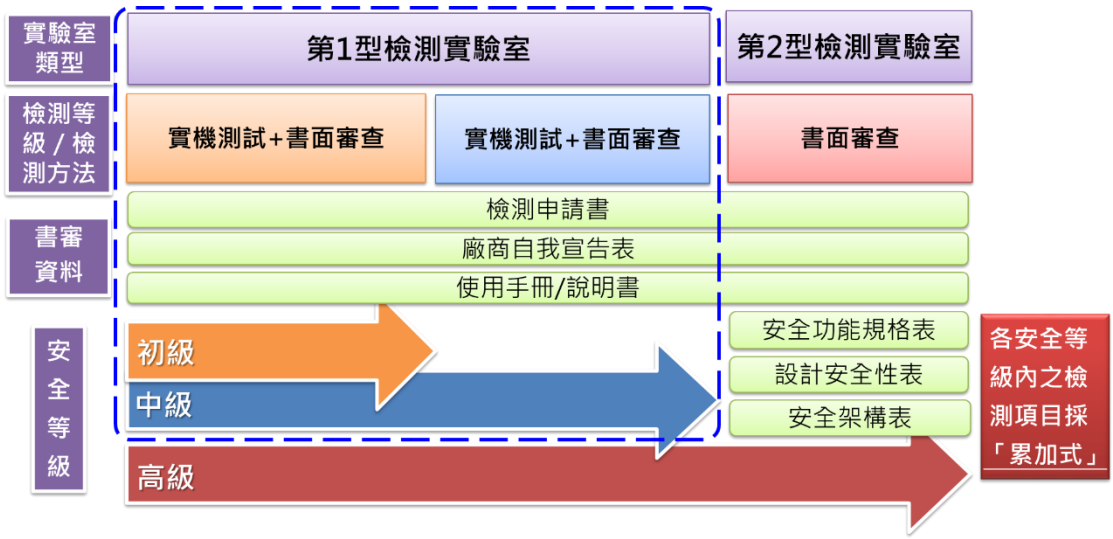
(一)檢測實驗室資格修訂要點

本會執行前期研究計畫時，於 100 年完成資通設備安全檢測實驗室管理作業要點草案，並已公告於通傳會網站。為使智慧型手機系統內建軟體資通安全檢測技術規範於未來落實檢測時，能確保資通安全品質，故修訂資通設備資通安全檢測實驗室管理作業要點，內容包括下列項目：

- 實驗室應具備之檢測能力

- 實驗室人員(含技術主管、品質主管、報告簽署人)具備之資格
- 實驗室申請書(含檢測範圍與檢附文件)
- 檢測實驗室認可證書
- 檢測費用
- 其他相關規定

智慧型手持式行動臺安全檢測實驗室依檢測範圍等級區分實驗室資格包含「第 1 型」與「第 2 型」，第 1 型檢測實驗室須提供安全等級初級與中級之檢測服務，第 2 級檢測實驗室則須提供安全等級高級之檢測服務。本要點參考資通設備安全檢測實驗室相關規定外，亦參考工業局經濟部工業局行動應用 App 基本資安自主檢測推動 v1.0 之檢測實驗室認可程序審查修調內容如下表所示，並修調要點如附件 4。



資料來源：本計畫彙整

圖13　檢測實驗室分類圖

表15 智慧型手持式行動臺安全檢測實驗室管理要點訂定重點摘錄

修改項目	調整主要內容
前言	1. 國家通訊傳播委員會(以下簡稱本會)為確保智慧型手機系統內建軟體資通安全品質，執行智慧型手機系統內建軟體資通安全檢測實驗室(以下簡稱檢測實驗室)認可與管理作業，特訂定本要點。 2. 本會認可之檢測實驗室分為第 1 型及第 2 型檢測實驗室，由申請擔任檢測實驗室者(以下簡稱申請人)依智慧型手機系統內建軟體資通安全檢測技術規範之檢測範圍申請之。
一般規定	應審查下列各款事項： 1. 智慧型手機系統內建軟體資通安全檢測實驗室申請書。 2. 依法設立之本國法人、機構之證明文件影本。 3. 取得本國實驗室認證組織核發符合中華民國國家標準（以下簡稱 CNS）17025 或國際標準化組織所定標準(以下簡稱 ISO/IEC）17025 有關測試與校正實驗室能力一般要求規定之認證證明影本。
實驗室成員(含技術主管、品質主管、報告簽署人)具備之資格	1. 第 1 型檢測實驗室： (1). 技術主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且具資訊安全相關管理職經驗 2 年以上或從事資安測試評估實務工作達 2 年以上，並具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。 (2). 品質主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且從事品質管理、專案管理或稽核相關工作經驗 2 年以上，並具備品質管理、專案管理或稽核相關訓練合格證書。 (3). 報告簽署人：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且具資訊安全相關工作經驗 3 年以上，並符合以下規定：

修改項目	調整主要內容
	A. 具備道德駭客認證（Certified Ethical Hacker，CEH）或國際網路資安認證（CompTIA Security+）有效之資訊安全相關專業證照。 B. 具備下列任一證照:資訊系統安全專家認證(Certified Information Systems Security Professional, CISSP)、資安軟體開發專家認證(Certified Secure Software Life-cycle Professional, CSSLP)、資安分析專家認證(EC-Council Certified Security Analyst, ECSA)、資安鑑識調查專家認證(EC-Council Computer Hacking Forensic Investigator, CHFI)、滲透測試專家認證(GIAC Penetration Tester, GPEN)或行動裝置資安分析專家認證(GIAC Mobile Device Security Analyst, GMOB)、安全程式設計師認證(EC-Council Certified Secure Programmer, ECSP)、資安專業人員認證(Systems Security Certified Practitioner, SSCP)。 C. 非屬本目所列有效之資訊安全相關專業證照者，需經 NCC 認可。 2. 第 2 型檢測實驗室： (1). 技術主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且具資訊安全相關管理職經驗 2 年以上或從事資安測試評估實務工作達 2 年以上，並具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。 (2). 品質主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且從事品質管理、專案管理或稽核相關工作經驗 2 年以上，並具備品質管理、專案管理或稽核相關訓練合格證書。 (3). 報告簽署人：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、

修改項目	調整主要內容
	電信工程、電子工程、電機工程或其他相關科系畢業，並具備接受 CCRA 或本會認可實驗室之 ISO/IEC 15408 測試評估相關專業訓練時數至少 360 小時以上之證明文件影本，且從事資通設備資安檢測評估實務工作達 2 年以上。 3. 智慧型手持式行動臺安全檢測實驗室基本成員至少 3 人，應分別為： (1). 具備技術主管資格者 1 人 (2). 具備品質主管資格者 1 人 (3). 具備報告簽署人資格者 1 人 4. 實驗室主管與智慧型手持式行動臺安全檢測報告簽署人不得同時擔任品質主管。
檢測能力	1. 第 1 型檢測實驗室： (1). 須具備 3 年內智慧型手機系統內建軟體資通安全檢測實際執行經驗，並提供執行之證明文件。 (2). 須具備下列檢測工具，並建置可與智慧型手機連線及檢測之操作環境： A. 於藍牙、WLAN 及行動通訊網路之無線傳輸環境下，可攔截、分析及修改網路傳輸封包之工具。 B. 可連線及操作智慧型手機作業系統（至少包含 Android 和 iOS 平臺）之指令作業工具。 C. 具掃描網路連接埠功能之工具。 D. 具檢測加密演算法強度之工具。 E. 具模擬藍牙與 WLAN 無線傳輸發射端和接收端功能之模糊測試（Fuzz Testing）工具。 F. 軟體開發工具（Software Design Kit）及軟體反組譯工具（至少包含 Android 和 iOS 平臺）。
檢測費用	1. 檢測費用依安全等級區分為初級、中級及高級之檢測費用。 2. 經檢測合格之智慧型手機，當作業系統版本或系統內建

修改項目	調整主要內容
	軟體版本更新時，應針對有變更之部分重新申請檢測。其檢測費用以全項檢測費用乘以重新檢測項目數占全部檢測項目數之比例計算；需重新檢測之項目，由受測者提供並由檢測實驗室認定之。 3. 檢測實驗室通知受測者檢測未符合規定時，應列舉不符合事項並通知受測者改善，通知改善方式及收費機制由檢測實驗室自訂。
實驗室申請書	1. 增加智慧型手持行動臺安全檢測實驗室申請書，檢測實驗室性質區分第 1 型與第 2 型，由申請單位依需求勾選申請。 2. 檢附文件包含：法人/機構之身分證明文件影本、本國實驗室認證組織之認證證明文件影本、向本國實驗室認證組織申請檢測實驗室認證時，所檢附相關資料之光碟片，以及其他經本會指定者。
實驗室認可證書	以三年為期

資料來源：本計畫彙整

(二)試辦期之檢測實驗室資格

手機檢測規定在國際並無國家強制規定，在台灣也規劃以電信業行政要求與軟性宣導引導業者自願檢測，因此規劃於政策正式推動前，先進行為期 4 個月的試辦期，規劃試辦期間為 105 年 6 月 1 日至 105 年 9 月 30 日；105 年 10 月 1 日起正式執行。

於試辦期內，檢測實驗室應向國家通訊傳播委員會提出認可申請，認可程序由國家通訊傳播委員會選任之專家執行之，而試辦期間資格要求另訂如下：

表16 智慧型手持式行動臺安全檢測實驗室(試辦期)資格重點摘錄

資格類別	資格要求
前言	1. 國家通訊傳播委員會（以下簡稱本會）為確保智慧型手機系統內建軟體資通安全品質，規劃於正式辦理智慧型手機系統內建軟體資通安全檢測實驗室（以下簡稱檢測實驗室）認可前，先行試辦檢測實驗室認可程序，特訂定本說明。 2. 自 105 年 6 月 1 日至 105 年 9 月 30 日為試辦期，本會保留變更之權利。 3. 本會認可試辦之檢測實驗室（以下簡稱試辦實驗室）分為第 1 型及第 2 型試辦實驗室，由申請擔任試辦實驗室者（以下簡稱申請人）依智慧型手機系統內建軟體資通安全檢測技術規範之檢測範圍申請之。
實驗室要求	1. 智慧型手持行動臺安全檢測實驗室申請書(試辦期)。 2. 依法設立之本國法人、機構之證明文件影本。
一般規定	1. 取得本國實驗室認證組織核發符合中華民國國家標準（以下簡稱 CNS）17025 或國際標準化組織所定標準（以下簡稱 ISO/IEC）17025 有關測試與校正實驗室能力一般要求規定之認證證明影本。 2. 申請人得以「智慧型手機系統內建軟體資通安全檢測服務計畫書」替代前項規定。前揭計畫書內容應載明申請人具備之實驗室管理程序，包括：檢測方法及流程、檢測設備及軟體工具、檢測結果品質管理程序等。 3. 試辦實驗室之基本成員至少應有 3 人，分別為技術主管、品質主管及報告簽署人。 4. 試辦實驗室技術主管與報告簽署人不得同時擔任品質主管。
專業規定	三年內曾經實際執行智慧型手機系統內建軟體資通安全檢測經驗之證明文件。

資格類別	資格要求
實驗室之成員要求	1. 至少有一人具資訊安全相關管理職經驗 2 年以上或從事資安測試評估實務工作達 2 年以上，並具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。 2. 至少有一人須取得道德駭客證照(Certified Ethical Hacker , CEH)或國際網路資安證照(CompTIA Security+)。 3. 至少有一人取得下列任一資安證照：資訊系統安全專家認證(Certified Information Systems Security Professional, CISSP)、資安軟體開發專家認證(Certified Secure Software Lifecycle Professional, CSSLP)、資安分析專家認證(EC-Council Certified Security Analyst, ECSA)、資安鑑識調查專家認證(EC-Council Computer Hacking Forensic Investigator, CHFI)、滲透測試專家認證 (GIAC Penetration Tester, GPEN)或行動裝置資安分析專家認證(GIAC Mobile Device Security Analyst, GMOB)、安全程式設計師證照(EC-Council Certified Secure Programmer, ECSP)、資安專業人員證照(Systems Security Certified Practitioner, SSCP)。 4. 非屬前款資安證照者，需經 NCC 認可。 5. 第 2 型檢測實驗室之成員，除須符合上述要求外，應至少有 1 人取得 CCRA 或本會認可檢測實驗室之 ISO/IEC 15408 測試評估專業訓練時數達 360 小時以上之證明文件影本。
合格效期	認可證書自核發之日起算六個月內有效，試辦實驗室得於本會正式辦理智慧型手機系統內建軟體資通安全檢測實驗室認可時，向本會申請認可。
證書	試辦實驗室於認可證書有效期間出具之智慧型手機系統內建軟體資通安全檢測報告（以下簡稱檢測報告），可由受測者提交向本會申請核發智慧型手機系統內建軟體資通安全審驗證明。

五、評估技術規範草案可行性

依據計畫規定時程，技術規範草案可行性評估程序時間為 104 年 12 月至 105 年 2 月間，在此期間進行手機測試與規範修訂程序，並依據期末審查提交之規範版本進一步確認可行性，故本章節(105 年 3 月)後又將規範中有疑慮之用字進行調整，因此可行性評估之規範測試版本為期末審查版本(詳見表 23)，故與本次期末報告審查後修訂版之規範內容略有差異，僅此說明。

(一)測試手機之選定

因市場手機廠牌眾多，為能適切瞭解我國人普遍使用之手機可能潛在之資安問題，乃針對作業系統及代表性廠牌市占率高者為優先考量。在手機作業系統方面，以 IDC 國際數據資訊提供之調查報告顯示 2011 年至 2014 年有關智慧型手機作業系統排名，因 Android、iOS 及 Windows 這三款作業系統即佔了整個市場的 98.8%，故測試上即考慮這三類作業系統之手機，IDC 調查報告結果如下表所示。

表17 2011~2014 年智慧型手機作業系統市占率變化

作業系統 / 時間	Android	iOS	Windows	其他
2014 年第 2 季	84.7%	11.7%	2.5%	1.2%
2013 年第 2 季	79.6%	13.0%	3.4%	4.0%
2012 年第 2 季	69.3%	16.6%	3.1%	11%
2011 年第 2 季	36.1%	18.3%	1.2%	44.4%

資料來源： Worldwide Smartphone OS Market Share(Q2 2011 - Q2 2014)(IDC 國際數據資訊, 2014 年)

而手機廠牌部分的考慮，以 Vpon 之市調顯示 2013 年至 2014 年之手機廠牌在台熱銷前 5 名有三星、蘋果、HTC、SONY 及華碩，，

Vpon 調查結果如下圖所示；iOS 系統之手機就以蘋果的近期新款手機，Windows 系統手機雖無擠進前 5 名但屬重要代表性作業系統，故其中 1 款待測樣機為微軟之智慧型手機；Andorid 系統手機則依據熱銷及代表性程度，故選擇 SAMSUNG、HTC、SONY 及小米之近期新款手機作為測試標的，其選定之受測樣機詳見表 18。

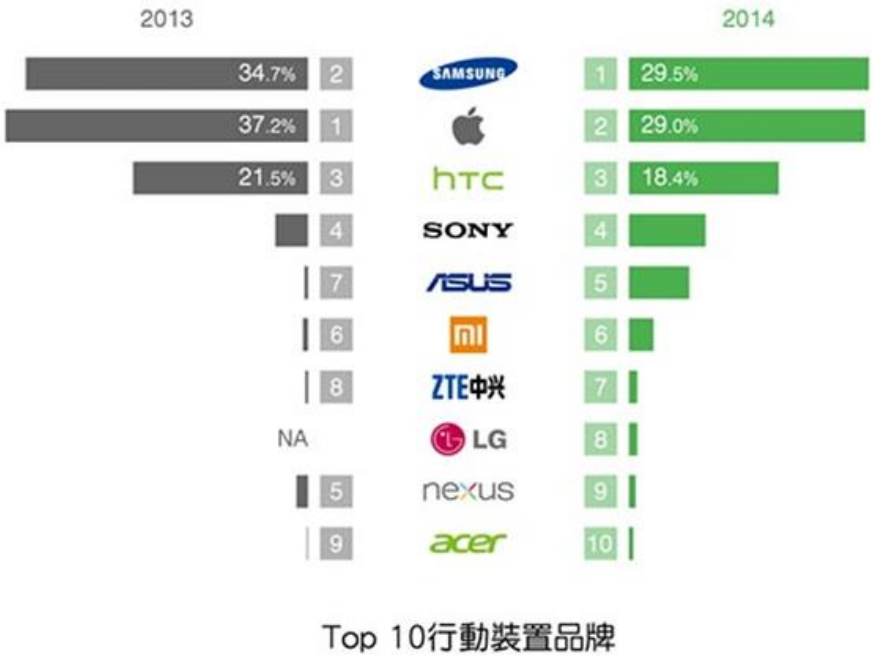


圖14　台灣智慧行動手機廠牌排名

資料來源：2014 年行動廣告市場年終報告(Vpon, 2014 年)

表18　專案測試標的

對應代號	廠牌	型號
MOBILE01	SAMSUNG(Galayx S6)	SM-G9250
MOBILE02	Microsoft	RM-1065
MOBILE03	APPLE(iPhone 6)	3A019TA/A
MOBILE04	HTC	Desire 728 dual sim
MOBILE05	SONY	Xperia Z3+

對應代號	廠牌	型號
MOBILE06	MI	Redmi Note 2

資料來源：本計畫彙整

(二)測試結果說明

1.測試範圍

自 12/1 起針對初版技術規範內容進行 6 支手機安全等級中級(M)之完整可行性測試，高級規範內容則因手機業者無法配合填寫相關書審內容，故未納入本次可行性評估範圍。

2.可行性測試評估結果

本規範相關檢測項目因涉及到不同的作業系統，包含 Android、iOS 及 Windows 這三大作業系統，不同作業系統之設計架構各異，實際測試作業上發現部分檢測項目因其系統原本之特性而無法確實執行測試，以及檢測條件、方法、判定標準等有疑慮之測項將其測項內容與屬性進行修改。

初版規範內容共規劃基本與進階 2 個安全等級，計有 41 個檢測項目，其中 Android 作業系統之手機，除部分測項需獲得手機管理者權限方可檢視判斷該測項是否通過檢測外，均可執行測試；iOS 系統與 Windows 系統因較為封閉，其中又以 Windows 之手機更甚，故初次檢測時共有 11 個測項因這兩個作業系統之特性而不適用無法進行檢測，而相關不適用之測項將於稍後說明。第一版規範之檢測項目於各作業系統適用性測試結果彙整詳見表 19。

表19 第一版規範之檢測結果系統比較

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
D.1 首次執行手機系統內建軟體時，於存取敏感性資料前須經過使用者同意。	D.1.1 手機系統內建軟體存取敏感性資料之提示機制	基礎	可	可	可	
D.2 手機系統應提供使用者拒絕內建軟體存取敏感性資料之權利。	D.2.1 手機系統內建軟體提供使用者拒絕存取敏感性資料之機制	基礎	可	不適用	不適用	納入選測項目
D.3 手機系統之內建軟體間，應提供敏感性資料分享之提示機制，避免未經許可的資料共享行為。	D.3.1 手機系統內建軟體間分享敏感性資料之提示機制	基礎	可	可	可	
D.4 手機系統內建軟體須將敏感性資料儲存於作業系統保護區域，並提供資料加密功能，避免遭不	D.4.1 手機系統內建軟體不應將敏感性資料儲存於暫存檔或記錄檔中	進階	可 (需 root)	可 (需 JB)	不適用	調整檢測項目，將暫存檔與記錄檔改為非作業

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
正當方式取得資料並得以解密回明文資料。						系統保護區內
	D.4.2 手機系統內建軟體儲存敏感性資料時應以密文方式儲存	進階	可 (需 root)	可 (需 JB)	不適用	納入選測項目
	D.4.3 手機系統內建軟體與遠端伺服器溝通之帳號密碼不應儲存於非作業系統保護區內	基礎	可	可	可	
	D.4.4 手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於程式碼中	進階	可 (需 root)	不適用	不適用	納入選測項目
D.5 手機系統內建軟體透過無線網路傳輸敏	D.5.1 手機系統內建軟體使用	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
感性資料時，應使用加密傳輸，以確保敏感性資料安全。	WLAN 傳輸敏感性資料					
	D.5.2 手機系統內建軟體使用行動通訊網路傳輸敏感性資料	基礎	可	可	可	
D.6 手機系統應提供使用者資料之遠端保護能力及相關安全設定，讓使用者可在遠端啟動保護功能，以保護手機系統內之資料。	D.6.1 使用者資料的遠端鎖定	基礎	可	可	可	
	D.6.2 使用者資料的遠端刪除	基礎	可	可	可	
D.7 手機系統應支援備份功能。 使用者資料的備份包括本機備份與遠端備份兩種：本機備份是通過手機的周邊介面進行資料備	D.7.1 使用者資料的本機備份	基礎	可	可	不適用	調整檢測項目，不區分遠端或本機備份型態
	D.7.2 使用者資料的遠端備份	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
份；遠端備份是通過 WLAN 或行動網路將使用者資料備份至遠端伺服器。						
A.1 手機系統內建軟體執行手機系統功能前，須經使用者同意。	A.1.1 手機系統內建軟體執行手機系統功能	進階	可 (需 root)	可 (需 JB)	不適用	調整檢測項目強調未經同意於背景執行系統功能，並納入選測項目
A.2 手機系統內建軟體在使用付費服務前，應提示並取得使用者同意後才能進行資源之使用。	A.2.1 付費服務的提示	基礎	可	可	可	
A.3 手機系統內建軟體在初次存取使用者帳戶時 ，應先行認證使用者	A.3.1 手機系統內建軟體使用者身分認證與授權機制	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
身分與其權限，以避免使用者帳戶遭到誤用或濫用。						
A.4 手機系統內建軟體須避免交談識別碼被重送攻擊。	A.4.1 手機系統內建軟體交談識別碼安全	進階	可	可	可	
A.5 手機系統內建軟體應確認伺服器憑證之有效性，以避免使用過期的憑證。	A.5.1 手機系統內建軟體伺服器憑證有效性	基礎	可	可	可	
A.6 手機系統內建軟體與伺服器間之資料加密傳輸，應使用安全之加密演算法。	A.6.1 手機系統內建軟體與伺服器加密演算法檢測	進階	可	可	可	
A.7 手機系統內建軟體應可識別其發行商與版本資訊，以確保使用者瞭解其來源。	A.7.1 來源識別	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
A.8 手機系統應提供使用者可查詢與關閉執行中之內建軟體。	A.8.1 手機系統內建軟體之關閉	基礎	可	可	可	
	A.8.2 手機系統內建軟體之背景執行關閉	基礎	可	不適用	不適用	納入選測項目
A.9 關閉手機系統內建軟體時，應停止該內建軟體所有相關程序。	A.9.1 手機系統內建軟體關閉之功能檢測	進階	可 (需 root)	可 (需 JB)	不適用	修改檢測方法並合併 A.9.2 納入選測項目
	A.9.2 手機系統內建軟體背景執行關閉之功能檢測	進階	可 (需 root)	可 (需 JB)	不適用	修改檢測方法並合併 A.9.1 並納入選測項目
A.10 手機系統內建軟體應具惡意字串的處理能力。	A.10.1 隱碼攻擊字串檢測	進階	可	可	可	
	A.10.2 延伸標記語言安全檢測	進階	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
A.11 手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路服務連接埠」相符。(搭配我宣告)	A.11.1 網路連接埠控管	進階	可	可(調整測試方式)	可(調整測試方式)	調整檢測方式
A.12 手機系統內建軟體應僅使用其所需之權限，且權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。	A.12.1 功能權限聲明之驗證	基礎	可	可	可	
P.1 手機與不同設備以有線周邊介面進行第一次連接時，應給予使用者相對應的提示機制。	P.1.1 有線周邊介面連接建立之提示機制	基礎	可	可	可	
P.2 對於具備無線介面的手	P.2.1 無線介面之開關	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
機，應提供使用者可進行開啟及關閉之功能介面。						
P.3 當手機的無線介面確認開啟時，應給予使用者相對應的提示狀態。	P.3.1 無線介面連線之提示狀態	基礎	可	可	可	
P.4 手機與不同設備以無線周邊介面進行第一次連接時，應給予使用者相對應的提示機制，且須經使用者同意後才可建立連線。	P.4.1 無線介面配對連線建立之提示機制	基礎	可	可	可	
P.5 手機系統內建軟體應具通訊協定內容的錯誤處理能力。	P.5.1 強健性測試	進階	可	可	可	
O.1 手機系統應支援待機時	O.1.1 手機開機及螢幕	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
設定保護機制，以保護個人資訊，避免遭未經授權的使用。	解鎖保護機制					
	O.1.2 手機之強制鎖定	基礎	可	可	可	
	O.1.3 手機密碼儲存之檢測	進階	可 (需 root)	可 (需 JB)	不適用	修改檢測條件
O.2 手機的作業系統更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。	O.2.1 作業系統更新來源	基礎	可	可	可	
O.3 手機的作業系統下載更新或安裝更新時應提供更新公告，並告知使用者安全風險之資訊。	O.3.1 作業系統更新公告	基礎	可	可	可	
O.4 當手機韌體更新方式為手動上傳方式，作業系統應檢	O.4.1 韌體保護機制	進階	可	不適用	不適用	建議刪除，現大多以網路更

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
查韌體簽章、完整性及可用性，以避免遭惡意修改之韌體更新至手機系統。						新系統而不以韌體更新，且iOS &WP皆不適用，故刪除
O.5 手機系統內建軟體應提供回報安全性問題之管道。	O.5.1 手機系統內建軟體問題回報	基礎	可	可	可	
O.6 手機的作業系統應具備位址空間配置隨機化功能，以避免程式與參考函式在記憶體中的位址為固定值。	O.6.1 位址空間配置隨機化	進階	可	可(廠商提供佐證資料)	可(廠商提供佐證資料)	調整檢測方法

資料來源：本計畫彙整

(1)不適用之檢測項目說明

於上述測試分析結果有 11 項被評斷為不適用，其詳細說明如下：

- 原技術要求 D.2 與原檢測項目 D.2.1 之測項

在 iOS 系統手機上僅 GPS 可設定關閉，而 Windows 系統之手機也僅部分內建軟體有提供可拒絕存取的功能，而在 Android 系統之手機雖然也有類似狀況，但因為 Android 系統之手機獲得管理者權限後就能下指令方式去查看其軟體存取之動態行為，故該測項會因作業系統不同而無法落實測試之執行。

- 原技術要求 D.4 與原檢測項目 D.4.1、D.4.2 之測項

  該測項因需檢視暫存檔或紀錄檔中是否有儲存敏感性資料，故需取得最高管理者權限才可檢視作業系統保護區之資料，而本次執行試測之樣機其中僅 Android 系統之手機有獲得管理者權限，且目前沒有任何關於 Windows 系統手機於管理者權限的操作方法，所以無法執行該檢測項目。

- 原技術要求 D.4 與原檢測項目 D.4.4 之測項

  該測項需考慮逆向工程之技術來檢視程式碼內是否有發現帳密是明文方式儲存，目前僅 Android 系統較為可行，而 iOS 與 Windows 系統之內建軟體均因技術尚無法克服而目前判斷為不適用。

- 原技術要求 D.7 與原檢測項目 D.7.1 之測項

  因該測項考慮本機之備份機制，但 Windows 系統之手機僅提供雲端備份機制，故該測項判斷為不適用。

- 原技術要求 A.1 與原檢測項目 A.1.1 之測項

  該測項需檢視通話紀錄與簡訊資料檔，但是同樣沒獲得管理者權限之手機則無法查詢，有技術上問題。

- 原技術要求 A.8 與原檢測項目 A.8.2 之測項

該測項需有介面供瀏覽正在執行中的應用軟體之功能，但在 iOS 與 Windows 系統之手機卻無提供此功能服務。

- 原技術要求 A.9 與原檢測項目 A.9.1 之測項

  該測項需透過系統指令的方式去查看所有執行之應用軟體，故需獲得最高管理者權限外，且 Windows 系統之手機尚無相關可查詢之指令資訊，亦無法判斷。

- 原技術要求 A.9 與原檢測項目 A.9.2 之測項

  iOS 與 Windows 系統均無提供瀏覽執行中程式的功能，故判斷為不適用。

- 原技術要求 O.1 與原檢測項目 O.1.3 之測項

  該測項需針對生物辨識螢幕所定功能之手機去判斷，但目前 Windows 系統之手機並不支援此功能。

- 原技術要求 O.4 與原檢測項目 O.4.1 之測項

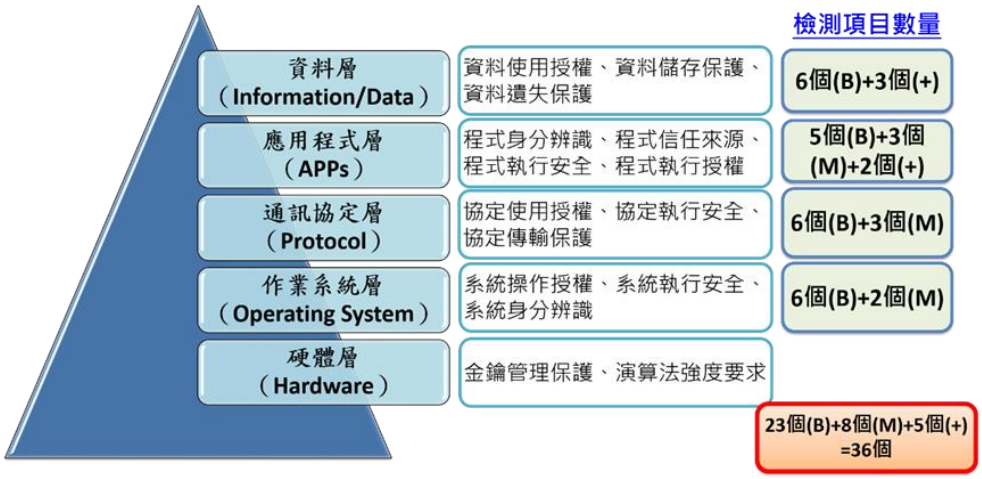
  目前 iOS 與 Windows 系統之手機並不支援手動更新韌體之功能，故判斷該項為不適用。

上述這 11 項測項，經判斷非均適用於 Android、iOS 及 Windows 之系統手機，故經建議可修改檢測條件、檢測方法或判定標準，以達可跨平台檢測之目標，但若因作業系統設計關係或條件與技術無法進行，則建議可將刪除測項或將其設計為選測項目，由送測單位自由選擇是否檢測，以確保本規範必檢測項目可滿足跨平台的要求，建議調整方式詳見表 19 之說明。

(2)修正規範檢測結果

經過規範調整後，安全等級調整為初級(B)、中級(M)及高級(H)，中級相關必測項目與選測項目共 31+5=36 個測項，其檢測層

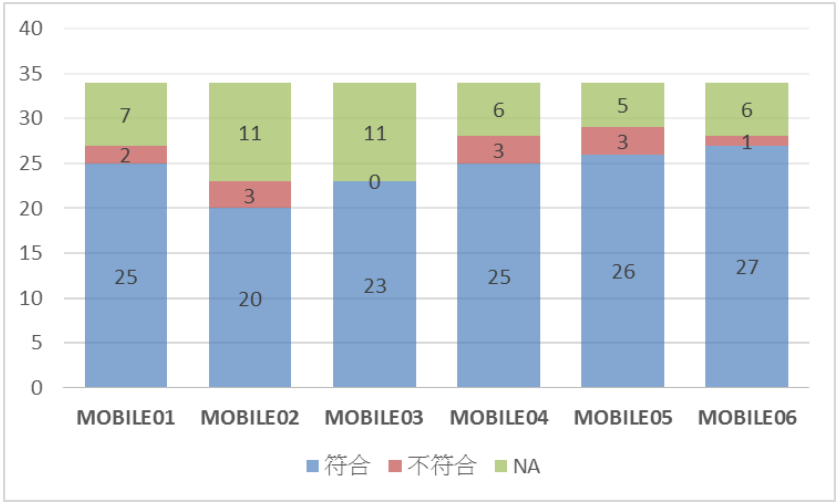
別與測項分佈詳見圖 15。



資料來源：本計畫彙整

圖15　檢測層別與測試項目

依本次 6 款測試樣機，包含 4 款 Android 系統手機及 iOS 與 Windows 系統手機各 1 款，針對修正更新後之 34 個測項，各詳細檢測細項結果說明請詳見附件 5。其中該測項之試測結果若符合檢測判定標準則標示為符合，若不符合判定標準則標示為不符合，若因特殊原故導致測試結果無法判斷或不適用則標示為 NA。各測試樣機於初、中級測項之試測結果之統計比較詳見圖 16：



資料來源：本計畫彙整

圖16 各手機試測結果統計比較

(3)檢測結果比較分析摘錄

針對各測試樣機之測試結果有不符合或 NA 之測項進行比較與分析如下。

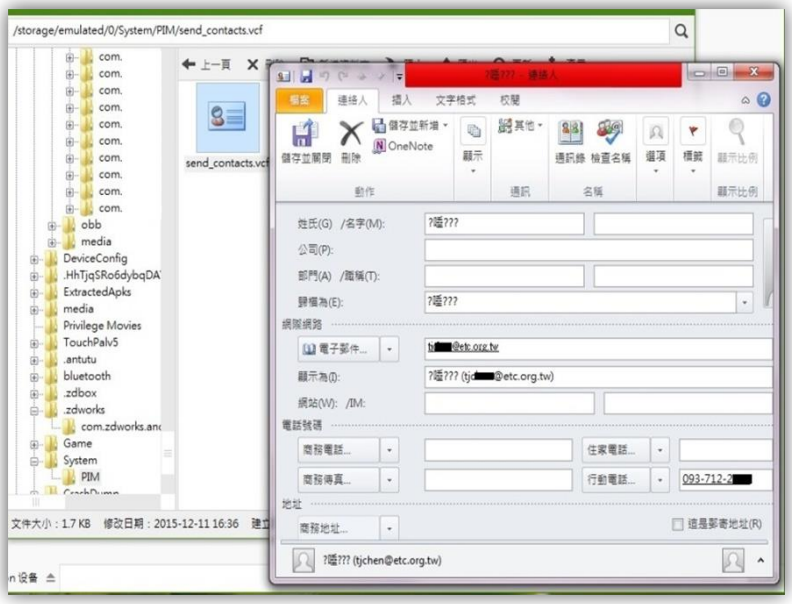
A.資料儲存保護之比較(檢測細項：D.2.1.B)

該測項之測試結果統計如表 20，在 6 款測試樣機中有 5 款手機符合測試要求，1 款不符合測試要求。

表20 測項 D.2.1.B 之試測結果

各手機之試測結果	
符合	5
不符合	1

該款手機乃因發現有敏感性資料以明文方式儲存於非作業系統保護區，故不符合檢測要求，詳見圖 17。



資料來源：本計畫彙整

圖17　敏感性資料以明文方式儲存於非作業系統保護區圖示

B.程式執行安全之比較(檢測細項 A.4.3.M)

在該測項之測試結果統計如表 21，6 款測試樣機均不符合測試要求。

表21　測項 A.2.1.B 之試測結果

各手機之試測結果	
符合	3
不符合	3

3 款不符合檢測要求之手機乃因發現可成功竄改封包內之圖檔連結，若置入之圖檔有植入木馬，則手機使用者將可能因點擊了具木馬圖檔而有資安之疑慮，故不符合該測項要求，詳細攻擊成功之畫面詳見圖 18。

資料來源：本計畫彙整

圖18　伺服器有效憑證過期圖示

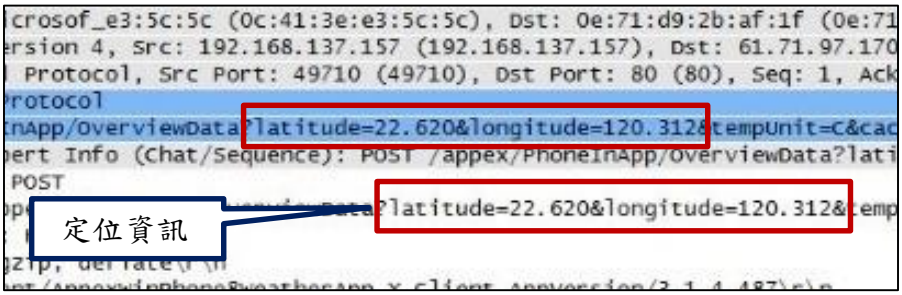
C.協定傳輸保護之敏感性資料加密傳輸保護比較(檢測細項：P.2.1.B)

在該測項之測試結果統計如表 22，6 款測試樣機中，有 5 款符合檢測要求，1 款不符合檢測要求。

表22　測項 P.2.1.B 之試測結果

各手機之試測結果	
符合	5
不符合	1

未通過測試之手機乃因發現定位資訊以明文方式傳輸，故不符合該測項之檢測要求，詳細結果請見圖 19。



資料來源：本計畫彙整

圖19　定位資訊明文傳輸圖示

上述為檢測結果比較分析摘錄，詳細之檢測結果比較分析請參閱附件 5。

(三)檢測技術規範修訂(期末審查版本)

期末報告審查所擬訂之完整版檢測細項如表 23，依據此版本內容

進行規範可行性評估，然而經期末審查後，依照委員建議，以及檢測結果判定，除了將各檢測項目以及規範說明用字統一調整，將用語更加精準外，並招開多場工作會議針對下列幾點內容修調規範為審查後修訂版之規範內容。

- 檢測細項 D.1.2.B 因分享行為亦屬使用者個人使用行為，因此不須再經過使用者同意機制鎖定使用者行為，故將此測項合併至 D.1.1.B。
- 檢測細項 P.1.1.B 因有線周邊傳輸亦屬使用者個人使用行為，不須額外提供提示機制，容易降低使用者警覺性，故刪除此測項。
- 清楚定義個人資料、敏感性資料、非作業系統保護區、本地服務、無線傳輸技術等，並酌修相關測項文字。

表23 檢測細項(期末審查版)

檢測編號	檢測項目	檢測細項
D.1	資料使用授權	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意並提供相關提示機制。
		D.1.2.B 手機系統內建軟體間應提供分享敏感性資料之提示機制，以避免未經許可的資料共享行為。
		D.1.3.M(+)手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。
D.2	資料儲存保護	D.2.1.B 手機系統內建軟體不應將敏感性資料儲存於非作業系統保護區內，以避免遭非經授權使用。
		D.2.2.M(+)手機系統內建軟體於儲存敏感性資料時提供資料加密功能，以避免遭不正當方式取得敏感性資料。
		D.2.3.M(+)手機系統內建軟體與遠端伺服器溝通之帳號

檢測編號	檢測項目	檢測細項
		密碼不應以明文方式存在於程式碼中，以避免遭不正當的方式存取。
D.3	資料遺失保護	D.3.1.B 手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，讓使用者可在遠端啟動鎖定。
		D.3.2.B 手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，讓使用者可在遠端移除資料。
		D.3.3.B 手機系統應提供資訊備份功能。
A.1	程式身分辨識	A.1.1.B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。
A.2	程式信任來源	A.2.1.B 手機系統內建軟體應使用有效之伺服器憑證，以避免使用過期的憑證。(A.2.1.B(+)適用無圖示軟體)
		A.2.2.B 手機系統內建軟體應可識別其發行商與版本資訊，以確保使用者瞭解其來源。
A.3	程式執行授權	A.3.1.B 手機系統內建軟體在使用付費服務前，應提示並取得使用者同意後才可執行。
		A.3.2.B 手機系統內建軟體應僅使用其所需之權限，且權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。
		A.3.3.M 手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路服務連接埠」相符。(A.3.3.M(+)適用無圖示軟體)
		A.3.4.M(+)手機系統內建軟體不應在未取得使用者同意之情況下，於背景執行手機系統功能。
		A.3.5.M(+)手機系統內建軟體於使用者設定關閉時，應

檢測編號	檢測項目	檢測細項
		停止該內建軟體所有相關程序。
A.4	程式執行安全	A.4.1.M 手機系統內建軟體應具隱碼攻擊字串的處理能力。
		A.4.2.M 手機系統內建軟體應具延伸標記語言攻擊字串的處理能力。
P.1	協定使用授權	P.1.1.B 手機與其他設備以有線周邊介面進行第一次連接時，應給予使用者相對應的提示機制。
		P.1.2.B 對於具備無線介面的手機，應提供使用者可進行開啟及關閉之功能介面。
		P.1.3.B 當手機之無線介面確認開啟時，應給予使用者相對應的提示狀態。
		P.1.4.B 手機與其他設備以無線周邊介面進行第一次連接時，應給予使用者相對應的提示機制，且須經使用者同意後才可建立連線。
P.2	協定傳輸保護	P.2.1.B 手機系統內建軟體透過 WLAN 傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。(P.2.1.B(+)適用無圖示軟體)
		P.2.2.B 手機系統內建軟體透過行動通訊網路傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。(P.2.2.B(+)適用無圖示軟體)
		P.2.3M 手機系統內建軟體應避免交談識別碼遭重送攻擊。
		P.2.4.M 手機系統內建軟體與伺服器間之資料加密傳輸，應使用安全之加密演算法。(P.2.4.M(+)適用無圖示軟體)
P.3	協定執行安全	P.3.1.M 手機系統內建軟體應具通訊協定內容的錯誤處理能力。。
	系統操	O.1.1.B 手機之作業系統更新來源應與「廠商自我宣告

檢測編號	檢測項目	檢測細項
O.1	作授權	表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。
		O.1.2.B 手機之作業系統於下載或安裝更新時應提供更新通知，並告知使用者安全風險之資訊。
O.2	系統身分辨識	O.2.1.B 手機系統應支援開機及螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。
		O.2.2.B 手機系統應支援密碼強制鎖定的保護機制，以保護個人資訊，避免遭未經授權的使用。
		O.2.3.B 手機之作業系統應提供至少 52 種密碼輸入值，包含英文大/小寫、數字及特殊符號等，且應支援 14 種以上之排列組合。
		O.2.4.M 手機系統之密碼儲存不應以圖片形式儲存於手機上，以避免遭未經授權的使用。
O.3	系統執行安全	O.3.1.B 手機系統內建軟體應提供回報安全性問題之管道。
		O.3.2.M 手機之作業系統應具位址空間配置隨機化功能，以避免程式與參考函式在記憶體中的位址為固定值。
		O.3.3.H 手機之作業系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。
		O.3.4.H 手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。
		O.3.5.H 手機之作業系統應具備驗證錯誤計數機制，當嘗試錯誤超過門檻值，應抹除受保護之資訊。
H.1	金鑰管理保護	H.1.1.H 手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀。應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。

檢測編號	檢測項目	檢測細項
		H.1.2.H 手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。
		H.1.3.H 金鑰不得以明文方式存放於非揮發性之記憶體、且不得用任何方式匯出或直接對外傳輸。
H.2	演算法強度要求	H.2.1.H 手機實作之加/解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發布之金鑰演算法標準。
		H.2.2.H 手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。
		H.2.3.H 金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。

資料來源：本計畫彙整

(四)檢測技術規範修訂(期後修調版本)

期末報告審查後經通傳會招開多場工作會議針對規範進一步修訂如下表為審查後修訂版之規範內容。

表24 檢測細項(期後修調版)

檢測編號	檢測項目	檢測細項
D.1	資料使用授權	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。
		D.1.2.M(+)手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。
D.2	資料儲存保護	D.2.1.B 手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。
		D.2.2.M(+)手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資

檢測編號	檢測項目	檢測細項
		料。
		D.2.3.M(+)手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。
D.3	資料遺失保護	D.3.1.B 手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。
		D.3.2.B 手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。
		D.3.3.B 手機系統應提供資料備份功能。
A.1	程式身分辨識	A.1.1.B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。
A.2	程式信任來源	A.2.1.B 手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。
		A.2.2.B 手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。
A.3	程式執行授權	A.3.1.B 手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。
		A.3.2.B 手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。
		A.3.3.M 手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路連接埠(本地服務)」相符。
		A.3.4.M(+)手機系統內建軟體不應在未取得使用者同意

檢測編號	檢測項目	檢測細項
		之情況下，於背景撥打電話或發送簡訊。
		A.3.5.M(+)手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。
A.4	程式執行安全	A.4.1.B 手機系統內建軟體應提供回報安全性問題之管道。
		A.4.2.M 手機系統內建軟體應具備隱碼攻擊字串的處理能力。
		A.4.3.M 手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。
P.1	協定使用授權	P.1.1.B 手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。
		P.1.2.B 當手機之無線傳輸技術功能確認開啟時，應給予使用者相對應的提示狀態。
		P.1.3.B 手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。
P.2	協定傳輸保護	P.2.1.B 手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。
		P.2.2M 手機系統內建軟體應避免交談識別碼遭重送攻擊。
		P.2.3.M 手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。
P.3	協定執行安全	P.3.1.M 手機系統應具備通訊協定內容的錯誤處理能力。
O.1	系統操作授權	O.1.1.B 手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。

檢測編號	檢測項目	檢測細項
		O.1.2.B 手機系統於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。
O.2	系統身分辨識	O.2.1.B 手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。
		O.2.2.B 手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。
		O.2.3.B 手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。
		O.2.4.M 手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。
O.3	系統執行安全	O.3.1.B 手機系統應提供回報安全性問題之管道。
		O.3.2.M 手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。
		O.3.3.H 手機系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。
		O.3.4.H 手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。
		O.3.5.H 手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。
H.1	金鑰管理保護	H.1.1.H 手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。
		H.1.2.H 手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。
		H.1.3.H 金鑰不得以明文方式存放於非揮發性之記憶體，且不得用任何方式匯出或直接對外傳輸。

檢測編號	檢測項目	檢測細項
H.2	演算法強度要求	H.2.1.H 手機實作之加密、解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發布之金鑰演算法標準。
		H.2.2.H 手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。
		H.2.3.H 金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。

(五)估計之檢測時間

檢測過程已記錄各檢測項目需要之檢測時間，包括測試之前置作業時間、測試一個 APP/一項功能時間，以及製作一個 APP/一項功能報告時間，統計單支手機於初級與中級之必測測項所需花費檢測時間，檢測初級所需花費時間平均為 32 個人天，中級不含選測項目則平均需花費 56 個人天，詳細必測檢測項目之檢測時間分析結果詳見表 25。

表25 檢測項目之檢測時間(必測項)

必測項			
初級檢測項目	測試時程下限	測試時程平均值	測試時程上限
測試時程(分鐘)	7,105	11,410	15,715
測試時程(小時)	119	191	262
測試時程(人天)	20	32	44
中級檢測測項(不含+)	測試時程下限	測試時程平均值	測試時程上限
測試時程(分鐘)	11,715	19,875	28,035

必測項			
測試時程(小時)	196	332	468
測試時程(人天)	33	56	78

資料來源：本計畫彙整

另外，亦記錄選測測項之檢測時間，中級之選測測項所需花費時間平均為 35 人天，無圖示之選測測項所需花費時間平均為 74 人天，詳細選測檢測項目之檢測時間分析結果詳見表 26。

表26　檢測項目之檢測時間(選測項)

選測項			
中級選測測項 M(+)	測試時程下限	測試時程平均值	測試時程上限
測試時程(分鐘)	6,575	12,338	18,100
測試時程(小時)	110	206	302
測試時程(人天)	19	35	51
無圖示之檢測測項	測試時程下限	測試時程平均值	測試時程上限
測試時程(分鐘)	19,575	26,363	33,150
測試時程(小時)	327	440	553
測試時程(人天)	55	74	93

資料來源：本計畫彙整

由於本規範檢測項目數量較多，所需花費檢測時間亦較長，為降低檢測時間，建議可請送測廠商提供多支手機進行檢測作業，初級檢測平均所需時間為 32 人天，若廠商一次檢送 2 支手機，即可縮短測試時間為 16 人天，若再加上檢測實驗室共有 4 人共同作業，則可縮短工時為 8 人天，應可於 1 週半內完成。為降低檢測時間，是以建議送測單位皆提供 2 支以上手機進行測試，詳細檢測工時平均估計表詳見表 27。

表27 檢測工時平均估計表

單位：工作天

等級	總測試時間	同時 2 支手機 總測試時間	同時 2 支手機與 4 人進行 檢測估計檢測時間
初級	32	16	8
中級	56	28	14
中級含(+)	91	46	23
中級含(+)及 無圖示測項	165	83	42

資料來源：本計畫彙整

(六)建議計費模式

依據上述試測時間與人天工時計算，茲將各測試層別與級別之檢測人天工時表列如表 28。

表28 測試層別與級別檢測時間

單位：人天

測試層級	初級	中級	中級(+)	高級
D(資料層)	32	56	91	-
A(應用程式層)				-
P(通訊協定層)	16	32	32	-
O(作業系統層)				15
H(硬體層)	-	-	-	30

考量 P(通訊協定層)與 O(作業系統層)，於各手機測試時皆須測試，並不會因為內建 APP 數量造成工時影響，因此建議各手機檢測時，費用上分別以基本費(含 P+O+行政文書處理等費用)與 APP 數量個別計費較為合理，建議檢測費用計算基準參考如表 29。

表29 檢測費用計算基準建議

測試層級	初級	中級	中級(+)	高級
D(資料層)	依據 APP 數量計費	依據 APP 數量計費，另加成 50%	依據 APP 數量計費，另加成 100%	-
A(應用程式層)				-
P(通訊協定層)	以基本費[註]L1 計費(含行政作業費用)	以基本費[註]L2 計費(含行政作業費用)	以基本費[註]L2 計費(含行政作業費用)	-
O(作業系統層)				建議依人天費用計費
H(硬體層)	-	-	-	

[註]基本費於同一規格系列產品時，僅收取一次性費用，內建 APP 部分則依據實際計算數量計費，建議單一 APP 費用比照工業局 APP 檢測費用 1 萬元/個。

六、辦理座談會

配合本計畫各項工作項目需要於期中前辦理 3 場座談會，應邀請政府機關 4 機關以上(至少包括行政院消費者保護處、行政院資通安全辦公室及經濟部附屬單位等)、經我國型式認證手機之廠商、通傳會電信設備驗證機構、資安設備檢測實驗室，及手機資安檢測/防護專家學者少 5 人以上參加，討論智慧型手機系統內建軟體資通安全檢測技術規範草案及檢測實驗室認可草案初稿架構，以使本計畫擬定之技術規範符合需求。

(一)第一次專家學者座談會

1.時　　間：104 年 08 月 18 日(星期二) 15:30~16:50

2.地　　點：臺大醫院國際會議中心 401 會議室(4 樓)

3.主　　席：計畫主持人喻維貞副秘書長

4.與談人員：

出席代表	單位	姓名
專家學者	財團法人資訊工業策進會	陳組長
	趨勢科技股份有限公司(全球核心技術部門)	蔡資深協理
	台灣威瑞特系統科技股份有限公司	鄭技術經理
政府機關	行政院資通安全辦公室	吳副主任(請假)
	行政院資訊處	洪高級分析師
	經濟部工業局	曾技正
	經濟部技術處新世代通訊技術推進辦公室	許資深技術經理
檢測實驗室代表	香港商立德國際商品試驗有限公司	蕭協理
	台灣檢驗科技股份有限公司	陳技術經理
	交大網路測試中心	許執行主任

5.報告事項

由研究團隊報告手機安全檢測國際發展現況分析與 NCC 手機系統內建規範解決方向，由各與會者及台下參與來賓針對與會討論議題一同討論。

6.會議決議

(1)安全等級規劃應以使用者角度為出發點，以使用者隱私相關的資料安全為主，確保所有資料在各狀態下可被安全使用。

(2)規範撰擬須與國際規範標準一致，將參考 OWASP Mobile Security Project、NIST 800-164.163 及 ITU-T YD 2407-2013.2408-2013。

(3)資料型別以是否屬於敏感性資料，以及是否為使用者輸入作為判定標準，將資料區分 4 種型態。

(4)自我宣告屬於本規範之書審重點，未來期望透過公開廠商自我宣告表及實驗室檢測結果，讓民眾可上網審視手機權限要求是否與廠商自行聲明相符與妥適性。

(5)詳細會議紀錄請參考附件 6-1。

(二)第二次專家學者座談會

1.時　　間：104 年 09 月 18 日(星期五) 14:00~17:00

2.地　　點：中華民國資訊軟體協會

3.主　　席：計畫主持人喻維貞副秘書長

4.與會人員：

出席代表	單位	姓名
政府機關	行政院資通安全辦公室(技術服務中心)	陳組長
	行政院消費者保護處	王消保官(請假)
	經濟部工業局	曾技正(請假)
	經濟部標準檢驗局	林科長
檢測實驗室代表	香港商立德國際商品試驗有限公司	蕭經理
	台灣檢驗科技股份有限公司	張經理
專家學者代表	台灣威瑞特系統科技股份有限公司	吳總經理
手機業者代表	台灣三星電子股份有限公司	洪總監
	台灣三星電子股份有限公司	高經理
	台灣三星電子股份有限公司	葉資深專員

出席代表	單位	姓名
	宏達國際電子股份有限公司	陳副總經理
	宏達國際電子股份有限公司	巫經理

5.報告事項

(1)由研究團隊進行「我國智慧型手機系統內建軟體資通安全檢測技術規範草案」說明，針對規範訂立之安全等級與檢測項目進行討論。

(2)由研究團隊進行「第三方檢測實驗室認可規定修訂草案」說明，針對檢測實驗室之資格要求進行討論。

6.會議決議

(1)規範分級應以使用者角度重新劃分與定義，並以一般民眾容易理解之論述重新定義。

(2)相關檢測技術規範與實驗室認可規定內容修正方向，將參考與會專家建議並提請本計畫主辦單位確認後調整於規範內容中。

7.詳細會議紀錄請參考附件 6-2。

(三)第三次專家學者座談會

1.時　　間：104 年 10 月 02 日(星期五) 14:00~18:00

2.地　　點：中華民國資訊軟體協會

3.主　　席：計畫主持人喻維貞副秘書長

4.與會人員：

出席代表	單位	姓名
政府機關	經濟部標準檢驗局	林科長
	國家發展委員會資管處	楊科長
	經濟部工業局	曾技正(請假)
	行政院資通安全辦公室(技術服務中心)	陳組長
檢測實驗室代表	香港商立德國際商品試驗有限公司	蕭經理
	台灣檢驗科技股份有限公司	陳技術經理
專家學者代表	台灣威瑞特系統科技股份有限公司	吳總經理
	台灣國際商業機器股份有限公司(IBM)	曾技術顧問
手機業者代表	宏達國際電子股份有限公司	巫經理

5.報告事項

(1)依據第二次座談會議決議修訂後內容，針對「我國智慧型手機系統內建軟體資通安全檢測技術規範草案」修改項目說明，並針對規範訂立之安全等級與檢測項目進行討論。

(2)依據第二次座談會議決議修訂後內容，針對「第三方檢測實驗室認可規定修訂草案」修改項目說明，並針對檢測實驗室

之資格要求進行討論。

6.會議決議

(1)安全等級請以消費者容易理解之說明再次調整，並明顯區隔等級之差異。

(2)檢測實驗室要點可用章節完全區分「資通設備安全檢測實驗室」與「智慧型手持行動臺安全檢測實驗室」。

(3)檢測實驗室資格要求建議研究團隊與 TAF、檢測實驗室及 NCC 共同討論。

(4)請依今日會議討論共識，進行規範與檢測實驗室資格之修調。

7.詳細會議紀錄請參考附件 6-3。

七、辦理說明會

為使業界了解智慧型手機系統內建軟體資安檢測技術規範草案內容、評估測試結果以及後續政策推動計畫，舉辦 2 場次說明會，邀約型式認證手機商、行動通訊業務經營者、手機內建軟體開發商、通傳會電信設備驗證機構、資安設備檢測實驗室、APPs 程式開發商等共計 68 位出席。

(一)會議相關資訊

表30 推廣說明會場次資訊

場次	參與人數	時間	地點
第一場	36	105 年 2 月 19 日 10:00~12:00	北科大集思會議中心 2 樓 205 室-瑞特廳

場次	參與人數	時間	地點
第二場	32	105 年 2 月 19 日 14:00~16:00	(台北市忠孝東路三段 193 巷旁<台北科技大學億光大樓>)
合計	68		

表31 說明會議程資訊

第一場 (上午)	第二場 (下午)	活動內容	主講人員
09:30 - 10:00	13:30 - 14:00	與會者報到	
10:00 - 10:10	14:00 - 14:10	主辦單位/協辦單位致詞	通傳會 吳銘仁簡任技正 中華軟協 喻維貞副秘書長
10:10 - 10:40	14:10 - 14:40	手機系統內建軟體資通安全檢測技術規範要點說明	計畫團隊 安華聯網公司 洪光鈞 總經理
10:40 - 11:00	14:40 - 15:00	手機系統內建軟體資通安全試測結果說明	計畫團隊 電子檢驗中心 葉錫勳 組長
11:00 - 11:15	15:00 - 15:15	休息時間	
11:15 - 11:30	15:15 - 15:30	手機系統內建軟體資通安全檢測制度說明	計畫團隊 中華軟協 楊蕙如 組長
11:30 - 12:00	15:30 - 16:00	意見交流	
12:00	16:00	會議結束	

資料來源：本計畫彙整

圖20 說明會現況

(二)意見交流討論與回覆

針對 2 場說明會上與會人員共同提出之議題彙整如下，詳細會議紀錄詳見附件 9。

序	討論議題	回覆
1	檢測天數 60 人天，對於手機商而言有些過長，可否再請壓縮檢測時間？	目前 60 人天是一支手機與一個檢測人員所計算之工作天，若有時程上要求，建議手機業者送測時提供多支手機以利檢測實驗室多工同步測試，以利縮短天數。
2	聽說初級是強制性，那現在最終的規劃會是強制性嗎？	通傳會委託中華軟協訂立技術規範草案，後續將先推動試辦期，希望手機商與檢測實驗室可以於此試辦期調整時程安排，因此目前此規範推動先以廠商自願性檢測為主，將來會看整個市場發展情況決定是否要強制規定。
3	APPs 開發時會分架上版與內建版，然而內建 APPs 可以透過 STORE 進行更新，而更新後的版本可能會出現問題，那更新後產生的問	若開機有連網行為後立即更新 APPs，則此更新版本為檢測的第一版本，若 APPs 連網後未有更新，則以送測版本進行檢測。若是使用一段時間後才於 APPs store 更新者，則屬於工業局 APP 規範

序	討論議題	回覆
	題與工業局的規範是否有共同的管控機制？而版本更新該如何管控？	之範疇。若手機於取得標章後仍有內建軟體之更新，應由送測單位提供手機依據更新部分內容進行檢測，通傳會也會規劃以抽測方式管理已核發之標章是否皆符合規定。
4	是否有計畫多久之後會更新技術規範，進而推動強制性要求？	該技術規範參考多國之規範內容進行擬定，因此通傳會希望先由電信業者綁約手機須經資安檢測作為第一步，手機業者則為自願性檢測，規範後續之更新規劃，將端看國際潮流以及國內運作狀況而定。
5	上市後的版本更新之送測該如何進行？	若手機於取得標章後仍有內建軟體之更新，應由送測單位提供手機依據更新部分內容進行檢測，通傳會也會規劃以抽測方式管理已核發之標章是否皆符合規定。

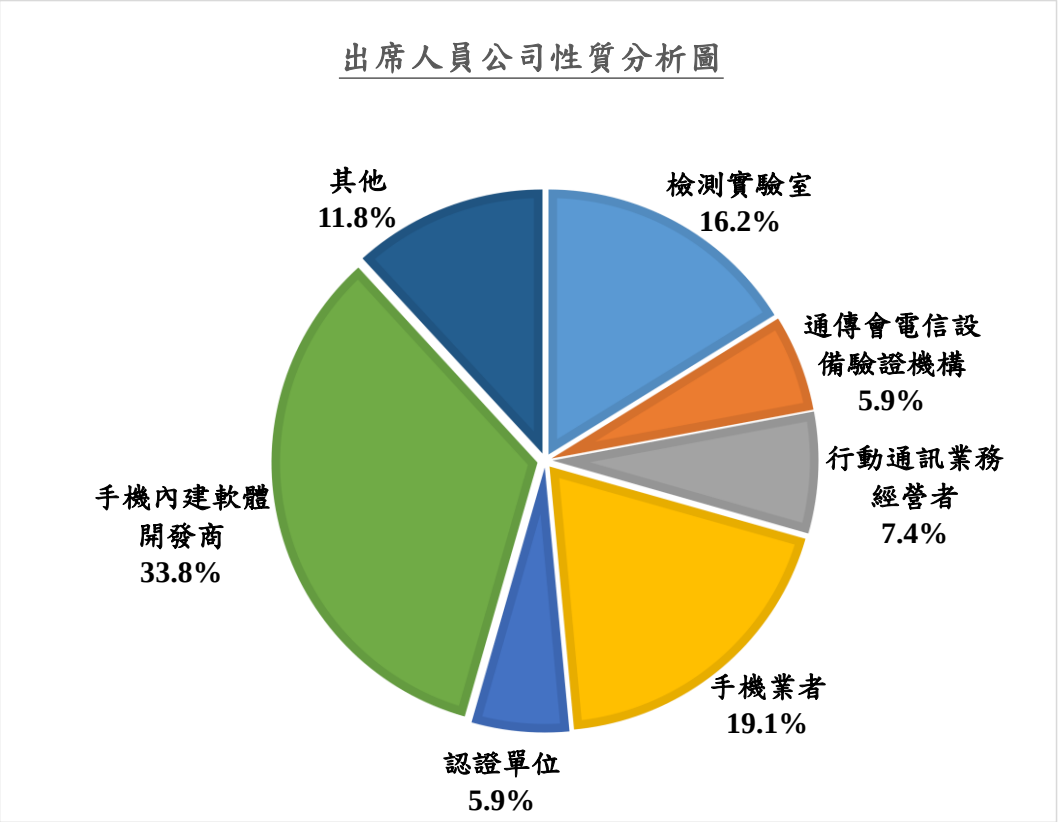
(三)問卷調查

本計畫於推廣說明會進行性別與公司型態相關資料進行統計，2 場共報名 104 人，共 68 位出席，出席率達 68%，其中手機內建軟體開發商佔 33.8%最多，其次為手機業者佔 19.1%，第三為檢測實驗室佔 16.2%，性別方面則以男性居多，佔比 89.7%。檢測規範制度需要通訊商以及手機商協助配合，台灣大哥大、遠傳電信、中華電信、三星電子、宏達電子、蘋果電子及索尼行動通訊等業者皆出席參與，詳細出席名單詳見附件 7。

表32　出席人員公司性質與性別統計分析表

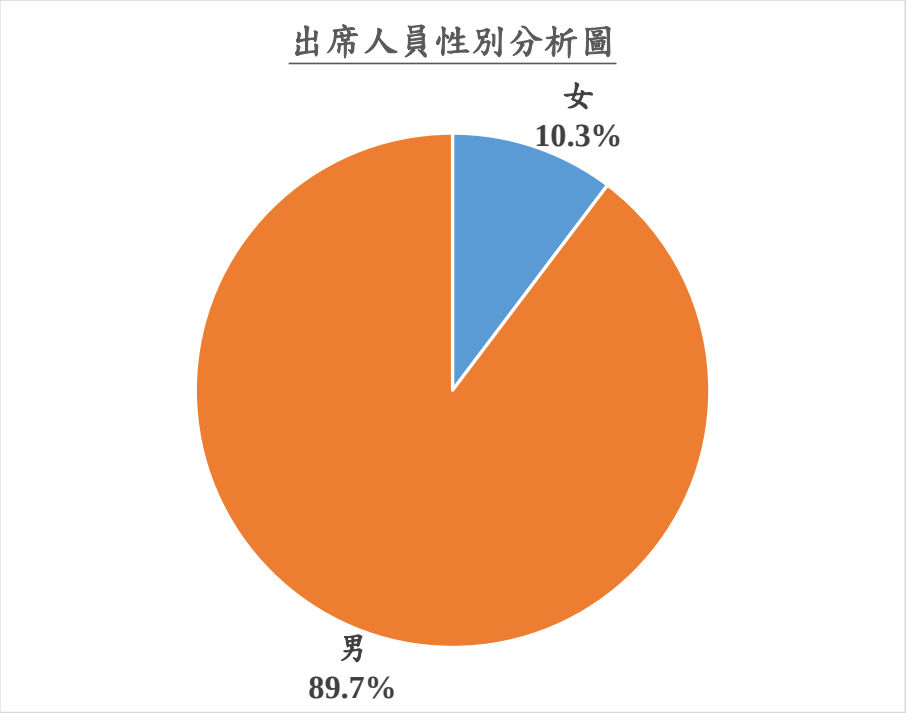
	性別			
公司性質	**女性**	**男性**	**總計**	**佔比**
檢測實驗室		11	11	16.2%
通傳會電信設備驗證機構	1	3	4	5.9%
行動通訊業務經營者	1	4	5	7.4%
手機業者	2	11	13	19.1%
認證單位	1	3	4	5.9%
手機內建軟體開發商	1	22	23	33.8%
其他	1	7	8	11.8%
總計	**7**	**61**	**68**	**100%**

資料來源：本計畫彙整



資料來源：本計畫彙整

圖21　出席人員公司性質分析圖



資料來源：本計畫彙整

圖22　出席人員性別分析圖

為了解手機業者、檢測實驗室以及相關業者對於檢測規範認同度以、檢測時間期望，以及檢測制度建議，於說明會後發放問卷調查予各與會者，共發出 68 份問卷，回收 45 份，回收率達 66.2%，以下將針對填答人員基本資料面、政策面、申請意願以及檢測時間認知面進行分析，問卷內容如圖 23。

國家通訊傳播委員會
NATIONAL COMMUNICATIONS COMMISSION

104 年手機系統內建軟體資安檢測計畫

手機系統內建軟體資安檢測技術規範推廣說明會

問卷調查表

感謝您撥冗出席本次說明會，請您撥冗填答本問卷，將您對本次說明會內容的建議與想法讓我們知道，您的寶貴意見將會是本計畫改善之目標，為本國手機系統內建軟體資安檢測技術規範制訂更加符合國內需求，感謝您。

性別	□男 □女	**學歷**	□高中職以下 □大學 □碩士 □博士以上
年齡	□25 歲以下 □25-35 歲 □35-45 歲 □45 歲以上		
產業	□手機商 □電信商 □檢測實驗室 □資訊業者 □資安業者 □學者 □其他_____		
公司型態	□型式認證手機廠商 □行動通信業務經營者 □手機內建軟體開發商 □通傳會電信設備驗證機構 □資安設備檢測實驗室 □APP 程式開發 □其他_____		
職類	□管理人員 □工程人員 □研發人員 □行政人員 □其他_____		

內容說明：請依照下方問項給予評分（單選，請打勾，並請填寫原因）

一、技術規範

1. 該技術規範是否符合與國際接軌？

□符合 □尚可 □不符合(原因：　　)

2. 該技術規範之檢測內容是否涵蓋完整？

□完整 □尚可 □不完整(原因：　　)

3. 該技術規範之判定標準是否清楚明瞭？

□清楚 □尚可 □不清楚(原因：　　)

4. 若要申請檢測，將有意申請之安全等級為何？(請手機商/通訊商填寫)

□普級 □中級 □高級

□無檢測意願(原因：　　)

5. 若要申請檢測，您認為檢測時間為多久最為適宜？

普級：□3 週 □1 個月 □1.5 個月 □2 個月

中級：□1 個月 □1.5 個月 □2 個月 □2.5 個月

高級：□1.5 個月 □2 個月 □2.5 個月 □3 個月

請翻至背面填答，感謝您！

國家通訊傳播委員會
NATIONAL COMMUNICATIONS COMMISSION

104 年手機系統內建軟體資安檢測計畫

6. 檢測時間超過多久則為手機商/通訊商無法接受？(請手機商/通訊商填寫)

普級：□1 個月 □1.5 個月 □2 個月以上

中級：□1.5 個月 □2 個月 □2.5 個月以上

高級：□2 個月 □2.5 個月 □3 個月以上

7. 您認為本技術規範是否應列為強制檢測？

□依國家政策訂定 □應列為強制檢測(原因：)

□不應列為強制檢測(原因：)

8. 您認為檢測實驗室申請要點符合目前市場需求(請檢測實驗室填寫)

□符合 □不符合(原因：)

9. 是否有意願申請為手機系統內建軟體之檢測實驗室?(請檢測實驗室填寫)

□有意願(□第 1 型檢測實驗室 □第 2 型檢測實驗室)

□須公司內部進行討論，但個人認為有意願

□須公司內部進行討論，但個人認為無意願(原因：)

□無意願(原因：)

10. 對於規範內容/檢測實驗室申請要點/制度實施，您有何其他建議?

檢測細項編號	建議
檢測實驗室/制度	

感謝您抽空填答，別忘記檢查是否有遺漏之處喔!

圖23 問卷內容

1.基本資料面

主要針對與會者的產業類別進行分析，填答問卷者有 26.7%為手機業者居多，並且多以工程人員及研發人員為主，其次為檢測實驗室則佔 22.2%，多以管理人員與工程人員居多。

表33 與會人員產業與職位類別分析表

	職稱類別						
公司型態	1.管理人員	2.工程人員	3.研發人員	4.行政人員	5.其他	**產業總計**	**公司型態佔比**
1.手機業者	1	9	2			12	**26.7%**
2.行動通訊業務經營者	1	2	1			4	**8.9%**
3.手機內建軟體開發商			4	1		5	**11.1%**
4.通傳會電信設備驗證機構	2	1				3	**6.7%**
5.檢測實驗室	2	2	3		1	8	**17.8%**
6.APP程式開發商	1	1	3		1	6	**13.3%**
7.其他	2	2	2		1	7	**15.6%**
職位類別總計	**9**	**17**	**15**	**1**	**3**	**45**	**100.0%**
職位類別佔比	**20.0%**	**37.8%**	**33.3%**	**2.2%**	**6.7%**	**100.0%**	

資料來源：本計畫彙整

2.政策面

主要了解與會人員對於智慧型手機檢測政策是否應強制性進行調查，42.2%的人認為依照國內政策決定，而認為應強制性要求以及自願性要求者人數比例相當，認為應強制要求者多半認為自願性檢測意願低，以及初級等級應列為強制要求，中級與高級則可自願性檢測，然而認為應以自願性檢測為主多半認為國際上並無強行要求，以及擔心產品生命週期短暫，強制要求會影響手機上市時間。

表34 政策是否強制性調查分析表

	是否強制性				
產業型態	**依政策決定**	**2.強制性**	**3.自願性**	**未填**	**總計**
1.手機業者	5	2	5		12
2.電信業者		1	2		3
3.檢測實驗室	3	4	3		10
4.資訊業者	5	2	2		9
5.資安業者	3	2		1	6
6.學者	1		1		2
7.其他(TAF.顧問公司.工作室)	2	1			3
總計	**19**	**12**	**13**	**1**	**45**
佔比	**42.2%**	**26.7%**	**28.9%**	**2.2%**	**100.0%**

資料來源：本計畫彙整

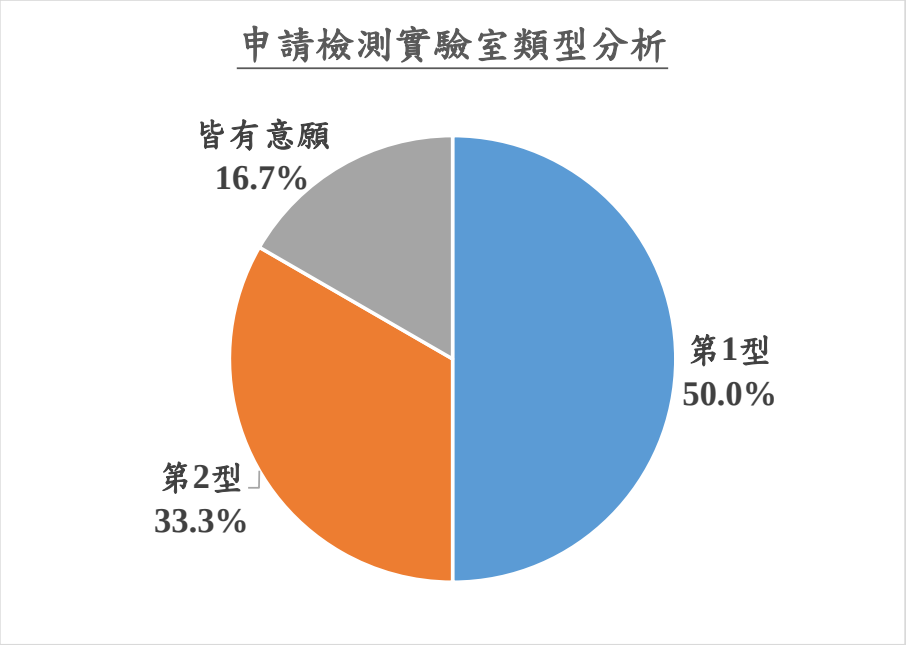
3.申請意願

對於檢測實驗室，細分電信設備驗證機構實驗室以及資安設備檢測實驗室，並納入其他有意加入之廠商進一步了解申請智慧型手機檢測實驗室之意願，調查結果可知有 24%有意願申請，而以申請為第 1 型檢測實驗室居多，另也有 28%認為公司須內部討論，但認為該制度有商機，公司會有意願申請。

表35 與會者申請檢測實驗室意願調查分析表

公司型態	通傳會電信設備驗證機構	檢測實驗室	APP程式開發商	其他	**總計**	**佔比**
0.未填寫		1			**1**	**4.0%**
1.有意願	2	4			**6**	**24.0%**
2.公司討論,但認為有意願	1	1	1	4	**7**	**28.0%**
3.公司討論,但認為無意願		2			**2**	**8.0%**
NA.免填			5	4	**9**	**36.0%**
總計	**3**	**8**	**6**	**8**	**25**	

資料來源：本計畫彙整

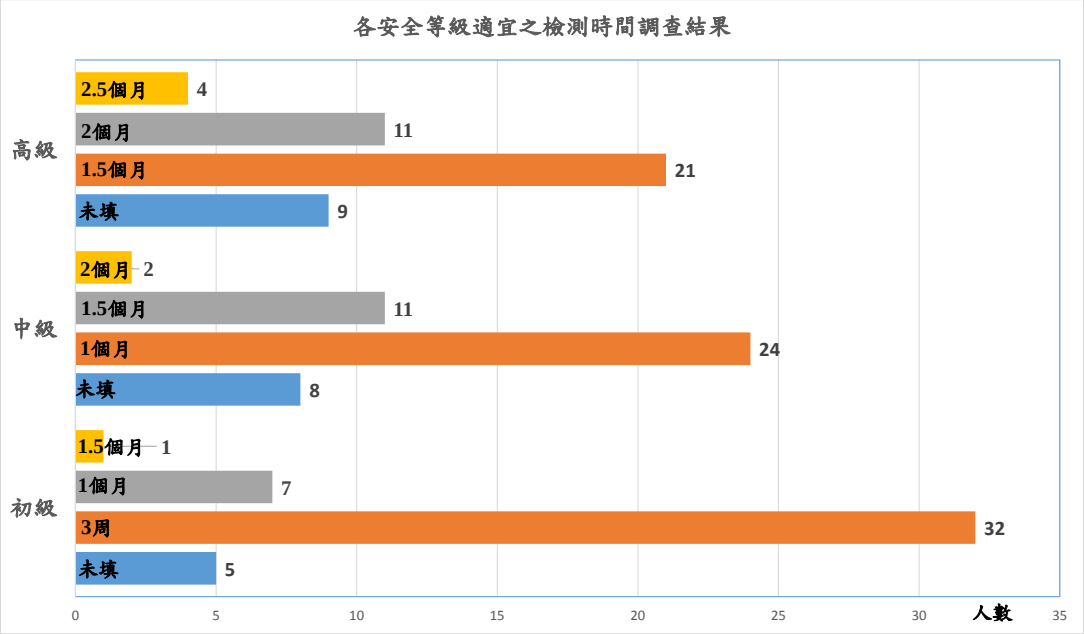


資料來源：本計畫彙整

圖24　申請檢測實驗室類型分析圖

4.檢測時間認知調查

於初級的檢測時間，71.1%(32 位)的人認為應於 3 週內完成；於中級的檢測時間上，53.3%(24 位)的人認為應於 1 個月內完成；而高級的檢測時間上，46.7%(21 位)的人認為應於 1.5 個月內完成。而本技術規範於中級檢測評估結果，估計一支手機檢測需 60 人天即可完成，申請時若送測單位提供 2 支手機進行送測，則可縮短至 30 人天，若廠商提供多支手機，檢測實驗室測試人員 4 位以上，則可大幅降低檢測時間，可符合外界期待。



資料來源：本計畫彙整

圖25　各安全等級適宜之檢測時間調查結果

八、智慧型手機之安全宣導資料

智慧型手機宣導資料主要讓民眾了解資安重要性，以及使用智慧型手機該注意之事項，段落撰寫主要以手機存在風險進行簡易分析，並將使用手機可能遇到的攻擊媒介進行分類，以近年重大手機安全事件輔助說明，以利民眾了解手機安全嚴重性，並提供民眾正確使用手機觀念，最後提出國內外相關手機使用之參考指引，由淺入深方式循序漸進讓民眾得以完整吸收。完整的宣導資料詳見附件 8。

(一)手機使用習慣之潛在風險：手機中毒徵兆

在台灣智慧型手機已成為人們生活必需品，然而在享受行動裝置便利有趣的同時，民眾於手機資安防護意識卻非常薄弱，防毒大廠卡巴斯基的實驗室研究發現，Android 木馬病毒可透過藍牙或 Wifi 快速傳播，不僅回傳手機的相關資訊，更會自動傳送簡訊至手機所有聯絡人，然而這類型病毒卻是看不到、刪不掉，因此許多民眾手

機中毒卻渾然不知。

其實手機中毒仍有跡可循，當手機出現下列幾點徵兆，民眾便可懷疑手機是否感染病毒，盡快尋求專業援助，降低受害可能性。

- 使用效能無故變差
- 電池壽命突然變短
- 莫名其妙通話中斷
- 電信費用突然暴增
- 出現自動下載軟體

(二)手機資安事件與犯罪手法：常見手機詐騙手法

手機的方便性已與民眾的生活密不可分，行動網路已成為人人生活中的必需品，手機快速上網更是多數民眾嚮往，傳輸速度快，各裝置間同步連結、資料傳輸方便，但卻衍生更多個人資料安全問題。

對於有心人士而言，竊取資料盜賣是門穩賺不賠的生意，資料量越大獲取價金越高，因此在現代人手一機的社會中，手機犯罪手法不斷推陳出新，目的便是為了竊取個人資料，多變的手機犯罪手法，不外乎可區分為三種媒介：連結網址、APPs 及 Wifi 連線，在此提供三種媒介常見的攻擊手法，提醒使用者注意。

表36 常見攻擊手法彙整表

攻擊媒介與方法	攻擊管道	結果
連結網址 含有惡意程式或網站的連結被點選 1. 社交工程	● 透過簡訊、通訊軟體(Line 或 what's APP 等)誘發使用者點選惡意連結 ● 民眾上網點選惡意連	● 小額付費 ● 下載惡意程式 ● 自動加密手機內資料要求付費解密

攻擊媒介與方法	攻擊管道	結果
2. 釣魚網站 3. 勒索軟體	結	
APPs 含有惡意程式之 APPs 直接或間接被下載	從未知來源下載 APPs	● 自動傳送惡意簡訊給朋友造成小額付費或使朋友遭受詐騙 ● 竊取手機內個人資料造成資料外洩
Wi-Fi 偽裝正常免費 Wi-Fi 吸引民眾連結	透過免費提供的誘因吸引民眾連結惡意 Wi-Fi	● 竊取姓名、密碼 ● 獲得手機控制權

資料來源：本計畫彙整

綜合上述的攻擊媒介，其實不外乎可區分為三種詐騙型態：結合社群網站與社交工程進行手機簡訊詐騙、網路釣魚惡意連結。

1.結合社群網站與社交工程進行手機簡訊詐騙

手機簡訊認證碼小額付款詐騙事件，不僅是最傳統的簡訊詐騙外，過往的 MSN(現在改為 Skype)等即時通訊、許多社群網站(如 Facebook)，以及通訊 APP 軟體(如 Line、What's APP 等)皆常出現此類型詐騙手法，駭客假冒手機使用者的親朋好友的方式要求使用者點選具吸引力的連結(例如投票網站、影片等)，進而造成社交攻擊事件，手機無意間遭受木馬程式攻擊，或是騙取手機簡訊認證碼，進行網路小額扣款付費的交易行為，輕則損失幾千元，重則被當成拍賣網站的人頭帳戶。

2.網路釣魚惡意連結

現今的手機功能已等同一般電腦，該有的功能幾乎都有，然而因使用者介面關係，手機瀏覽器所提供的資訊卻無法像電腦一樣能完整呈現，例如顯示 SSL 資訊的功能常因手機螢幕大小現

制而難以完整呈現，許多網站該跳出警示訊息要求使用者進行驗證時，手機版網頁為求畫面簡約性通常會跳過此步驟，行動版瀏覽器所提供的資訊往往不足以讓使用者判斷該網站是否有潛在的危險。

3.勒索軟體綁架手機重要資料

大部分的勒索軟體是透過釣魚網站入侵，大多經由特定的網址來散布，內容不外乎使用引起好奇心之字眼，引導使用者點選網址或免費廣告(內含惡意連結)。勒索軟體顧名思義屬於勒索行為，當使用者受到勒索軟體攻擊，該軟體會自動加密鎖住手機或儲存資料，並要求使用者特定期間內支付相當費用，否則將永遠無法使用手機或資料。

4.偽冒惡意 APPs 軟體下載

手機 APPs 商店裡有琳瑯滿目的免費 APPs 供民眾下載，然而這之中包含許多含有惡意程式的 APPs，魚目混珠難以分辨。當使用者不知 APPs 的真實性，下載到含有惡意程式的 APPs 時，最容易造成下列二種情況，讓使用者難以察覺。

(1)直接或間接幫使用者安裝廣告或不想安裝的 APPs。

(2)隱身在正常的 APPs 中。

(三)正確使用手機小撇步

網路上的詐騙方式很多種，所有的詐騙方法不外乎皆是運用民眾好奇心與求一時的方便心態進行攻擊，以下提供幾個正確使用手機的小撇步，避免手機對話紀錄、照片、密碼等隱私資料外洩，以保障個人隱私。

- 僅從信賴的來源下載 APPs

- 下載 APPs 前必須停看聽
- 要了解每支 APP 要取得哪些權限
- 檢查定位設定
- 點選網址請三思
- 別把個資用通訊軟體傳出去
- 即時更新作業系統
- 避免資訊自動儲存
- 當心免費無線上網熱點
- 手機使用複雜密碼與設定遠端可刪除資料

(四)正確使用手機方式與注意事項-手機操作十大步驟

美國聯邦通信委員會對於智慧型手機之使用，分別針對 Android 及 iOS 及 Windows phone 作業系統，擬定安全操作的十大步驟，摘述如後：

1.設定手機的個人識別碼及通行碼(Set PINs and passwords.)

2.請不要修改你的智慧型手機的安全設定(Do not modify your smartphone’s security settings.)

3.請備份並保護你的資料(Backup and secure your data.)

4.僅從信任之來源安裝 apps(Only install apps from trusted sources.)

5.請在安裝 APPs 前確認並明瞭軟體所要求的授權(Understand app permissions before accepting them.)

6.請安裝或啟用允許遠端定位及刪除資料之安全程式(Install security apps that enable remote location and wiping.)

7.請更新系統或軟體之更新程式(Accept updates and patches to your smartphone’s software.)

8.請謹慎使用開放的無線網路(Be smart on open Wi-Fi networks.)

9.請在捐贈、轉售或回收你的舊智慧型手機之前，應將資料刪除(Wipe data on your old phone before you donate, resell, or recycle it.)

10.向警察機關或電信公司回報遭竊之手機(Report a stolen smartphone.)

(五)參考指引要求之使用者防護安全

多數國家均在協助使用者的立場，藉由正確的設定智慧型行動裝置之相關安全機制，達到初期對於智慧型行動裝置基本使用安全之保護，因此本計畫歸納前述所有關於保護使用者資料安全之相關指引，將其彙整如下列 10 項使用者指引，以期防範資訊安全問題於未然。

表37 使用者指引參考表

項次	項目	說明
1	設定 PIN 碼、行動裝置密碼與多重身分驗證機制(例如:指紋辨識)。	避免行動裝置因送修或失竊而遭到未授權的存取內部資訊。
2	定期檢查並安裝原廠提供之更新與修補程式。	藉由原廠提供的修補機制，提升行動裝置安全性。
3	不移除行動裝置預設的安全機制。	不應對行動裝置進行”破解”、”越獄”或”取得 root 權限”，卸除行動裝置預設安全機制。

項次	項目	說明
4	僅從受信任的來源安裝應用程式。	避免安裝來源不明的程式造成安全威脅，應從正式的官方管道取得 Apps。如：Apple APP Store, BlackBerry World or Google Play。
5	不使用之行動裝置應刪除所有儲存之資料並恢復出廠預設值。	當不使用的行動裝置要移轉他人使用、廢棄、捐贈、轉賣、送修前，應刪除所有行動裝置上之資料，並恢復出廠預設值。
6	應透過建立信任安全的連線與機制傳送機敏資料。	使用點對點的安全通道(例如:SSL/TLS/ HTTPS)與金鑰加密機制，對欲傳送之機敏資料(如：網路銀行之帳號、密碼)加以保護。
7	所有介面在不使用的狀況下應關閉，並避免建立不信任連線。	防止不經意的狀況下，在公共場合主動連線或被不明連線。例如：藍牙的探索模式應於使用後立即關閉，並盡可能避免使用。以及不連線到公共場合中不明的無線基地台(或無線熱點)。
8	特別留意軟體蒐集使用者資料之要求。	在行動裝置軟體提示並要求時，應注意盡可能避免不必要之資訊之上傳。例如：不任意依據軟體指示上傳通訊錄資訊。
9	不任意相信並點選可疑的郵件或簡訊所提供之連結位址。	對不明簡訊內容應提高警覺，以防範簡訊詐騙與避免遭受安裝惡意程式之威脅。
10	對於任何應用程式執行過程所產生的錯誤代碼應加以求證。	那有可能是惡意程式欲繞過系統防禦機制所導致，應對不明訊息代碼向原始供應商進一步求證。

資料來源：本計畫彙整

九、本案與性別相關之統計及分析

2014/11/25 由傳立媒體與 Yahoo 奇摩共同發表「跨螢行為 vs.品牌溝通」研究報告中預估 2018 年，台灣將會有 1500 萬台數位裝置，且以大螢幕手機最受到青睞。無獨有偶，國內最大會員資料庫鼎鼎聯合行銷之「GO survey 市調網」亦於 2014/8 月之調查發現，智慧型手機普及率高達 89.6%，較去年同期調查結果高出 6.7%，其中以「20～30 歲」比例最高(94.3%)，「男性」(92.1%)智慧型手機普及率也稍高於女性(86.7%)。

調查中亦發現，民眾使用智慧型手機直接「收、發」電子郵件的比例也高達 8 成以上，是行動辦公室概念的體現，其中以女性的比例較高(87.3%)，男性則多透過網路進行「資訊查詢」。更有 38.6%的人天天使用，使用主要目的則是使用智慧型手機進行「社群」互動，包括：Facebook、LINE……等通訊軟體。

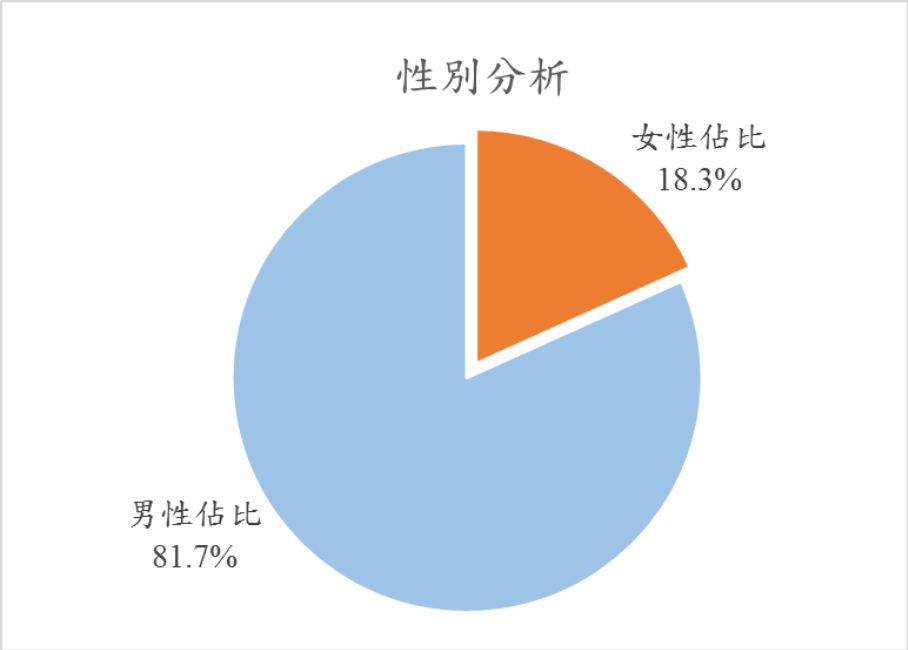
資料來源： GO survey 市調網

圖26 智慧型手機使用需求狀況分析

依據上述就使用者端所進行的調查中顯示智慧型手機的普及率與使用率以男女比例而言差異不大，男女主要差異則在於使用習慣與喜好類別之差異。

然就本計畫而言，因手機設備與資安議題之特殊性，男女比例之差異實屬顯著，茲將計畫期間辦理之座談會、說明會中與性別相關之統計分析如下：

計畫內會議出席男女比例為 81.7%與 18.3%，詳如圖 27，在各類職位分析上，規劃人員於女性之比例約為 25%，較平均比例稍高，其餘職位比例大致相同，詳見圖 28。



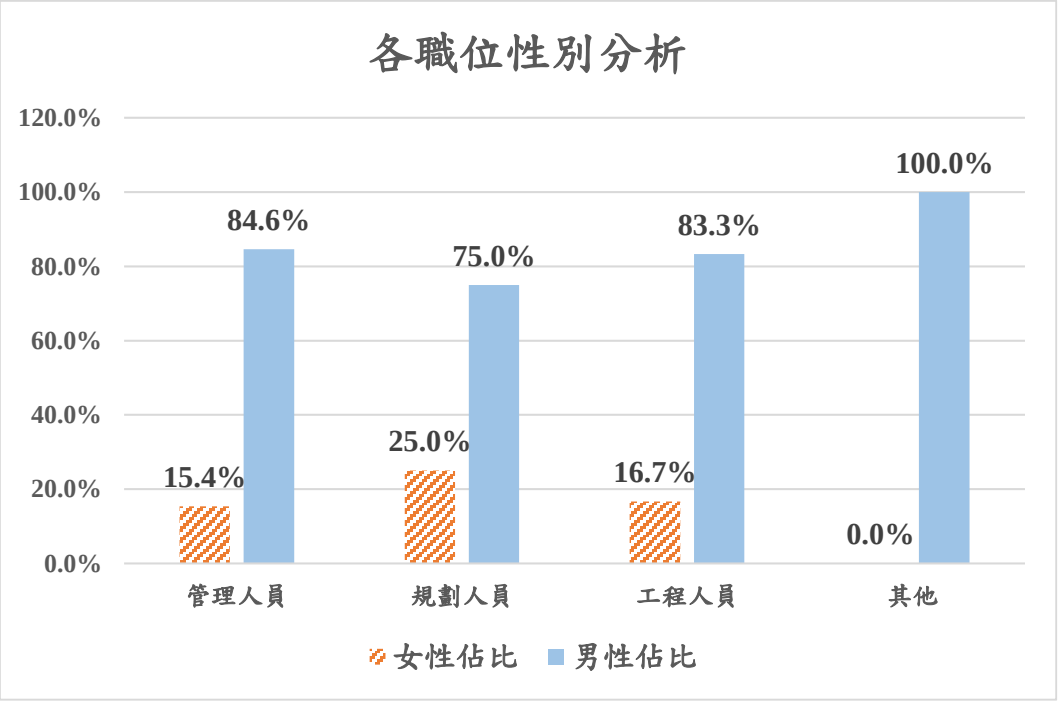
資料來源：本計畫彙整

圖27 計畫內會議出席男女比例

表38 計畫內會議各類職位男女人數分析表

	性別				
職位	女性	女性佔比	男性	男性佔比	總計
管理人員	10	15.4%	55	84.6%	65
規劃人員	9	25.0%	27	75.0%	36
工程人員	2	16.7%	10	83.3%	12
其他	0	0.0%	2	100.0%	2
	21	**18.3%**	**94**	**81.7%**	**115**

資料來源：本計畫彙整



資料來源：本計畫彙整

圖28 計畫內會議各類職位男女比例分析

十、專案工作會議

為掌控專案進度時程，除上述三場次座談會外，研究團隊定期召開工作會議，藉由工作會議聚集研究團隊成員以及與 NCC 共同針對專案內容進行進度說明，並就執行困難處共同討論，藉以達成共識。至 104/08/04 起至今共召開 9 場工作會議。各場次會議主題與會議時間整理如下表，詳細會議記錄詳見附件 9。

表39 專案工作會議進度表

場次	時間	主要議題
1	(起始會議) 104 年 08 月 04 日(星期二) 下午 2 時 00 分	● 硬體層檢測內容與 RFP 要求 ● 檢測實驗室修訂方向 ● 推廣說明會規劃
2	104 年 07 月 14 日(星期二) 下午 4 時 00 分	● 國際規範參考內容 ● 手機測試評估廠商名單 ● 規範擬定方向
3	104 年 10 月 5 日(星期一) 14:00~17:00	● 安全等級區分與定義 ● 自我宣告內容擬定 ● 檢測實驗室資格要求是否放寬
4	104 年 11 月 12 日(星期四) 16:00~17:30	● 「檢測實驗室主管」資格要求 ● 檢測實驗室資格與安全等級關係 ● 檢測實驗室試辦期規定 ● 功能權限聲明之驗證
5	105 年 1 月 5 日(星期二) 09:30~12:10	● 檢測項目細部調整 ● 檢測實驗室要點細部調整 ● 檢測結果報告細部調整
6	105 年 1 月 12 日(星期二) 09:30~13:20	● 檢測實驗室作業要點文句順修 ● 檢測實驗室資格區分準則

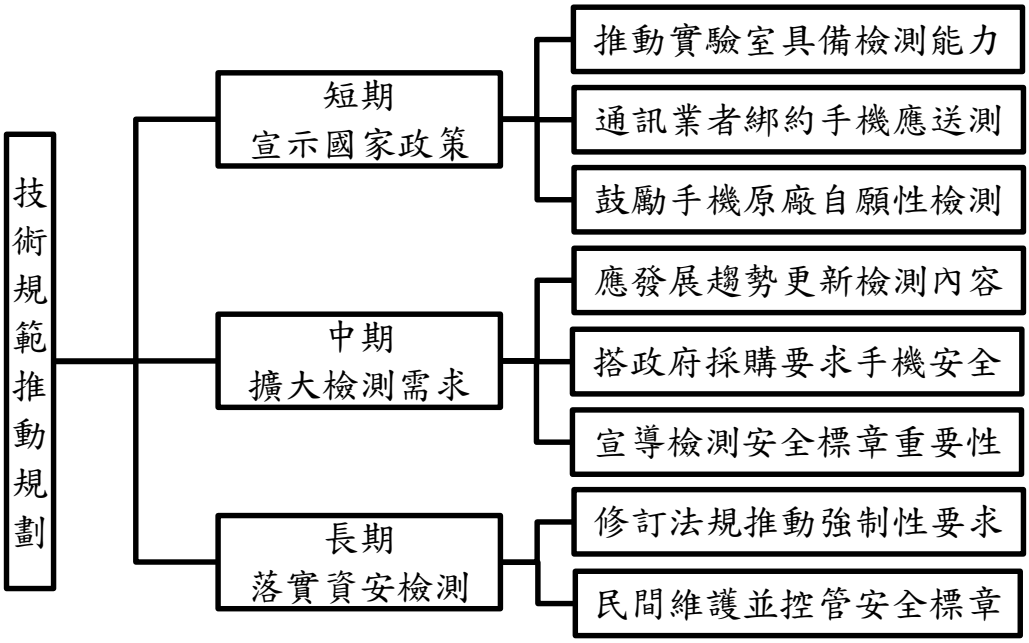
場次	時間	主要議題
		● 規範試辦期與正式期擬定
7	105 年 1 月 21 日(星期四) 09:30~12:00	● 與資策會擬定之 APP 規範交流
8	105 年 2 月 3 日(星期三) 16:40~19:40	● 檢測報告細部修改內容 ● 規範細部修改內容 ● 檢測實驗室區分類型
9	105 年 2 月 17 日(星期三) 16:30~20:30	● 規範草案定稿 ● 檢測實驗室管理作業要點內容細部修改

資料來源：本計畫彙整

以本規範訂立之手機五層架構而言，工業局 APP 規範的檢測範圍僅著重於 Data 層與 APPs 層，屬於手機層級較為上端層面，然而本規範檢測範圍涵蓋整支手機，從最上層之 Data 層延伸至手機 Hardware 層，因此檢測範圍較廣亦較深，為達到國家標準一致性，二份規範內容應須能相呼應，因此於 1 月 21 日研究團隊與工業局規範撰寫團隊進行交流會議，將二份規範內容以進行比對，比對雙方差異內容並進一步溝通討論，進行最適當之調整。

參、後續規範推動建議

由於目前國際間多數國家未強制性規定手機上市前須經資訊安全檢測，僅部分國際品牌手機業者以自主檢測方式宣稱手機安全性，然其檢測方式與檢測標準並未有統一規範，對於消費者來說無法明確判斷。為配合國家政策並維護消費者權益，本計畫研究團隊建議規範後續推動方向如下：



資料來源：本計畫彙整

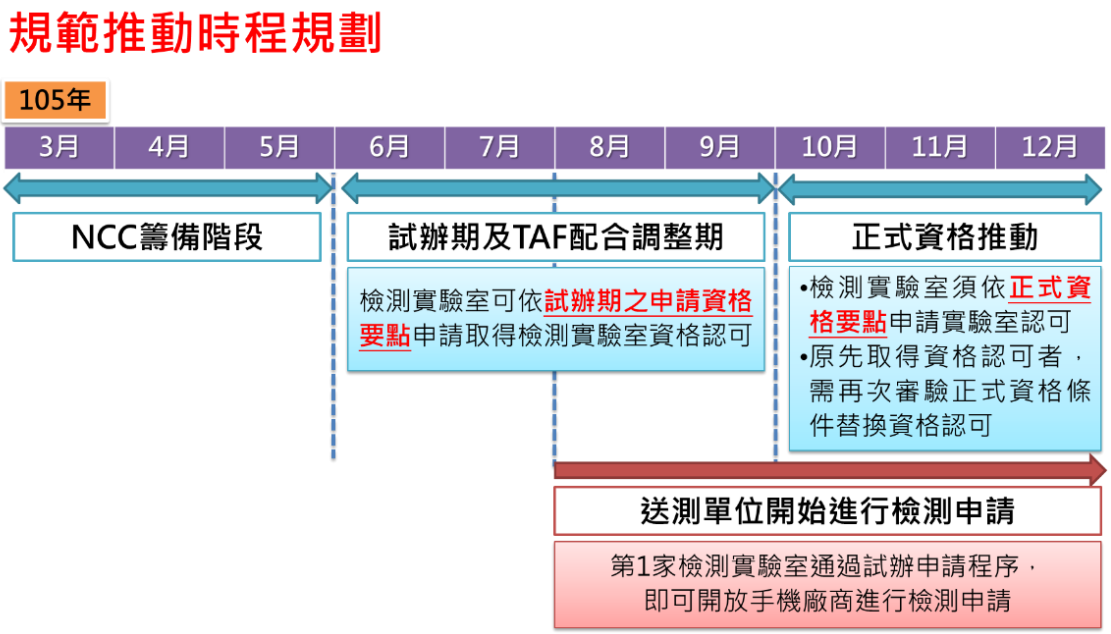
圖29 技術規範推動規劃

一、短期：自願性與半強制性推動規範藉以宣示國家政策

(一)推動實驗室具備檢測能力

規範推動第一步須先從檢測實驗室具備檢測能力著手進行，本規範之檢測實驗室須具備資安相關技術能力，因此檢測實驗室須有準備期程，故建議於本年 3~5 月間為主管機關籌備階段，將由 NCC 內部進行推動規劃前置作業，完成委員會審定程序，內容包含：檢測技術規範、試辦期說明文件、實驗室作業要點及審驗作業要點等文件，6~9 月間為檢測實驗室申請試辦期，開放檢測實驗室申請，

並同步由財團法人全國認證基金會(TAF)協助配合特定服務計畫之修訂，預計 8 月起即可開放檢測實驗室正式資格申請，並訂於 10 月 1 日正式啟動，於試辦期通過 NCC 與 TAF 認可之檢測實驗室可於試辦期間同時申請正式資格之檢測實驗室，試辦期間之檢測報告經 NCC 審定後即可取得安全標章。



資料來源：本計畫彙整

圖30　短期規範推動時程規劃

(二)通訊業者綁約手機應送測

目前智慧型手機主要銷售管道，不外乎是電信業者、通訊行、網路銷售等面向，高單價手機則以電信業者綁約手機為一主要銷售通路，由於電信業者屬特許行業，屬通傳會管轄，因此可由主管機關以行政命令要求智慧型手機於綁約販售前，須通過初級等級之內建軟體資通安全檢測。透過資通安全檢測可有效強化品牌手機之資通安全，更能有效提升非主流品牌手機安全性。更希望藉由資訊通透提供民眾購買智慧型手機的參考依據，進一步促使手機原廠業者提升手機安全性。

(三)鼓勵手機原廠自願性檢測

初期檢測除要求電信業者綁約手機須配合送測外，並鼓勵手機原廠自主性安全要求，進一步配合國家政策將智慧型手機送測，取得由 NCC 核發之安全標章。不僅可強調手機本身之安全性與保障消費者資訊安全之用心。

透過自願性送測與檢測實驗室檢測後之市場反應，了解檢測制度與檢測項目內是否因應國際檢測趨勢及手機技術發展趨勢，作為後續規範調整更新依據。

二、中期：因應趨勢調整規範並結合政府採購擴大檢測需求

(一)因應發展趨勢更新檢測項目

依據 2015 年第 16 屆國際共同準則研討會(ICCC)中，由韓國國家安全研究院(NSRI) Keunwoo Rhee 先生主講「Developing the Security Functional Requirements of Mobile Devices for the Korean Government」提到，為了解決行動裝置安全議題，韓國從 2014 年 8 月起集結產官學員各單位人馬針對行動裝置安全議題進行討論，以 CC 架構並列出行動裝置安全功能要求，包含資料保護、身分認證、安全管理、存取控管、可信賴路徑，以及延伸定義組件平台與應用管理保護，亦商討是否採納密碼模組認證機制。因此就研究團隊了解，國際間對於智慧型手機安全之檢測內容，並未有明確之安全標的，各項保護剖繪則有美國、韓國各自發展，仍處於草擬與規劃階段，尚未有實際 Test case 與檢測方法。並就目前所了解上述二國所研擬之安全標的內容，並未納入手機硬體層面向。除此之外，就研究團隊了解目前國內手機業者亦向各專業廠商採購硬體零件進行組裝，硬體(例如：手機晶片)相關安全性，實掌握在該硬體製造商而非手機原廠中。因此在此建議主管機關之後亦可參考國際手機資安的檢測管理模式，由主管機關將晶片硬體功能獨立檢測

並訂定相關檢測規範。另利用手機產品的分層架構特性及對應的檢測要求規範做法，將各類行動裝置或穿戴式裝置逐步納入資安檢測規範中，以提升國內行動裝置資通安全。

(二)搭政府採購要求手機安全

現在眾多民眾將手機應用延伸至公務應用上，一般大型企業透過導入行動裝置管理(MDM)方式進行使用管制，然而對於政府機關而言，不論是單位配發的公用手機，或個人攜帶的私人手機，行動裝置安全性管理實應更加嚴謹，因此建議除了要求通訊商販售手機給民眾時須經檢測外，中期則建議政府機關採購公務手機時，須採購取得本規範檢測安全標章之手機，搭配原機關所導入之行動裝置管理系統，進一步強化政府單位使用智慧型手機處理公務之安全性，有效敦促手機原廠提升資訊安全要求。

(三)宣導檢測安全標章重要性

智慧型手機系統內建軟體資通安全檢測機制，除可透過手機原廠自願性檢測並搭配原型式認證檢測要求外，更希望透過資訊通透公布與安全標章推廣，促使消費者重視手機安全，推廣方式可運用實體通路與虛擬通路雙管齊下共同進行，實體通路可運用電信業者通路推廣、政府計畫活動、記者會等實體廣宣。虛擬通路則可運用新聞媒體、網路廣告等方式進行，唯有強化消費者手機安全使用觀念與認知，提升消費者購買具安全等級標章之手機意願，方得以提升供需雙方對智慧型手機資通安全之重視。

三、長期：修訂法規並推動強制性要求落實資安檢測

(一)修訂法規推動強制性要求

智慧型手機已是民眾生活必需品，對於手機使用之安全性亦是刻不容緩的問題，本計畫於今年 2 月 19 日召開 2 場說明會，有 42%

的與會者支持國家以政策考量是否執行強制性檢測，更有 27%的與會者直接認為應列為強制性要求，二者加總已達 7 成比例。智慧型手機資安影響層面廣泛，基於保護消費者與資訊安全立場，實有必要成為國家安全政策之一，因此建議本規範與檢測制度長期應屬於強制性要求，依照手機應用範圍訂定安全等級進行強制性檢測要求，例如所有上市手機皆須通過安全等級初級，政府機關所使用之手機則須通過安全等級中級，執行機密業務者則須使用通過安全等級高級之手機，逐步推動強制性要求，使能強化手機整體安全性。

(二)民間維護並控管安全標章

智慧型手機生命週期短暫，作業系統版本更新快速，除手機原廠或電信業者於更新作業系統版本後，可將異動部分重新送測外，建議主管機關可定期進行市場抽測，進一步管控市面上手機是否符合規範要求，若執行成效良好，建議未來可考量將安全標章授權民間第三方公正單位發放，透過管理維運機制永續經營，更可有效降低政府機關維運與人事成本。

四、計畫研究期間相關問題討論與可行性作法建議

計畫團隊在研擬的過程中與多場次工作會議/座談會與說明會中，遇到相關問題與癥結點主要可分為以下幾個面向，並對應提出因應作為如下：

(一)規範適用於各類平台

規範訂定初期即以適用於各作業系統平台為優先，因此在試測期間依據各檢測細項予不同作業系統所產生之問題一一對應處理。因此考量檢測結果，檢測時是否需要管理者權限，及安全程度等因素，將檢測細項區分為三個等級。

並將因作業系統架構差異及需取得手機最高權限之部分檢測細項，列為選測項目，由送測單位選擇是否檢測。手機取得最高權限管理者之部分實涉及許多非技術性問題，包含廠商提供意願、取得權限之適法性問題等，是以將此部分測項以廠商自行選測方式辦理，避免引發上述相關問題。

(二)手機原廠自我宣告表深度

以資安檢測角度而言，若能用原始碼檢測方式，將可大幅節省測試時間及資源，但廠商角度則考慮智慧財產權及專利等相關公司資產保護，多僅願意以黑箱測試方式進行，然而黑箱測試若無法取得手機設備最高權限，則有些檢測項目將耗費較多時間及資源。

(三)同款手機是否需因不同通訊商進行送測

本規範以內建軟體為主要檢測標的，若相同型號之手機因配合不同行動通訊商而加載不同通訊商之 APPs，基於內建軟體差異仍需個別申請檢測。可考量二種檢測方案，以有效縮短檢測時程與費用，方案一：建議可由手機原廠進行送測，並於通訊商送測時檢附原廠手機檢測報告，僅針對通訊商加載之軟體進行檢測。方案二：於各家通訊商銷售之手機使用同一版本之內建軟體，並由手機原廠進行送測。

(四)檢測時程是否會耽誤上市時程

手機原廠擔心檢測時程耽誤上市時程，因此本規範於初級檢測項目中，已依循各界所期待透過提高送測手機數量與檢測人員配置，期可於兩周內即可檢測完成，相關時程安排則需請各手機原廠與通訊商納入整體排程考量。

(五)手機版本更新檢測方式

1.送測版本判定

依送測單位送來之測試機以及申請書填寫之版本為主，於手機開機後第一次連接網路時，若手機即刻更新，則以更新版本進行檢測，檢測實驗室則須與送測單位進行版本確認，以達送測版本共識。

2.版本更新控管

檢測完成後，若手機進行後續系統改版，則應重新申請檢測與更新安全標章，檢測項目則僅測試更新的部分即可，並依據新測項目為計價準則。

(六)手機資訊安全認證標章發放與張貼原則

手機資訊安全認證標章如同第貳章第二節所述，依安全等級區分，當送測手機通過安全檢測，可由送測單位提交檢測報告、及標章申請書一同送至 NCC 審核，並由 NCC 頒發符合檢測結果安全等級之資安認證標章，然手機若有更新版本進行重測，則應於完成重測後重新申請標章。

肆、附件

一、國際智慧型手機行動裝置資通安全相關研析報告

二、智慧型手機資安風險評估報告

三、智慧型手機系統內建軟體資通安全檢測技術規範草案

四、資通設備資通安全檢測實驗室管理作業要點修正草案

五、所測暢銷市售手機資安檢測結果

六、座談會會議紀錄、簽到表及研析意見

七、所辦說明會之紀錄及研析意見

八、智慧型手機之安全使用宣導資料

九、專案工作會議會議紀錄

十、手機內建軟體資安認證安全標章(電子檔)

附件 1 國際智慧型手機行動裝置資通安全相關研析報告

國際智慧型手機行動裝置資通安全相關研析報告

目 次

壹、 研究目標 ..... 附件 1-1

貳、 國際智慧型手機行動裝置資通安全檢測發展現況 ..... 附件 1-2

一、 國際組織 ..... 附件 1-4

(一) 開放網路軟體安全計畫 ..... 附件 1-4

二、 美國 ..... 附件 1-14

(一) 聯邦資訊長委員會 ..... 附件 1-14

(二) 國家標準技術研究院 ..... 附件 1-24

(三) 國土安全部 ..... 附件 1-33

(四) 國防部 ..... 附件 1-35

(五) 聯邦通信委員會 ..... 附件 1-45

(六) 國家安全局 ..... 附件 1-47

三、 歐盟 ..... 附件 1-54

(一) 歐盟網路資訊安全局 ..... 附件 1-54

(二) 歐盟執行委員會 ..... 附件 1-55

四、 中國大陸 ..... 附件 1-58

(一) 大陸工業和信息化部 ..... 附件 1-58

五、 英國 ..... 附件 1-60

(一) 英國通訊電子安全局 ..... 附件 1-60

(二) 英國資訊委員辦公室 ..... 附件 1-61

(三) 英國通訊傳播管理局 ..... 附件 1-62

六、 日本 ..... 附件 1-64

(一) 日本智慧型手機安全協會 ..... 附件 1-64

(二) 資訊技術促進機構 ..... 附件 1-65

七、 新加坡 ..... 附件 1-67

(一) 新加坡金融管理局 ..... 附件 1-67

八、 韓國 ..... 附件 1-68

(一) 大韓民國廣播通信委員會 ..... 附件 1-68

參、 各國標準研析與比較 ..... 附件 1-70

一、 全國強制性之標準規範 ..... 附件 1-70

二、 政府組織內部規範 ..... 附件 1-70

三、 組織與企業指引 ..... 附件 1-70

四、 使用者/開發者指引 ..... 附件 1-70

五、 風險評估 ..... 附件 1-70

肆、 現行國際行動終端硬體晶片檢測說明 ..... 附件 1-88

伍、 結論 ..... 附件 1-92

一、 OWASP Mobile Security Project - Top Ten Mobile Risks ... 附件 1-92

二、 SP 800-164, DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices 及 YD/T 2407-2013 移動智能終端機安全能力技術要求(包含配套文件 YD/T 2408-2013 移動智能終端機安全能力測試方法) ..... 附件 1-92

三、 Security Requirements for Mobile Operating Systems ..... 附件 1-92

四、 Commercial Mobile Device Implementation Plan、Mobile Device Strategy、Mobile Operating System Security Requirements Guide 、Mobility Security Guide ..... 附件 1-92

五、 SP 800-163, Vetting the Security of Mobile APPlications.... 附件 1-93

圖 目 次

圖 1　行動裝置威脅模型.....附件 1-6
圖 2　行動裝置遭受之威脅.....附件 1-9
圖 3　行動裝置十大風險.....附件 1-9
圖 4　行動安全參考架構.....附件 1-18
圖 5　行動運算決策框架.....附件 1-24
圖 6　五層式行動裝置架構.....附件 1-28
圖 7　計畫實作框架.....附件 1-38
圖 8　組成政府組織行動化架構的各個基本區塊.....附件 1-49
圖 9　行動式智慧型終端安全能力框架.....附件 1-59

表 目 次

表 1　國際間智慧型手機行動裝置資通安全相關文獻整理表 .....附件 1-2
表 2　行動運算對應服務與基礎設施.....附件 1-17
表 3　各國規範綜合研析比較表.....附件 1-71
表 4　OWASP 與 YD/T 2407-2013 分類對應表 .....附件 1-78
表 5　國際組織與各國規範所公告之相關技術細節彙整對應表 .....附件 1-80
表 6　共通準則硬體安全深度彙整分析表.....附件 1-89
表 7　使用者指引參考表.....附件 1-94

壹、研究目標

隨著智慧型手機軟、硬體技術一日千里，且功能日趨多元化與複雜化，行政院國家資通安全會報 103 年 6 月 24 日第 26 次會議決議，參考各國管制機制，規劃並制訂資安檢測標準，反觀當前國際間並未有一致性的檢測標準，且歐美等部份先進國家亦無強制性規範。因此藉由蒐集國際智慧型手機行動裝置資通安全檢測發展資料，以提供後續研擬適合我國智慧型手機系統內建軟體資通安全檢測技術規範及檢測實驗室認可規定等，以完備智慧型手機資通安全檢測及認證機制，並藉由對智慧型行動裝置加強基礎安全要求，以保障民眾個資及隱私之防護。

貳、國際智慧型手機行動裝置資通安全檢測發展現況

此章節主要提供國際間因應智慧型行動裝置資訊安全問題，所整理或制定政策之相關內容，本計畫將各國相關之發佈文件收集並彙整如下表，且提供對應之說明如後，以作為後續研擬資通安全檢測技術規範及檢測實驗室認可規定之參考。

表1　國際間智慧型手機行動裝置資通安全相關文獻整理表

編號	地區	發佈單位	相關發佈文件
1	國際組織	A. OWASP(Open Web APPlication Security Project)	1. OWASP Mobile Security Project - Top Ten Mobile Risks(2014)
2	美國	A. U.S. Chief Information Officer and the Federal CIO Council	1. Government Mobile and Wireless Security Baseline(2013/5)
		B. National Institute of Standards and Technology(NIST)	1. SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations(2013/4) 2. SP-800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise(2013/6) 3. SP 800-142, Practical Combinatorial Testing(2010/10) 4. SP 800-164, DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices(2012/10) 5. SP 800-163,Vetting the Security of Mobile APPlications (2015/1)
		C. Department of Homeland Security(DHS) (US-CERT)	1. Cyber Threats to Mobile Phones(2011)
		D. Department of Defense(DoD)	1. Commercial Mobile Device Implementation Plan(2013)

編號	地區	發佈單位	相關發佈文件
			2. Mobile Device Strategy(2012) 3. Mobile Operating System Security Requirements Guide Version 1, Release 3 (2013/6)(DISA)
		E. Federal Communications Commission (FCC)	1. Ten Steps to Smartphone Security(2012/12) 2. Ten Steps to Smartphone Security (Android)(2012/12) 3. Ten Steps to Smartphone Security (iOS)(2012/12) 4. Ten Steps to Smartphone Security (Windows Phone)(2012/12) 5. Ten Steps to Smartphone Security (BlackBerry)(2012/12)
		F. National Security Agency(NSA)	1. Mobility Security Guide v2.3(2013/11) 2. Security Requirements for Mobile Operating Systems v1.0 (2013/1) (NIAP)
3	歐盟	A. European Union Agency for Network and Information Security (ENISA)	1. Smartphone secure development guidelines for APP developers(2011/11) 2. Top Ten Smartphone Risks(2014)參考到 Smartphones: Information security risks, opportunities and recommendations for users(2010/12)
		B. European Commission	1. Opinion 02/2013 on APPs on smart devices(2013/02)
4	中國	A. 工業和資訊化部	1. YD/T 2407-2013 移動智能終端機安全能力技術要求(2013/4) 2. YD/T2408-2013 移動智能終端機安全能力測試方法(2013/4)

編號	地區	發佈單位	相關發佈文件
5	英國	A. Communications-Electronics Security Group(CESG)	1. End User Device Strategy: Security Framework & Controls(2013/2) (ERG)
		B. Information Commissioner's Office (ICO)	1. Personal information online small business checklist
		C. Office of Communication(Ofcom)	1. Safer smartphones–keeping your device secure(2013/10)
6	日本	A. Japan Smartphone Security Forum (JSSEC)	1. Security Guideline for using Smartphones and Tablets(2011/12)
		B. Information-technology Promotion Agency (IPA)	2. 10 Major Security Threats (2013/3)
7	新加坡	A. Monetary Authority of Singapore	1. Technology Risk Management Guidelines(2013/6)
8	韓國	A. Korea Communications Commission	1. KCC announces 'Comprehensive Plans for Smart Mobile Security'(2010/12)

資料來源：本計畫整理

一、國際組織

(一)開放網路軟體安全計畫

開放網路軟體安全計畫(Open Web APPlication Security Project 簡稱 OWASP)，是一個開放社群、非營利性組織，全球目前有 82 個分會，其主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善應用程式的安全性。美國聯邦貿易委員會(FTC)更強烈建議所有企業務必遵循 OWASP 所發佈的十大網路弱點防護守則，美國國防部亦將此守則列為最佳實務。(Simplifying APPlication Security and Compliance with the OWASP Top 10) 此網站每年度收集之資料分析相關行動裝置 APP 之風險與威脅並公告，目前已知歐盟文件在 2011 年 11

月發表的 Smart-phones secure development guidelines for APP developers 參考此資料做為制定指引之基礎。

因應雲端技術快速的發展，不論是使用者或應用程式開發者，資訊的操作模式已逐漸地從主機平台移至可攜式行動裝置或智慧型手機，即使平台不同，仍會產生一定程度的弱點風險。

OWASP 採用行動威脅模型(Mobile Threat Model)的研究方法，行動威脅模型是一個系統的過程，必須定義以下幾個方面以用於理解可能造成應用程式的威脅：

- 行動裝置應用架構：主要描述行動裝置中使用之特定功能，包含：無線傳輸協議、數據傳輸、傳輸型態，硬體介面和其他應用程式與服務的交互應用。整體架構應包含網路基礎設施、網路/端點服務、可信任邊界及第三方 APIs 等。
- 行動數據傳輸：行動裝置內之資料與應用程式間如何安全傳輸？不同行動裝置之作業系統資料間如何互通？應用程式是否使用雲端進行資料備份？資料存取時是否可識別由取得授權者進入存取？上述資料應包含靜態數據與動態傳輸數據。並應考量越獄(Jailbreaking)與取得原始管控權力(Rooting)之面向。
- 威脅代理鑑定：定義何種威脅適用於行動應用，故採取三個步驟—S1 將須保護之敏感資料列表，S2 將預計索取 S1 資料之程序過程列表，S3 將上述二個步驟分析進行威脅判定(例如：哪一個程式在哪一個過程中試圖傳送須保護之敏感資料，故判定上述狀況屬威脅)。
- 攻擊方法：攻擊主要可分為二個類型，一種屬計畫性攻擊，另一種則為觸發式攻擊。攻擊方法可能包含讀取本機資料、中間人攻擊、無線網路端點攻擊、應用程式層攻擊等，透過定義上述這些攻擊方式，以利控制被侵入並減輕攻擊。

- 控制措施：定義如何防止攻擊，例如：哪些方式可檢測攻擊方法？如何最小化攻擊所造成之影響？如何保護個人隱私資料？依據各類型之攻擊方法找出對應之控制措施，進而防止或減輕攻擊。

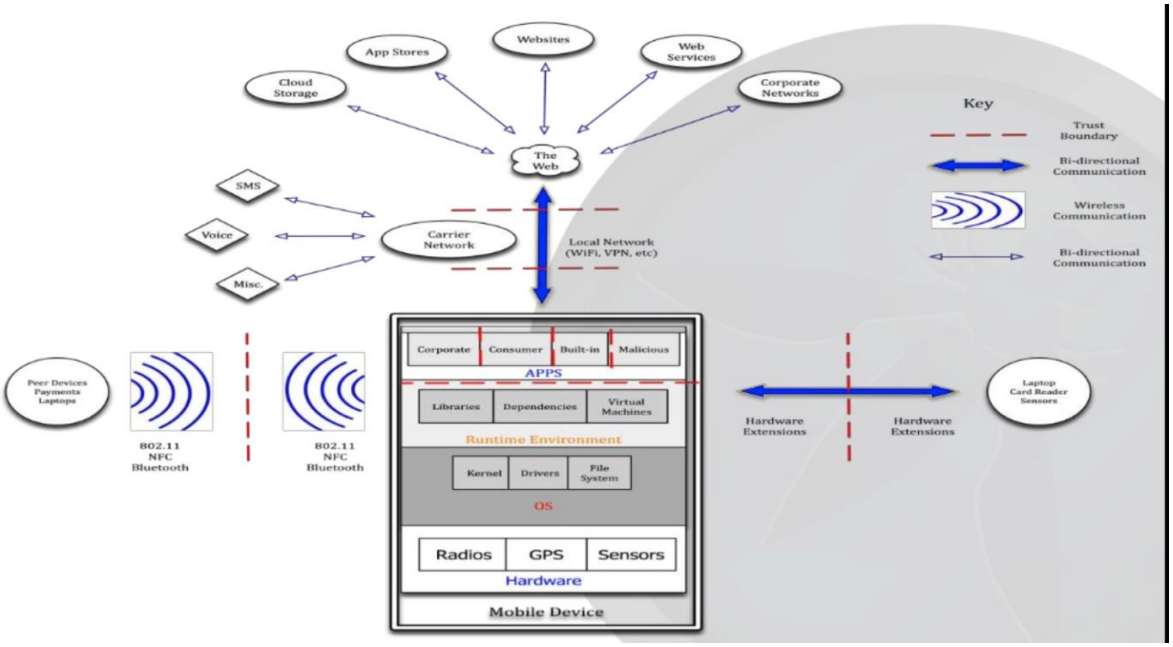


圖1　行動裝置威脅模型

資料來源：OWASP

該研究方法將可攜式裝置遭受的威脅分成 6 大分類，分別為：

1.詐欺(Spoofing)：是一種技術用以取得非經授權的存取電腦，其手法主要以偽裝發送訊息、郵件的位址或偽裝成為已被授權的使用者，在未經許可下進入安全的電腦系統，以進行任何不法的行為。Spoofing 多為垃圾郵件發送者、駭客或網路詐騙者所使用，藉以達到犯罪行為而不被發現。

2.拒絕/否認(Repudiation)：讓沒有修改權利的人或系統能夠竄改他人資訊或否認某些事實，其目的在破壞資料的完整性。否認的反面為不可否認 (non-repudiation)，是指藉由提供原本的證據，使發件人不能否認曾發出信息，而收件人也不能否認曾收到信息。例如在網路上購物，商家有時不只要求消費者提供信用卡

號，還要信用卡的 PIN。藉由消費者的身分確認，商家就有不可否認的證據來進行交易。

3.阻斷服務(Denial of Service)：亦稱洪水攻擊，是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其對目標客戶不可用。當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時，其稱為分散式阻斷服務攻擊(Distributed Denial of Service attack，縮寫：DDoS)。攻擊發起者一般針對重要服務進行攻擊，如銀行，信用卡支付閘道器，甚至網域名稱伺服器。該類攻擊也常見於部分遊戲，被心懷不滿的玩家或是競爭對手廣泛使用。DDoS 攻擊可以具體分成兩種形式：頻寬消耗型以及資源消耗型。它們都是透過大量合法或偽造的請求占用大量網路以及器材資源，以達到癱瘓網路以及系統的目的。

(1)頻寬消耗型：可以又分為兩個不同的層次；洪泛攻擊或放大攻擊。

A.洪泛攻擊的特點是利用殭屍程式傳送大量流量至受損的受害者系統，目的在於堵塞其頻寬。

B.放大攻擊與洪泛攻擊類似，是通過惡意放大流量限制受害者系統的頻寬；其特點是利用殭屍程式傳送資訊，但是資訊卻是傳送至廣播 IP 位址，導致系統子網路被廣播 IP 位址連線上之後再傳送資訊至受害系統。

(2)資源消耗型攻擊：協定分析攻擊(SYN flood，SYN 洪水)傳送控制協定(TCP)同步(SYN)攻擊。TCP 行程通常包括傳送者和接受者之間在封包傳送之前建立的完全訊號交換。啟動系統傳送一個 SYN 請求，接收系統返回一個帶有自己 SYN 請求的 ACK(確認)作為交換。傳送系統接著傳回自己的 ACK 來授

權兩個系統間的通訊。若接收系統傳送了 SYN 封包，但沒接收到 ACK，接受者經過一段時間後會再次傳送新的 SYN 封包。接受系統中的處理器和記憶體資源將儲存該 TCP SYN 的請求直至超時。DDoS TCP SYN 攻擊也被稱為「資源耗盡攻擊」,它利用 TCP 功能將殭屍程式偽裝的 TCP SYN 請求傳送給受害伺服器，從而飽和服務處理器資源並阻止其有效地處理合法請求。它專門利用傳送系統和接收系統間的三向訊號交換來傳送大量欺騙性的原 IP 位址 TCP SYN 封包給受害系統。最終，大量 TCP SYN 攻擊請求反覆傳送，導致受害系統記憶體和處理器資源耗盡，致使其無法處理任何合法用戶的請求。

4.篡改(Tampering)：是指未經授權的刪除、插入、或更改資訊，並期望別人無法察覺。例如學生更改考試成績，或是駭客進銀行網路刪除信用卡消費紀錄等。

5.資訊洩漏(Information Disclosure)：將資料洩漏給不該接收的使用者，例如，攻擊者在沒有存取權的情況下，讀取機密性的檔案。

6.提升權限(Elevation of Privilege)：讓一個遠端一般使用者，透過非正常的管道，提升權限能夠執行一些只有系統管理員才能使用的指令集。

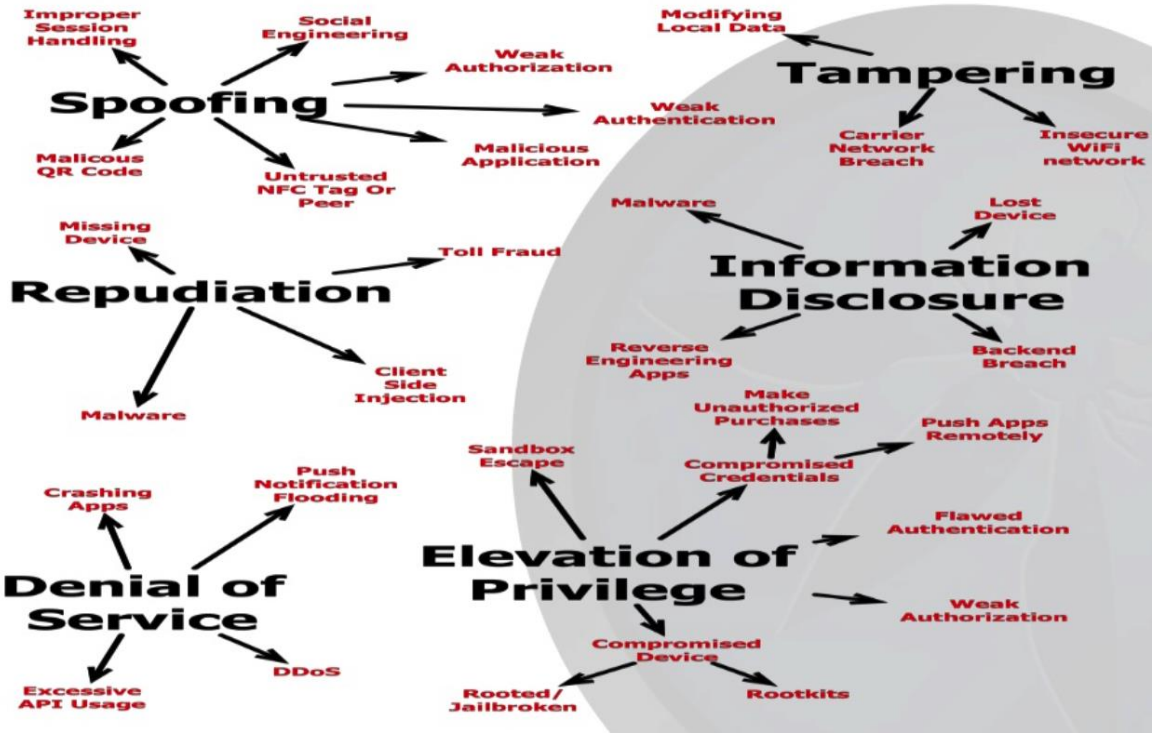


圖2　行動裝置遭受之威脅

資料來源：OWASP

此外 OWASP 再將上述分類依照風險所造成嚴重性衝擊(例如：機密性、完整性、可用性)加以定出十大弱點。相關內容彙整如下：

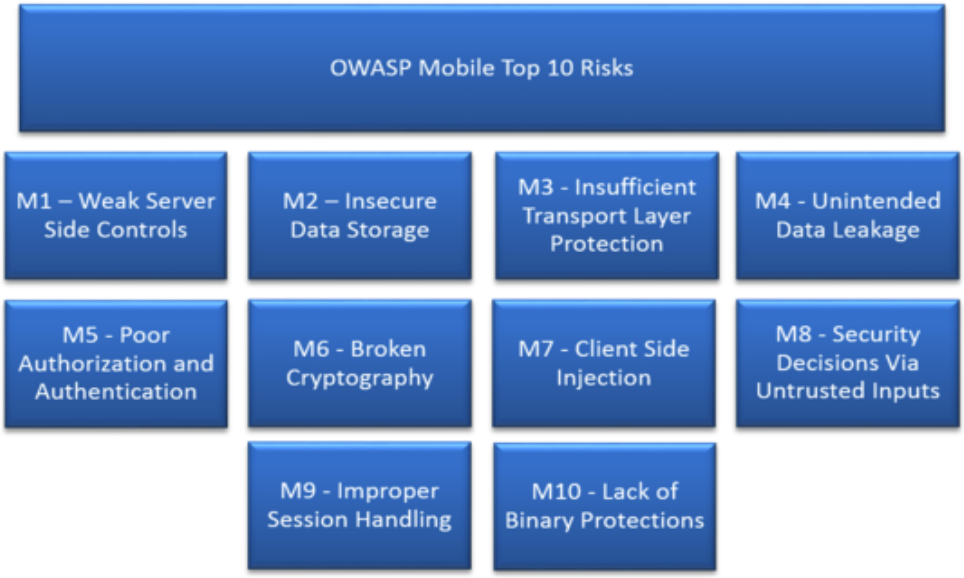


圖3　行動裝置十大風險

資料來源：OWASP

1.脆弱的伺服器端控制(M1:Weak Server Side Controls)

主要是說明 Mobile 的弱點並不只單存在於 Mobile 端，所開發的 APP 應用程式或雲端系統的程式亦有可能存在弱點，例如：OWASP Cloud Top 10。

【建議防護措施】人員於伺服器端開發應用程式時，應避免產生 OWASP Web Top 10 或 OWASP Cloud Top 10 相關弱點。

2.不安全的資料儲存(M2:Insecure Data Storage)

意指敏感性資料未受到適當的保護，一般常見如敏感性資料未加密，或是一些不常用到的暫存資料可能含有敏感訊息(例如：登入帳號與密碼)，可能會造成機密性資料損失、憑證外洩、侵犯隱私權等衝擊。

【建議防護措施】只儲存必要資訊，不將敏感資料存放於開放式的儲存媒體(例如：SD 卡)，採用安全的檔案加密應用程式介面，設定檔案的讀取與寫入設定權限等。

3.傳輸層保護不足(M3:Insufficient Transport Layer Protection)

可攜式行動裝置於傳輸機敏性資料時，很常發生未加密情況，例如：瀏覽器本身不支援 HTTPS 功能，或是使用的 APP 應用程式未採用加密方式進行資料的傳輸(如：登入系統、交易資料等)，因此可能會造成駭客使用中間人攻擊(Man-in-the middle attacks)，從中竄改或竊取封包資料，進而造成機敏資料的洩漏。

【建議防護措施】程式開發者應確保所有敏感性資料有採用加密方式進行傳輸，傳輸媒介可包含網路連線、Wifi 連線，甚至是近場通訊(Near Field Communication, NFC)連線等，若只採用明文方式傳遞，攻擊者可輕易透過網路監聽方式(Sniffer)竊取機敏性資料。

4.非故意或意外造成的資料外洩(M4:Unintended Data Leakage)

可攜式行動裝置中的第三方應用程式可能會自動幫使用者儲存一些敏感性資訊，例如：網頁暫存(Web Cache)、按鍵側錄(Keystorke Logging)、擷取畫面(Screenshots)、日誌檔(Logs)或暫存目錄(Temp Directories)等，一但攻擊者成功取得行動裝置權限時，將會侵犯使用者隱私，甚至導致資料洩漏情形。

【建議防護措施】一些較敏感性的資料應避免自動儲存於可攜式行動裝置內(例如：憑證資訊、帳號、密碼等)，檢查部分應用程式是否會儲存敏感性資訊，建議加以手動移除，或是選擇不自動儲存功能。

5.粗糙的授權與認證(M5:Poor Authorization and Authentication)

部分可攜式行動裝置的網頁應用程式僅採用永不變的數值來執行身分驗證與授權階段，例如：國際行動設備識別碼(International Mobile Equipment Identify Number, IMEI)、國際行動用戶識別碼(International Mobile Subscriber Identify, IMSI)或通用唯一識別碼(Universally Unique Identifier, UUID)。

【建議防護措施】使用嚴謹的身分驗證與授權(例如：雙因素認證)，避免使用可攜式行動裝置的硬體 ID 標籤或永不變的 ID 識別碼做為身分驗證的因素。

6.加密失效(M6:Broken Cryptography)

所謂加密失效分為兩種情況，一種是使用複雜的加密演算法卻遭到破解，另一種為使用過於簡單的加密演算法遭到破解。前者要實現的困難度較高，後者則是相當常見。OWASP 提出幾個對於加密方法的謬誤，例如：編碼(Encoding)、混淆(Obfuscation)、序列化(Serialization)，上述嚴格說起來，並非為

嚴謹加密方式，攻擊者能輕易破解簡單的加密演算法後，取得可攜式行動裝置的完整資訊，同樣也可做到提升權限或機敏資料遭洩漏等情況。

【建議防護措施】開發應用程式建議使用強健的加密演算法，並不斷進行反覆測試，直到應用程式開發完成時，仍需執行嚴格的挑戰測試(Battle-Tested)。

7.客戶端注入(M7:Client Side Injection)

Injection 攻擊即使從傳統電腦轉移到了可攜式行動裝置上的網頁應用程式，若網頁應用程式存有 Injection 弱點，攻擊者仍可利用 SQL Injection 或 XSS 攻擊手法來提升可攜式行動裝置的權限，或是利用網路盜打市話(Toll Fraud)的情況發生。

【建議防護措施】網頁應用程式傳遞參數給雲端資料庫的內容，需過濾不受信任或不應該接受的內容，例如：SQL 執行語法、特殊字元等，同樣可採用 prepared statement 功能進行過濾。

8.安全決策是經由不受信任的輸入(M8:Security Decisions Via Un-trusted Inputs)

在各種可攜式行動裝置的平台均會發生(例如：iOS、Andriod)，應用程式可能經由惡意攻擊者精心設計，或是應用程式遭攻擊者透過 Client Side Injection 攻擊方式來消耗可攜式行動裝置的硬體資源或提升權限情形。舉例來說，假設 Skype 應用程式具有 HTML 或 Script Injection 弱點，攻擊者只要事先把具有惡意連結的 inframe 寫入某個特定網頁，一旦可攜式行動裝置的瀏覽器讀取到此段程式碼時，則應用程式將無需使用者授權，自動開始播號給指定的電話號碼。

【建議防護措施】每個應用程式在設計時應注意身分認證與授

權的問題，以確保可攜式行動裝置需經過使用者的身分驗證後才允許執行特殊的行為或功能。

9.不適當的會話處理(M9:Improper Session Handling)

可攜式行動裝置的應用程式 session 過期時間，一般而言會設定的比較長，原因是對使用者方便存取或使用，通常這些 session 經由 HTTP Cookies、Oauth Token、Single Sign-on 等方式來進行維護，建議避免使用裝置的硬體識別碼來當作 session 值，很容易讓攻擊者猜到 session 內的機密性內容(例如：帳號或密碼)，進而造成提升攻擊者於可攜式行動裝置的權限，進行非授權的存取。

【建議防護措施】若需要提高安全性，相對其軟硬體設計(演算法或操作方式)的複雜度亦會增高，只要 session 值的過期時間應設定在一個可接受範圍內，就無需擔心讓使用者太頻繁的重新驗證；另外可攜式行動裝置遭遺失或竊取時，應有能夠快速撤銷 Token 的機制，使裝置無法更近一步遭受到濫用情況。

10.封裝檔案保護不足 (M10:Lack of Binary Protections)

此弱點的洩漏方式，乃是指應用程式原始碼中，把輸入或輸出的相關參數直接寫入在程式碼當中，因此只要攻擊者能夠取得應用程式的原始碼(例如：透過逆向工程手法)，若原始程式碼內容含有敏感資訊，像是 API 金鑰、帳號或密碼等，可能會造成企業內部的智慧財產暴露或各人憑證洩漏等情況。

【建議防護措施】程式開發者應避免將敏感資訊寫入於原始程式碼中。

本計畫依據 OWASP 公告之相關技術細節，分析彙整如下以作為後續檢測項目編寫之參考。

二、美國

(一)聯邦資訊長委員會

2009 年 3 月，隨著歐巴馬上任，才首度在美國聯邦政府體制內設立聯邦首席資訊辦公室(Federal Chief Information Officer; 簡稱 Federal CIO)，負責主導聯邦 IT 預算的策略規劃、政策方向，並且監督聯邦科技預算的支出情形。

1.Government Mobile and Wireless Security Baseline

資訊科技帶來的資通訊安全問題，促使資通訊安全議題成為各國關注的焦點。數位政府策略(Digital Government Strategy，簡稱 DGS)由聯邦 CIO2012 年 5 月發行，說明應用於的電源與數位科技的創新，使民眾能隨時隨地利用在任何設備安全的接收數位訊息和其他服務的願景。該策略意識到行動裝置、應用程式、網路和無線網路有效整合安全和隱私的挑戰。

DGS 為促進安全和可靠的新技術被採用，DGS 的里程碑行動 9.1 任務是由美國國土安全部(DHS)部，國防部(Department of Defense; 簡稱 DOD)和美國國家標準與技術研究院(NIST)一同發展關於行動電腦的安全需求之基本標準，以及行動安全參考架構(Mobile Security Reference Architecture，以下簡稱「參考架構」)，其中這個架構融合了安全和隱私的設計。從國家標準與技術研究院(NIST)、美國國土安全部(DHS)、國防部(DoD)、司法部(Department of Justice)，總務管理局(General Services Administration，簡稱 GSA)和行動技術勇士隊(Mobile Technology Tiger Team，簡稱 MTTT)的其他成員組成了技術工作群組，以制定行動安全基準。這樣的一個參考架構也同時發展成為由國土安全部聯邦網路應變部門所帶領，一種有組織的跨部門合作行動。

本文件包含行動安全基準，並解釋參考架構、行動運算決策架構及其他 DGS 行動安全活動之間的關係。那些為了里程碑行動 10.2(Milestone Action 10.2)而建立在 DGS 報告裡的，包含政府所使用行動技術：障礙、機會及缺陷分析(以下簡稱 DGS 障礙和機會報告)，確定了需要改進的四個關鍵領域，並包含所需的工具和流程，以「加速推動採用安全行動技術進入聯邦政府環境」：

- 行動設備管理(MDM)
- 行動應用程式管理(MAM)
- 身分和訪問管理(IAM)
- 數據管理

DGS 障礙和機會報告中描述一群典型數位化政府服務案例的集合(民眾、合作夥伴、地方政府、聯邦政府員工和國安系統)。為了發展行動安全基準，使用案例被分為受機構控制和非受機構控制的設備方案，且同時涵蓋安全的行動運算四個關鍵要素，每個案例都需要滿足上述四大功能。此份行動裝置安全要求基準，將依循 NIST 所發佈的標準與指引所建立，並聚焦於聯邦雇員的使用案例之基準要求，以及在這份文件中包含了對於本身所提出的參考架構及國防部聯邦網路應變部門所發佈的行動運算決策框架(Mobile Computing Decision Framework ; MCDF)。

經由本指引以協助政府的各部門單位，透過使用 MCDF 定訂出各自適當的安全相關要求與風險容忍指標，選擇出適合政府的各部門單位行動安全架構，以及應用行動安全基準在所定義的安全控制措施上。本文件主要目標在於引導政府的各部門單位導入行動安全方案於他們各自的資訊安全作業程序，但本文件不能被用來取代其他用於保護聯邦訊息及資訊系統的強制性要求。此準則依據下列主題分別說明如下：

(1)行動運算概述

行動運算技術允許讓聯邦各部門單位自行定義需求，以讓員工與人民存取政府資訊與服務不受時空限制。行動運算透過有線與無線的方式延伸，從行動裝置至聯邦各部門單位系統與基礎架構以提供數位化的政府服務。

此外，里程碑行動 10.2 中的四大關鍵領域，與一般行動運算架構之間的關係，以提供參考者一個全面性概念觀點。另對於風險與架構之間的對應分別加以討論如下。

A.了解行動威脅、風險和風險的對應方式

由於行動設備與電腦都面臨著相同的威脅，但行動 APPs 的普及與設備的多樣性，又額外增加了來自機密性、完整性與可用性對於資訊安全的威脅挑戰。然而面臨不斷演進的威脅，除了設法緩解及進行管制外，還需要人員資安意識的培訓，以解決行動裝置衍生的具體威脅、透過擬定資安策略對威脅行為之規則化加以定義、及管理行動裝置的使用核可。因此建議各部門單位應遵循 NIST 發佈的指引，並導入風險管理辦法加以識別、評估、行動運算相關的風險等級、以降低這些風險所可能造成的影響。

B.通用行動運算架構

本標準依據上述說明，歸納出當一個整合性的行動運算功能進入聯邦各部門單位的網路中，除了需要利用現有的基礎設施外，還需要額外增加新的服務與基礎設施，以加強管理與認證等。本計畫依據內容整理相關對應資訊如下表所示。

表2　行動運算對應服務與基礎設施

行動設備管理 MDM	行動應用程式管理 MAM	身分和訪問管理 IAM	數據管理
• 企業控制設備配置 • 實施安全策略 • 遵守監測及反應 • 安裝應用程式管理設備配置與安全,將設備狀態回傳到企業伺服器	• 白名單/黑名單的應用程式 • 遠端清除機構的應用程式和數據 • 應用程式的審核和認證 • 應用程式配置的管理和監控	• PIV-基於用戶身分驗證 • USB、NFC、HSM 身分驗證方法	• 數據分類與標記讓訊息共享及維護 • 加密存儲在行動裝置數據 • 使用 FIPS 認證加密模組

資料來源：本計畫整理

C.聯邦行動裝置使用案例

為了近一步闡述數位政府策略(DGS)的障礙與機會報告之內容，行動技術勇士隊(MTTT)定義了數位化政府服務所提供的五個使用者群層級，對應到各自的使用者案例。

(2)行動安全參考架構

由於國防部聯邦網路應變部門負責發展民間企業用的參考架構，故藉由各機構間的合作發展出行動安全參考架構，該架構參考了下圖的概念架構圖並加以延伸，定義了行動架構與裝置管理方案應用在某個單位中，需要能支援多個使用案例及能廣泛被應用於行動裝置的應用與服務上。該行動安全參考架構如下圖所示。

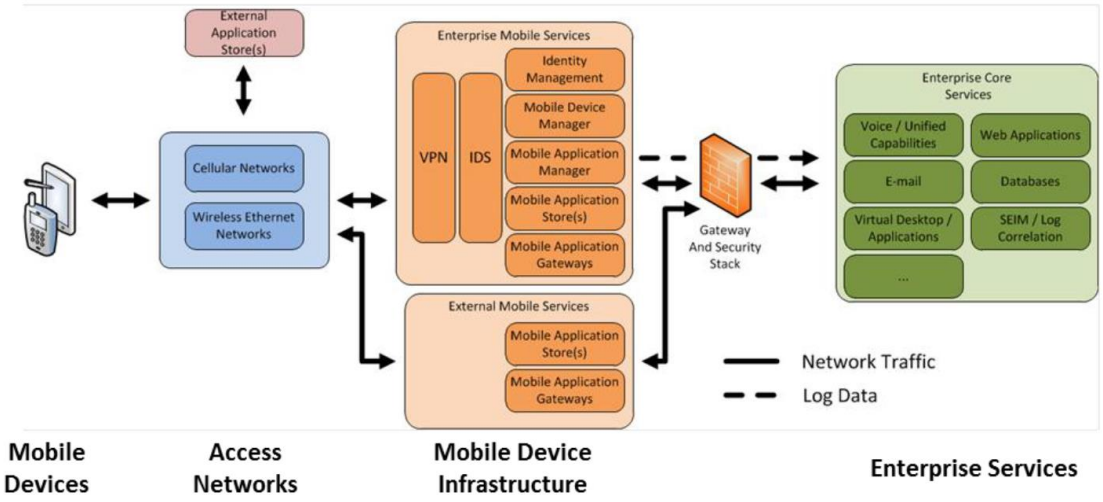


圖4　行動安全參考架構

資料來源：Federal C.I.O.

A.行動裝置(Device)

本框架中之行動裝置包含智慧型手機及平板電腦，行動裝置之硬體架構中，包含有蜂巢式電話(Cellure Phone)、WiFi 無線網路、攝影機、麥克風、衛星定位裝置、藍牙/NFC、USB 及所連接之外接裝置等。

行動裝置作業系統，得以特定韌體版本，建置初始安裝 APPs，在安全管理上，可以另行安裝行動裝置管理 APPs，以管理該行動裝置或是所安裝之 APPs。亦可以安裝虛擬作業系統，以納管指定之 APPs。

B.資料(Data)

行動裝置可以藉由 APPs 之安裝，以下載或是儲存電子資料，並依其作業系統架構之不同，例如：Apple　iOS 將 APPs 安裝之目錄加以隔離，每一 APPs 安裝目錄會有自己的文件夾，其中所存放之檔案，僅限該 APPs 所存取。

另有關資料之安全，主要可採行硬體或是軟體模式加密。

硬體加密模式方式之一，是利用 MicroSD 儲存媒體，內建加密晶片，以對於指定檔案或目錄，進行加密作業。

軟體加密模式主要由 APPs 軟體所實作，以確保資料在儲存、作業、傳送各階段之安全。

C.存取網路(Access Network)

行動裝置之存取網路主要以蜂巢式行動網路，例如：3G 或是 4G 行動電話網路，可以同時提供語音及數據傳輸之功能。採用分頻、分時多工或是展頻之技術，信號於空中傳輸過程，可以確保其傳輸安全，對於通信內容欲加以錄音或是監聽，需取得系統業者之同意，從系統機房掛線，或個人可於手機中安裝錄音軟體，錄下特定對象之通話內容。惟已有案例顯示，駭客藉由惡意程式，啟動手機麥克風或是監聽軟體，對於受害者進行非法之會議竊聽或是通話內容錄音。

行動裝置另提供無線 WiFi 網路介面，提供高速上網之能力，並可以在蜂巢式行動網路及無線 WiFi 網路，自動切換上網路由。

D.行動裝置基礎建設(Mobile Device Infrastructure)

行動裝置之普及，除了行動技術之提升外，主要也是因為雲端技術之所建構之基礎建設，使用戶得以在任何時間、任何地點、任何裝置上存取資料。

機關若擬利用行動裝置提供便民服務或是從事公務，亦需建置支援行動服務之基礎建設，包括：

a.虛擬私有網路(VPN)

基於傳輸安全的需求，虛擬私有網路可以提供有效的防護，以確保行動裝置與機關內部資源存取過程，不會揭露與不相關之第三者，原因在於行動裝置所存取之公眾網路，尤其是無線區域網路，可能是處於未加密的狀態。適用於機關內部員工使用或是特定之合作夥伴、合約商等。

b.身分識別管理(IAM)

當行動裝置欲從任何網路來存取機關內部資源，身分識別管理就變得很重要，傳統基於所知之帳號、通行碼驗證方法，已不足以應付外來之威脅，需強化基於所擁有之身分識別與鑑別機制，以憑證、一次性密碼、或是多因子認證等方法。

身分識別管理(IAM)基本概念與定義包括:認證(authentication)、授權(authorizaton)、稽核(auditing)，其支援業務的程序大致可以分成：

- 使用者管理。
- 認證管理。
- 授權管理。
- 存取管理。
- 資料管理與供應。
- 監測與稽核。

c.行動裝置管理(MDM)

行動裝置之設計，主要以供個人使用為主，並無群組授權、強制組態設定或是稽核記錄功能，故欲用之從事於公務使用，將會因之而衍生安全議題，例如裝置失竊後之資料清除，故資安產業遂發展行動裝置管理系統，藉由在行動裝置上安裝特定功能之 APPs，作為管理該行動裝置之媒介，強化對於行動裝置之管理。適用於行動裝置產權屬機關所有。

d.行動應用程式管理(MAM)

近年來因為將自己的裝置帶到工作場所(Bring Your Own Device;簡稱 BYOD)盛行，衍生出行動裝置的管理議題，因為裝置所有權屬個人所有，資訊擁有權屬機關所有，在管理上，機關僅有權對於機關所擁有之資訊進行管理與處分，故有行動應用程式管理之需求，以補強實務管理之需要。

e.行動應用程式商店(Mobile APPs Store, MAS)

行動 APPs 安裝，建議應從信任之來源下載，例如：作業系統廠商官方所提供之「公眾行動應用程式商店」。

除此之外，行動裝置製造商，亦可以透過韌體之封裝，或是安裝行動商店 APPs，例如：中華電信之「Hami APPs」，建置「外部行動應用程式商店」，提供給客戶下載之用。

若是行動 APPs 僅供機關內部所使用，則需透過經作業系統商認證之行動裝置管理系統(MDM)，建立機關專屬之行動應用程式商店。

f.行動應用程式閘道(Mobile APPlication Gateways)

行動應用程式閘道，多以軟體方式實作，主要是應用層的服務，類似 Proxy 的功能，提供過濾或是轉送網路流量至行動應用伺服主機。

必要時可以在 VPN 閘道與行動應用程式閘道之間，再建置入侵偵測、預防系統，或是資料洩漏防護系統，以避免外來之威脅，或是內部重要機敏資料的洩漏。

g.閘道及安全堆疊裝置(Gateway and Security Stack)

行動裝置具備有雙通道之網路介面(指 Cellurer 及 WiFi)，很容易作為攻擊其他網路裝置的平台，為了防範遭受污染的行動裝置，入侵機關內部網路，需要建置閘道及安全堆疊裝置，例如：應用程式防火牆等，進行內容過濾、封包過濾或是流量監察的功能。

同時也需要將相關之記錄資料，傳送給資安事件管理平台，進行資料關連性分析作業，以利事後稽核與查考，或作為事故鑑識之用，以彌補行動裝置本身紀錄資料之不足。

E.企業核心服務(Enterprise Core Services)

經由前述之閘道及安全堆疊裝置確認安全之後，行動裝置才可以存取機關內部之資源，使用語音(Voice over IP)、郵件、虛擬桌面、行動應用程式及資料庫等服務。

行動應用程式又區分為原生型行動程式(Native APP)及網頁應用程式(Web APP)，原生型應用程式主要意指，利用該平台官方建議的程式語言來開發應用程式，舉例來說：iOS 使用的是 Objective-C，而 Android 用的是 Java ，所以針對

不同的平台，需要不同的開發方式，可以強化對於行動裝置硬體的控制，例如：GPS 啟動或是推播功能等。但隨著 Html 5 語言的興起，其可以呈現的效果越來越佳，許多人不斷思考是否可否利用 Web 的跨平台性，來達到開發一次，而在所有平台上都可以利用的效果，所以延伸出來的，就是網頁應用程式的發展。

(3)聯邦行動運算安全基準

一個安全的基準是聯邦資訊系統與組織基於資訊系統的安全類別上，進行安全與隱私控制的最低限度之集合。該集合實現了各單位組織範圍內，資訊安全和隱私風險管理流程的一部分，並提供機構用一致性方法來管理組織風險及共同的方法來做安全評估、授權與連續監測。為此 NIST 在 SP800-53 第 4 版定義了資訊與資訊系統的安全控制的分類方式，並且為了減少對系統的影響，在聯邦雇員透過內部網路存取資訊與資訊系統的行動環境中，採用符合單位特定需求的基準，以加強行動運算在跨單位的應用。

一個加強安全的控制系統(指資訊受到全面的安全控制、強化控制管理與補充指引的集合)，適用於 NIST 或國家安全系統委員會(Committee on National Security Systems；CNSS)這類單位，訂製符合特定安全基準需求的最適化指引，依此發展一組能廣泛使用於運算模式的控制集合，例如:雲端運算或行動運算，讓相關的單位能依此進一步考量滿足單位任務需求的環境威脅、風險承受能力及選擇增加額外控制或改進控制的必要性。

(4)使用行動運算決策框架以選擇適當的行動架構方案

為了各單位對於移動性要求並選擇適當的行動架構，其中整

個參考體系架構包含一個決策框架，如下圖行動運算決策框架所示。該決策框架描述了和風險分析有關行動解決方案的業務決策優先順序，使各部會局評估行動風險解決方案時，作出明智決定的方法。

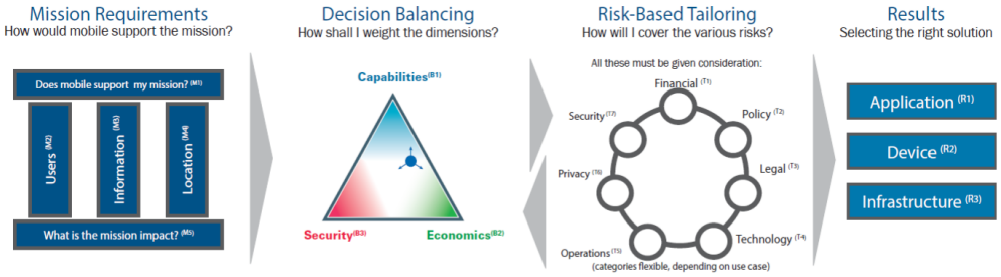


圖5　行動運算決策框架

(5)結論

數位政府策略(DGS)挑戰了各單位對於提供「在各種設備上，任何時點都能使用數位資訊服務」，而且「透過協調的方式，確保在數位時代資料的隱私和安全性」的因應能力。本次發布的行動安全基準和參考架構表示，聯邦政府的第一個階段在設立政府各部門之泛用標準和行動安全運算指引。透過導入行動安全基準和參考架構，各單位將能更容易對付行動裝置的各種弱點與威脅訂立策略，推行應用到單位的電腦運算環境中。

(二)國家標準技術研究院

美國國家標準技術研究院(National Institute of Standards and Technology，簡稱 NIST)，前身為國家標準局，是一家測量標準實驗室，屬於美國商務部的非監管機構。該機構對行動裝置所需之安全規範皆有制定相關指引。適用範圍橫跨所有資訊裝置與系統，垂直整合系統開發、營運、產品、評估與安全管理等，以下為所發佈的相關標準與相關說明。

1.NIST Special Publication 800-53 Rev 4

提供聯邦資訊系統與組織的安全和隱私控制目錄，以及選擇控制來保護組織的運營(包括任務、功能、形象及聲譽)，組織資產、個人及其他組織的一個過程，從對於民族或國家的威脅多樣化，包括惡意的網絡攻擊、自然災害、結構性故障及人為錯誤。該控制程序是可被依據需求所制訂，藉此實現組織範圍的過程管理資訊安全和隱私風險的一部分。該控制解決整個聯邦政府和關鍵基礎設施的安全性和保密性要求，從立法衍生行政命令、政策、指令、法規、標準和/或任務/業務需求多樣化。此外還介紹了如何制定專門的控制配套或覆(含)蓋於專為特定類型的任務/業務功能，技術或操作環境。最後，安全控制目錄，無論從功能的觀點來看(安全功能和機制提供的強度)和保證的觀點(實施可信賴的安全能力措施)地(位)址安全。基於這兩個安全功能和安全保證，以確保資訊技術產品和使用音響系統(sound systems)及安全工程學原理的產品，所建立之資訊系統是足以信賴的。

本文件提供更全面性的資訊安全和風險管理，基於提供組織廣泛且必要的需求，從環境根本上加強其資訊系統安全控制的深度，這些系統的運行，有利於系統在面對網絡攻擊等威脅更有彈性。此「構建正確」的策略加上對「連續監測」提供高層領導做出影響其關鍵任務和業務功能，並且不斷以風險考量為基礎的決策所不可或缺的即時資訊，作為管理組織並進行各種安全控制之依據。

2.NIST Special Publication 800-124 Rev 1

本標準提供了一些建議，用於確保特定類型的行動裝置(如智慧手機和平板電腦)達到安全目標：保密性、完整性及可用性。筆

記電腦將從本標準的範圍排除，因為用於筆記電腦的安全控制相較於智慧型手機、平板電腦和其他行動裝置是完全不同的類型。以最小的計算能力的行動裝置而言，例如智慧型手機和平板電腦，通常需要同時達到多種安全目標。為了實現這些目標，行動裝置應當固定以防止各種各樣的威脅。因為有限的安全選項和所面臨的威脅有限，也超出了範圍，因此集中的行動裝置管理技術被越來越多地使用作為一種解決方案。

本標準的目的是為了幫助企業集中管理行動裝置的安全性。因為是用最少的計算能力的行動裝置，提供建議、選擇、實施及使用集中管理技術，並解釋了固有的行動裝置使用的安全問題，並提供整個生命週期保護行動裝置的建議。所涵蓋的範圍包括安全組織所提供或並自帶裝置(帶上你自己的設備，BYOD)的行動裝置。其中，建議企業應實現以下原則，以提高他們的行動裝置的安全性。

- 企業應該制定行動裝置的安全政策。
- 企業應為了行動裝置和行動裝置存取的資源，進行制定系統化的威脅模型。
- 企業在佈署行動裝置時，應考慮各服務所能提供安全保護的優劣，並確定哪些服務需要為他們的環境所需要的，然後重新設計並獲得它們所必要服務的一個或多個解決方案。
- 企業應實施並在把解決方案實際投入應用前，完成該方案的先導測試。
- 企業在允許使用者存取之前，應該充分確保每個行動裝置的安全性。
- 企業應定期維護行動裝置的安全性。

3.NIST Special Publication 800-142

本標準介紹軟體開發過程的組合測試，並說明如何有效地使用此指引，降低開發成本、提升軟體有效性，藉由概念引導與模型方法，保障資訊系統及系統重要組成部份之安全性。標準中提供關於對軟體進行組合測試行為流程，並且包含一個教學文件。此文件導入了關鍵的概念和方法，以解釋如何用以產生組合測試(可在 NIST 網站 csrc.nist.gov/acts 取得所使用的軟體工具)，並進階的討論如使用軟體的正式模型來確定預期結果符合各組的測試輸入。

每個主題均個別針對成本和實際的部分加以說明，並且進一步闡述如何在各種限制上進行取捨，其中部份可能會影響到資源或資金。相關的題材可以藉由尋問計算機科學本科學生或工程師加以討論，其中包括一套廣泛引用了論文，以使得每個主題更深入說明。

其中組合測試是一種可以降低成本並提高軟體測試有效性的應用的方法。底層這種測試形式的重要觀點是，並非每一個參數有助於每一次失敗的改善，大部分故障是由相對較少的參數之間的相互作用引起的。由 NIST 和其他收集經驗數據表明，軟體故障是由只有幾個變數相互作用(6 個或更少)所觸發。這一發現具有檢測重要的意義，因為這表示參數的測試組合可以提供高效的故障檢測。

4.NIST Special Publication 800-164

為了加速產業導入安全防護的能力，以提供具備高度資訊安全信賴保證的產品，制定 NIST Special Publication 800-164 以定義行動裝置基本安全能力之需求。其目的在提供一個可被廣泛的應用於行動裝置上，並協助確保企業環境開放使用個人自帶設

備時，能有所依循的資訊安全技術基準。以促進企業與消費等級的行動裝置能實現關鍵的資訊安全特性。將行動裝置視為一群受信任的基礎元件(Roots of Trust)之集合，此集合提供應用程式介面與提供應用程式叫用基礎元件，以及策略執行引擎檢查裝置狀況並強制實施安全管制行為。

此外透過概念架構呈現並加以描述行各層架構之間彼此的關聯性，其中分為硬體、韌體、作業系統、應用程式及資訊內容，共五層。其中下圖 Notional Mobile Device Architecture 是此文件中所描述行動裝置架構的最佳說明。

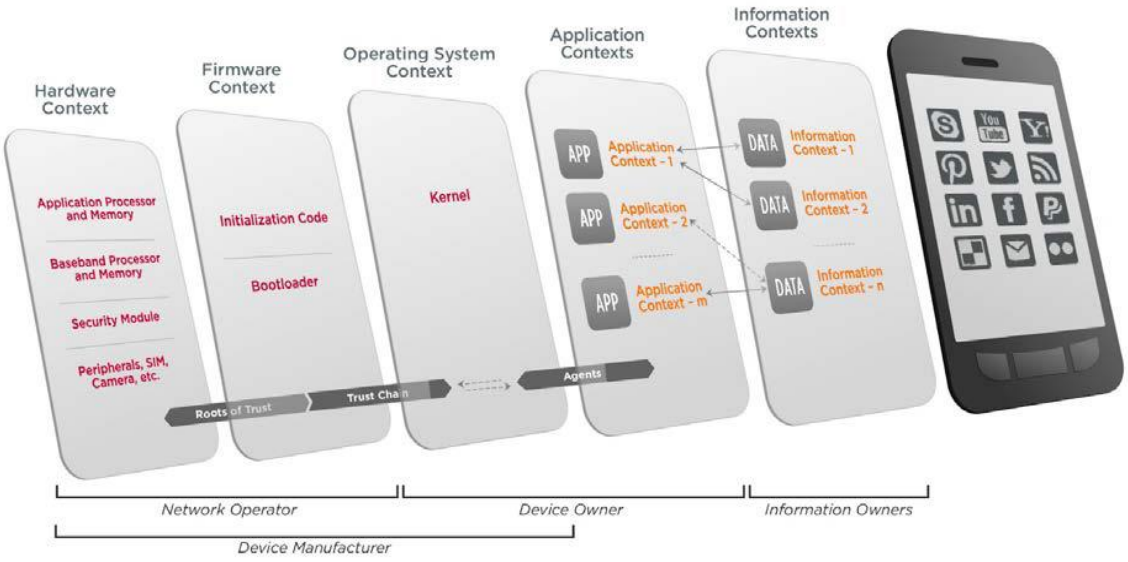


圖6　五層式行動裝置架構

資料來源：NIST

- 硬體：包含電池、行動通信單元、藍牙、NFC、攝影機、衛星定位晶片、重力、加速度、感應器、指北針及硬體可信任單元等。
- 韌體：包含初始化的硬體元件及作業系統。
- 作業系統：包含有作業核心單元、系統服務單元及組態設定

參數等。

- 應用程式：包含系統預載或是使用者自行安裝之應用程式，作業系統之核心會提供應用程式間相互隔離之機制。
- 資訊內容：包含應用程式運行所需之資料或是運行之後所產生之資訊。

最後，因目前大部分的行動裝置都不符合此要求。在以資訊安全為考量的前提下，需要相對應的安全規範以避免行動裝置衍生資訊安全的問題。故此文件要求未來所有移動式裝置都需要滿足下列三項功能，分別說明如下 ：

(1)裝置完整性(Device Integrity)

這是指在一個裝置中，不論軟體、硬體或韌體沒有任何的毀損。因此當某一個行動裝置可以被證明是持續維持在一個完整性的狀態，則此一狀態下的通訊機制是能夠被信任使用的。在此定義一個框架，使設備能依此評估本身的完整性，並且透過身分識別的建立、產生相關訊息並註冊、維護相關訊息、分享相關訊息、收集相關訊息、處理相關訊息等六個面向加以說明整個循環週期。

(2)隔離(Isolation)

用以避免同一裝置上的應用程式非故意的狀況下相互作用。藉由策略執行引擎與受信任的基礎元件能是當的保持不同處理程序之間，彼此訊息的流動存在著某種程度的隔離。

在此描述了六種實現基本的隔離功能的方式，分別為建立一個獨立的運作環境、以裝置完整性支援隔離之能力、妥善處理授權與資料共用通道、策略執行引擎需要有明確的策略模式、信任狀態的維護、信任狀態的撤銷控制與透過加密機制

進行資料隔離等。

(3)受保護儲存媒介(Protected Storage)

用以保護存放在裝置上資訊的機密性與完整性，當應用程式在非授權狀態下的試圖存取受保護的資料時，予以撤銷該存取之行為。由於受保護的儲存媒介通常很仰賴加密與完整性保護，因此多利用標準化的演算法保護資料與認證授權金鑰，而用戶端設備加密技術可參考 NIST SP800-111，關於靜態資料的加密則以 FIPS-140-2 標準為主。

此外應用程式的威脅需要透過裝置本身的信任儲存媒介元件提供保護。最後則是當裝置遺失後，系統需要能被選擇消除所有與使用者相關的訊息。為了有效保護所儲存的訊息，可以透過 FIPS-199, SP800-60, SP800-122 標準加強安全性。

其中加密機制的兩個基本組成為使用者金鑰與資料加密演算法，NIST 已經指定與認可了許多相關的標準演算法，適當的使用就能夠提供資料所需的保護。因此對於保護資料的基本要求則是透過金鑰建立、金鑰保護、遠端資料消除及資料生命週期等方面加以延伸其應用。

5.NIST Special Publication 800-163

此標準的目的是為了協助企業避免因員工將自己的裝置帶到工作場所(Bring Your Own Device, BYOD)享受效率的同時外，忽略了資訊安全導致的問題。因此發佈此文件主要是在幫助企業：

- 了解行動裝置應用程式安全的審核流程
- 計畫導入某個行動裝置應用程式的審核流程
- 開發行動裝置應用程式的安全要求

- 了解行動應用程式的弱點類型以及如何偵測
- 判定一個應用程式是否能被佈署在企業內部

藉由兩個對於應用程式主要的審批過程：應用程式的測試和應用程式核准/拒絕。此外應用程式的測試活動涉及到一個應用程式的測試軟體漏洞藉由服務、工具和人為推導漏洞並進行報告和風險評估。其中用以檢測應用程式的分析器，通常需要包含某些自動化工具針對應用程式進行弱點檢測，並產生報告。因此分析器可能需要包含 1.程式的正確性測試 2.應用程式的原始碼與二進制碼測試 3.針對原始碼與二進制碼進行動態或靜態程式分析 4.測試可以手動或自動化進行。

由於應用程式的原始碼通常無法從 google play 或 APP store 取得，因此**假設**可取得原始碼狀況下(eg., Open source)，就能夠使用各式工具加以分析，進而找出弱點並產生分析報告，這也就式進行程式碼審閱的主要目標。當原始碼無法取得時，可用二進制碼(byte-code or machine code)進行審核。

及於上述說明，在確認程式可正常被執行後，就可進入原始碼分析的程序，可透過靜態分析檢查原始碼與二進制碼是嘗試去推論在執行期間可能的行為，或(以及)進行動態分析，將成是實際執行並觀察其行為，由於動態分析無法提供絕對正確的結果，因此企業/組織在使用靜態或動態分析前，需先依據所訂定的目標加以權衡兩者的使用比例。

在自動化工具中，主要分成下列幾類：

- 模擬器
- 遠端裝置存取
- 自動化測試(包含使用者介面、界面切換時資料殘存狀況、

自動輸入、網路行為)

- 自動化進行重複的測試
- 靜態測試工具(包程式弱點的分析工具、開發過程的量測工具)

由於商用的自動化工具可能具有功能重複的現象，時間與成本也都需要納入考量，因此需要專業的審閱者去加以了解並將其量化。目前做法是透過審閱者讀取原始碼進行手動分析，即使有自動化工具也是處於輔助的角色，屬於勞力密集作業，可能可以透過建立大型資料庫簡化部份工作以及讓判定結果趨於一致，但無論是手動或自動化分析，都至少需要能產生對共同弱點進行共通化識別並標示(Common Weakness Enumeration (CWE) identifiers)以及使用泛用的專用術語表達。因此審閱者需要具備有應用程式安全方面的軟體開發以及特定領域的知識，為此企業/組織內須確保審閱者具備足夠的專業知識與技能。此外如果企業/組織打算自行開發，也應該參考安全程式開發的指引與軟體品質保證流程，以妥善處理整個軟體開發的生命週期。

應用程式核准/拒絕則是行動裝置依據這些分析與工具產生的報告和企業自行設定的風險評估準則，用以確定組織的安全要求和最終的佈署對組織其行動裝置行動裝置應用程式的批准或拒絕之一致性。因此在文件中將針對以下項次之內容進一步說明相關評估細節。

- 應用程式測試活動及其相關參與者。
- 測試過程中遭遇應用程式相關檔案安全的問題和提供建議。
- 一般應用程式對於安全的要求，其中包含防止未經授權的功能，保護敏感數據，並確保應用程序代碼的依賴關係。

- 發現的問題與提供建議是來自於使用的來源程式碼與二進制程式碼,靜態與動態分析和測試應用程式的自動化工具的對應處理。
- 發現的問題與提供建議是來自於共享的測試結果時的對應處理。
- Android 與 iOS 應用程式的漏洞。

為了進一步在不同行動裝置作業系統上，威脅行為與威脅的影響層面,此指引在附錄中特別針對 iOS 及 Android 系統各自可能面臨的威脅加以分類與定義威脅的影響層面，以引導讀者盡可能快速發現弱點，並依據弱點對應之型態盡快尋求適當之解決方案。

本計畫依據 SP 800-163 公告之相關技術細節，分析彙整如下以作為後續檢測項目編寫之參考。

(三)國土安全部

隸屬於美國國土安全部全國網路安全及通訊整合中心(National Cybersecurity and Communications Integration Center,簡稱 NCCIC)旗下的電腦緊急狀況備應小組(U. S. Computer Emergency Readiness Team,簡稱 US-CERT)，以引領並努力提高全國資訊安全態勢、協調網路訊息共享、主動介入管理網路風險之國家以保障美國的權益。

1.Cyber Threats to Mobile Phones

由於智慧型手機先天上安全防護能力不足，以及越來越多的人用來儲存個人敏感數據與相關活動，使得智慧型手機成為各式惡意程式攻擊的目標，為協助民眾所保護自己的智慧型手機免於受攻擊，因此發佈了此份文件提供民眾在選購與使用智慧型

手機時，選擇並應用適當的安全機制，使其資訊安全能夠受到充分的保護。

由於智慧型手機與電腦一樣都存在著系統或軟體的弱點甚至具備共通性，因此歸納出以下幾種可能衍生的攻擊型態：

- 因遺失造成資料失竊。相對而言，便於攜帶的智慧型手機也容易失竊，且相對脆弱的保護機制可能讓攻擊者有機可乘，取得儲存在智慧型手機內的金融或企業相關的機敏資訊。
- 任何人都可以開發 APPs 並上架，由於缺少適當的評價機制，因此許多看似合法的 APPs 仍暗藏危機。此外取得智慧型手機”Root”與”JB”使手機不受管制，也是問題的來源。
- 即使使用合法的智慧型手機 APP，也可能因為智慧型手機系統或 APP 本身存在弱點而被攻擊。惡意的攻擊者可以透過各種方式觸發該弱點，或智慧型手機系統服務已存在的運行弱點加以運用，而達到攻擊的作用。
- 網路釣魚攻擊，如同在個人電腦上的釣魚攻擊一般，藉由各種方法誘騙使用者安裝惡意 APPs，或藉此取得使用者的機敏資訊或進行電話詐騙。

基於上述的分析，建議採取下列措施，以減少遭受攻擊的機會與避免嚴重的後果。

- 藉由適當密碼的設定，使智慧型手機能夠更安全。
- 僅透過安全的連線(例如：SSL 或 HTTPS)傳送帳號資訊。
- 不任意點選來歷不明的郵件上之連結。
- 避免在公開網站上留下自己的電話號碼。

- 審慎考慮並盡量避免將重要資料儲存於智慧型手機上。
- 審慎選擇與安裝使用 APPs。
- 避免手機遺失，尤其是在公開或半公開場合。
- 藍牙、紅外線、無線網路介面，在不使用狀態下應關閉。
- 設定藍牙通訊為不可被搜尋模式。
- 避免連接來歷不明的無線基地台或公開場所的熱點服務。
- 當要把智慧型手機丟棄前，需要完全刪除手機上所儲存的資訊。
- 使用社群網路應用時應更加留心，避免留下不必要之資訊。
- 不要試圖對智慧型手機取得”Root”或進行”JB”。

(四)國防部

1.Commercial Mobile Device Implementation Plan

此備忘錄是提供商業行動裝置(Commercial Mobile Device ; CMD)分階段導入計畫，以做為促進在國防部內，發展與使用行動裝置在非戰略方面應用。由於行動技術被國防部參謀長會議認定是一項推動聯合部隊作戰行動的關鍵功能，行動技術的應用將進入全球一體化運作、安全與非安全通訊融合、便於攜帶、支援雲端指揮和控制能力，且未來將增加人們能夠合作並快速共享資訊的數量。此計畫建立框架並賦予使用者和行動方案管理者，以利用現有商用產品完善其功能、降低成本並提高個人生產力。

(1)願景

透過建立一個框架推動美國國防部訊息基礎設施來支持行動

設置的發展、制定行動設置的政策、推動行動裝置開發和國防部運用應用程式。目標是在於提供整個國防部一個成本管理流程。因此國防部參謀長會議的目標是發展全面的處理流程，一個集中的資料庫並讓行動應用程式可以快速開發、購買、認證並提供開發框架。

(2)方法

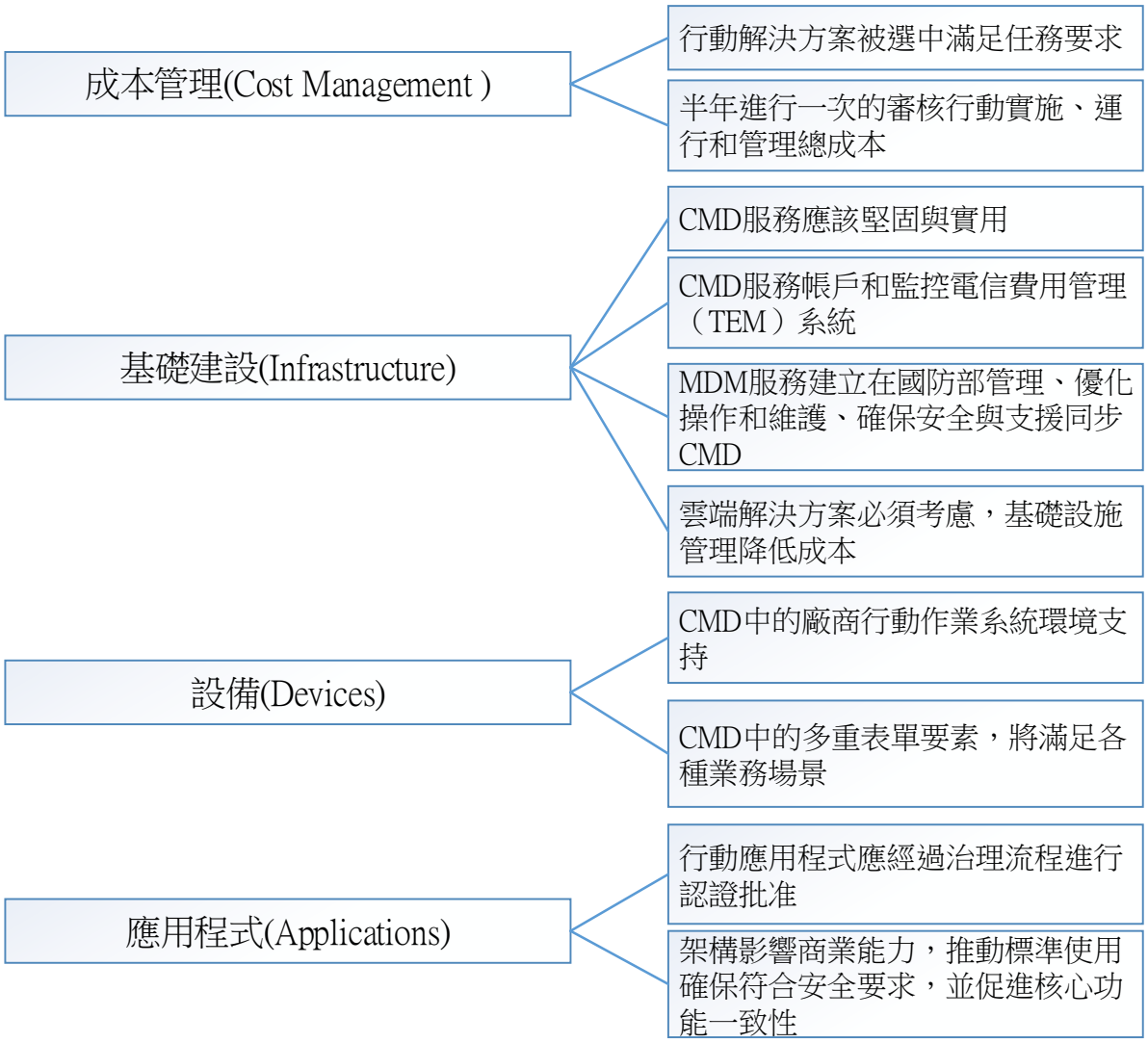
行動功能的實現是一個持續的過程，期間需要評估與分析商業案例指導，以確定開發解決方案的使命和成本效益。因此實施方法是透過 DISA、國防部元件(DoD Components)和總務管理局(General Services Administration，簡稱 GSA)提供採購和 CMD 操作。

(3)管理

根據國防部 CIO 執行委員會，元件/服務/機構(Components/Services/Agencies，簡稱 C / S/ A)將參與商業行動設備工作組(Commercial Mobile Device Working Group，簡稱 CMDWG)。該 CMDWG 將審查和批准標準、政策、行動解決方案流程和行動應用上的基礎管理。由 DISA 所建立的國防部行動計畫管理辦公室(Mobility Program Management Office，簡稱 PMO)，將提供安全保密和非保密的行動通訊能力。

(4)框架導入

以下為本計畫整理，當開始透過指引用來作為管理商業行動裝置的基礎建設、裝置與應用程式等，於框架導入之說明。


成本管理(Cost Management)
行動解決方案被選中滿足任務要求
半年進行一次的審核行動實施、運行和管理總成本
基礎建設(Infrastructure)
CMD服務應該堅固與實用
CMD服務帳戶和監控電信費用管理（TEM）系統
MDM服務建立在國防部管理、優化操作和維護、確保安全與支援同步CMD
雲端解決方案必須考慮，基礎設施管理降低成本
設備(Devices)
CMD中的廠商行動作業系統環境支持
CMD中的多重表單要素，將滿足各種業務場景
應用程式(Applications)
行動應用程式應經過治理流程進行認證批准
架構影響商業能力，推動標準使用確保符合安全要求，並促進核心功能一致性

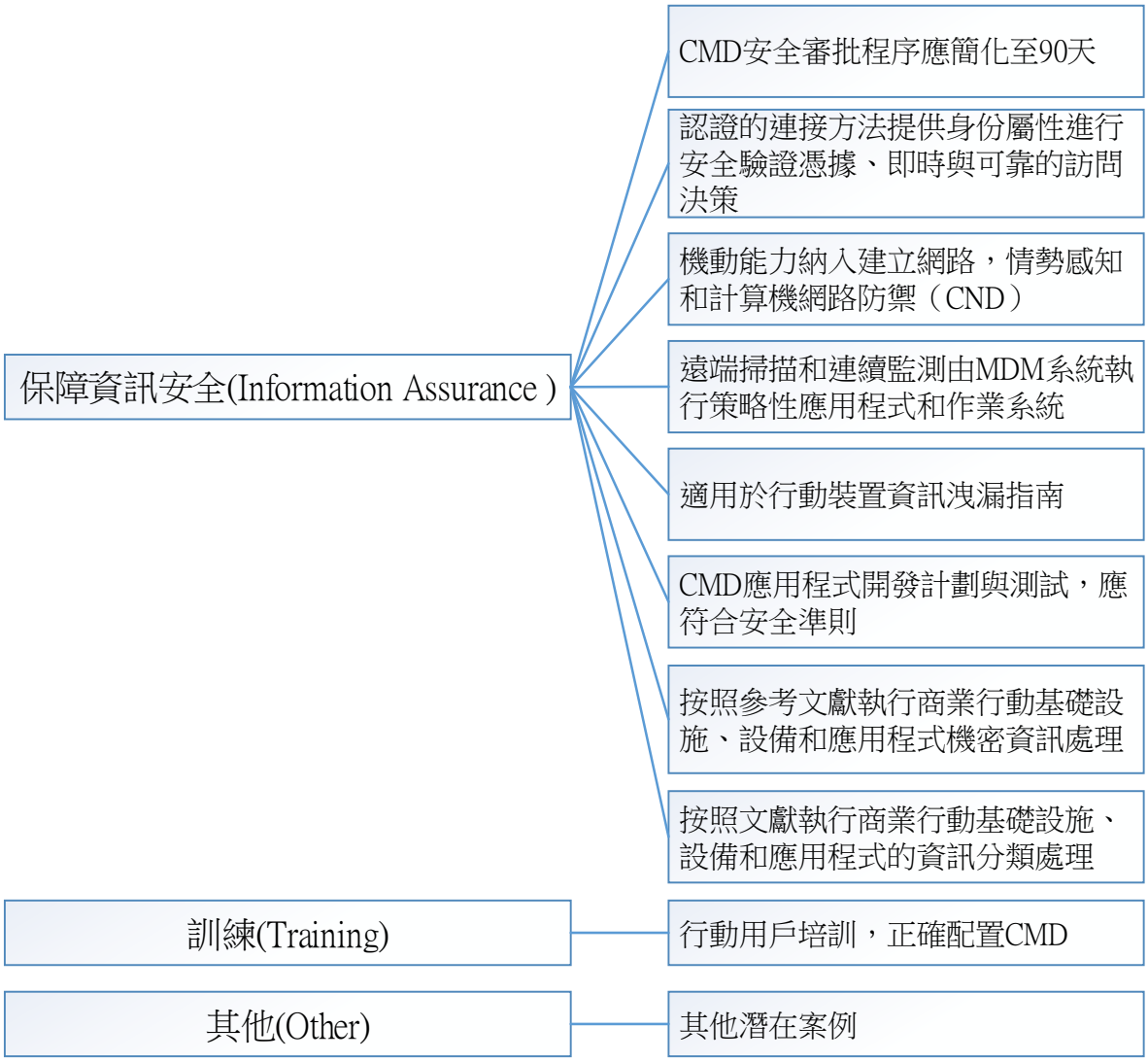


圖7　計畫實作框架

資料來源：本計畫彙整

2.Mobile Device Strategy

此份文件目的在希望能達成一個不受時空限制前提下，建立一個高度行動化的特定組織(此指國防部)，在此組織內能提供安全存取資訊與運算資源。考量國防部本身就是一個行動化的單位，此任務就是在避免來自各種型態之不利條件所造成的威脅。由於人員跨組織定期輪動，未來將有越來越多的遠端工作人員，透過行動化獲取資訊和運算能力可以提高資訊共享、溝通，並縮短行動反應時間導致更高的任務效率。手持式行動裝

置的高度成長與高滲透率，使其造成對人們生活的影響更為全面性，尤其在提升效率與資訊流通上。

從國防部戰略的角度來看，行動裝置有潛力為國防部各特定領域增強其能力。因此國防部將利用行動裝置發展資訊相關專案，並將其目標放在下列三點要項。

(1)推動發展國防部資訊基礎建設以支援行動裝置。

國防部與工業界和學術界合作，必須透過無線網路擴展、頻譜管理，並建立無線安全架構來推進移動基礎設施的能力。其作用在於：

A.頻譜管理

- 頻譜是有限的自然資源
- 行動裝置用戶不斷成長，頻譜管理流程帶來新負擔
- 迅速發展頻譜管理，其中包括流程與相關數據能力
- 研究技術發展頻譜最大利用率(如：動態頻譜接取、智慧天線、多重存取技術、頻譜共享技術)，並迅速制定過渡技術機制

B.擴大基礎設施支援無線功能

- 無線網路需要支援機密和非機密高頻寬流量，關鍵是無線覆蓋的建設及各種網路架構(例如：異質網路、載波聚合、移動 Ad-hoc 網絡、固定行動融合和自組織網路)
- 必須利用基礎設施與新興技術，並根據政策和標準使用商規現成電腦產品
- 整合電信費用管理解決方案，實現效率與蜂巢式網路通訊
- 國防部必須參與無線網路標準的機構制定標準
- 持續發展性 VPN 技術，確保關鍵任務行動應用

C.建立行動裝置安全架構

- 有效防堵越來越多的安全風險(如：病毒、垃圾郵件、蠕蟲或木馬)及其他新形式攻擊
- 商用無線網路和短距離網路必須減少其漏洞
- 開發無線安全架構，減輕行動裝置開發風險
- 架構啟用行動裝置、應用程式和網路連接管理，確保國防部網路和商業網路之間的接取
- 必須使用國防部公鑰基礎設施的安全性，訪問和識別網路、裝置和應用程式等級

(2)制訂行動裝置相關規範與標準。

行動裝置持續迅速成長為國防部尋求為員工提供行動技術優勢，但不受約束性也造成缺乏安全性和互用性的產品。先行探索互用性技術需要進行協調，確保安全性和互用性是一致的，並實現時間與資源的效率。國防部必須制定政策和標準，確保行動裝置的安全，並採取適當使用。這些政策和標準必須支援行動技術的移動性和動態特性，能夠及時部署並提供強大的管理和法規遵守驗證方法。

其作用在於：

A.發展國防部行動裝置政策與標準

- 商用行動裝置上執行作業系統，如：iOS、Android、RIM黑莓手機、Windows Phone，目標是利用一個或多個商業無線網路
- 商用行動裝置最具成本效益，但是只能搭載現成安全控制、接取協議並達到國防部要求必要的安全功能
- 制定政策和安全指導標準，採用商用行動裝置，並支援安

全性和互用作性要求一致與公開程序

- 簡化審查商用行動裝置流程，以便能及時部署不斷發展的技術與使用
- 探討使用個人行動裝置帶來的潛在安全風險

B.建立行動裝置管理服務

- 管理確保連續、安全的與低成本有效的方式操作與維護
- 行動裝置管理監控在行動運營商、服務供應商和企業部署的行動裝置
- 提供政策執行、完整性驗證、設備審查並視情況監控
- 建立聯合行動裝置管理服務、優化操作、維護、增強安全性、符合法規並支持裝置同步
- 規劃行動裝置訪問控制、加密、惡意軟體檢測、定期備份、定期掃描設備、安全更新、系統補丁及遠端執行/移除影響最小的行動裝置性能
- 必須採取連續監測技術，確保符合政策和國防部資訊保護

C.對行動裝置使用者進行教育與培訓

- 國防部人員必須意識到，國防部設備與日常使用行動裝置差異
- 許多重要安全控制實施，其中許多設定是由用戶，而不是一個安全策略服務器來控制
- 必須開發與評估符合終端用戶要求的程序
- 教育和培訓合理使用行動裝置和與工作有關的應用程式，如何正確設定用戶安全設定
- 整合廣泛行動裝置培訓納入適用現有人員的教育和培訓計畫

(3)推動發展與使用國防部核准的行動裝置應用程式與網頁應用程式。

行動應用程式(APP)提供最終用戶功能增強，測試和實驗證明國防部的移動應用程式提供潛在承諾。國防部行動應用程式主要吸引力是「低成本」，為作戰人員或技術支持人員發展更快、更簡單實用的功能。國防部必須促進開發和使用行動應用程式功能快速交付國防部的行動裝置用戶在一個安全與可互用的方式。國防部必須提供流程和工具，以便針對政策和標準的應用程式開發。

A.建立共同行動應用程式開發框架

- 行動應用程式開發框架包括開發工具、文檔與自動化流程，幫助構建和測試行動應用程式
- 建立共同行動應用程式開發框架，使其可以跨作業系統操作
- 框架必須利用商業能力、推動標準使用、確保符合安全要求並促進核心功能一致
- 應用測試標準、應用程式支援的作業系統平台、簽署開發應用程式與適當簽名密鑰

B.建立行動應用程式認證流程

- 確認應用程式安全簽章，確保惡意軟體和病毒沒有嵌入簽章後的應用程式，保證應用程式不受漏洞利用
- 驗證平台相容性與一致性能，強制執行共同格式進行數據交換
- 建立精簡認證過程按照政策支援行動應用程式快速部署
- 採用遠端掃描與連續監測，加強合法性和驗證應用程式和設備完整性

C.提供企業行動應用環境

- 行動應用環境提供集中託管、認證和審查程序、分配和管理服務
- 集中式應用環境促進國防部批准行動應用程式受到發現和利用，可能降低運營和維護多個應用程式託管環境相關成本
- 提高生命週期管理與應用程序的追踪
- 環境必須包括提交過程、開發過程、認證和審查流程、管理流程、符合規定流程、生命週期成本模型

D.「Web 功能」IT 能力支援行動裝置

- 行動辦公需求考慮當前和未來的 IT 功能與行動性
- IT 開發人員和服務供應商必須提供 web 功能在行動裝置產品上
- 顯示/呈現功能、用戶界面元素、『行動加值』技術(如：GPS、陀螺儀/加速計)

計畫初期將提供小型用戶群使用，並進一步評估策略的有效性。透過驗證提高生產效率與審查安全架構，以及藉由管理小部分用戶的商業案例，以作為未來開發支援企業級組織的解決方案。

3.Mobile Operating System Security Requirements Guide Ver1 R3

美國國防資訊系統局 (Defense Information Systems Agency; DISA) 為國防部 (Department of Defense, DoD) 內部機構發布安全需求指引 (Security Requirements Guides, SRG)以作為提升國防部資訊系統安全性的程序。在依據 SRG 所開發的安全性技術實作指南 (Security Technical Implementation Guides, STIG)，

所記載特定產品的原則、需求以及最佳設定作法實施。為了使行動裝置作業系統能依循 SRG 的安全規範，DISA 於 2012 年發布行動作業系統 SRG (Mobile Operating System SRG)，指定市售行動裝置若要部署到國防部 (DoD) 內應符合的安全需求。而各家行動裝置廠商能依據行動作業系統 SRG，撰寫符合之 STIG 並遞交審驗，一旦審驗通過，DoD 將允許採購此產品於內部使用。

安全需求指引(Security Requirements Guides; SRGs)是收集能應用到一個特定的技術族群之要求。藉此呈現一個介於控制關聯識別 (Control Correlation Identifiers, CCIs)與 安全技術實作指引 (Security Technical Implementation Guide, STIGs) 之間的步驟。

- 控制關聯識別 (Control Correlation Identifiers, CCIs)表示這些項目是離散的、可量測的與可實現行動的，其源自於政策中(e.g., DoDI 8500.2 and NIST SP800-53)所定義的資訊保證(Information Assurance ; IA) 控制。
- 安全技術實作指引 (Security Technical Implementation Guide; STIGs)提供具體的產品資訊以作為驗證，與取得該產品技術領域符合 SRG 的要求。

SRGs 有四個主要的核心內容，分別為：

- 應用程式
- 基礎網路架構
- 作業系統
- 資訊安全政策

每一個在該技術領域個內容，均定義適當的控制關聯識別(Control Correlation Identifiers, CCIs)。隸屬於這些 SRG 下技術發展的有更細緻的等級。因此本 Mobile OS SRG 是基於四個核心內容之一的 Operating Systems 而產生。其包含了一般性的檢查與應修補的資訊，可被用於未有安全技術實作指引(Security Technical Implementation Guide, STIGs)的產品，並將提供產品具體的技術實作導引。而安全技術實作指引則將提供涵蓋該產品具體的檢查與修補資訊。

依據 DoDI 8500.1 的要求，所有的資訊保證(Information Assurance, IA)與具備資訊保證功能的 IT 產品，納入 DoD information systems 將要被設定在符合 DoD 發佈的安全設定指南。

(五)聯邦通信委員會

聯邦通訊傳播委員會(Federal Communications Commission，簡稱 FCC)，是一個獨立的美國聯邦政府機構，並由國會領導。FCC 是依 1934 年美國國會法令所授權的聯邦傳播法案成立的聯邦機構，主要任務為規範所全美領土及領海的所有頻道管理業務以及傳播電信決策與執行，並負責規定所有的非聯邦政府機構的無線電頻譜使用(包括無線電和電視廣播)，美國國內州際通信(包括固定電話網，衛星通信和有線通信)和所有從美國發起或在美國終結的國際通信。

1.Ten Steps to Smartphone Security

由於逐年增加的行動網路犯罪攻擊事件，但多數智慧型裝置使用者缺乏對行動裝置安全威脅的抵禦能力，因此為了協助消費者保護行動裝置的安全，聯邦通訊傳播委員邀集國土安全部、國家超級電腦應用中心、聯邦貿易委員會..等公部門，以及黑莓

機、賽門鐵克、麥克菲…等公司，於 2012 年 12 月 18 日共同推出智慧手機安全檢查事項，透過線上工具與行動裝置作業系統的安全設定步驟教學，以協助消費者抵禦不斷增長的風險、病毒、惡意程式與行動裝置被盜/遺失所衍生的風險。基於上述所提，制訂出下列十項通用規則，以提升智慧型行動裝置的基本安全。

(1)設定 PIN 碼與手機密碼。

(2)不任意調整預設的手機安全設定。

(3)定期備份手機與雲端之資料於安全的本地端裝置，並於備份完成後刪除手機與雲端之資料。

(4)僅安裝來自可信任來源提供之 APPs。

(5)在允許安裝之前，了解 APPs 安裝時所要求的權限所可能衍生的風險。

(6)安裝能遠端定位智慧型裝置並刪除裝置上資料之 APPs。

(7)保持智慧型裝置的系統或軟體更新或修補程式為最新狀態，並允許修補。

(8)避免連接到不信任的無線網路熱點。

(9)在進行回收、出售、贈送舊有行動裝置前，應確實清除所有的資料。

(10)裝置被竊時應報案備查。

2.Ten Steps to Smartphone Security (Android)

聯邦通訊傳播委員會特別針對 Android 系統之行動裝置，依據前述所提十項規則輔以對應之操作連結(google)，以提升 Android

系統智慧型行動裝置的基本安全。

3.Ten Steps to Smartphone Security (iOS)

聯邦通訊傳播委員會特別針對 iOS 系統之行動裝置，依據前述所提十項規則輔以對應之操作連結(APPle)，以提升 iOS 系統智慧型行動裝置的基本安全。

4.Ten Steps to Smartphone Security (Windows Phone)

聯邦通訊傳播委員會特別針對 Windows Phone 系統之行動裝置，依據前述所提十項規則輔以對應之操作連結(Windows Phone)，以提升 Windows Phone 系統智慧型行動裝置的基本安全。

5.Ten Steps to Smartphone Security (BlackBerry)

聯邦通訊傳播委員會特別針對 BlackBerry 系統之行動裝置，依據前述所提十項規則輔以對應之操作連結(BlackBerry)，以提升 BlackBerry 系統智慧型行動裝置的基本安全。

(六)國家安全局

國家安全局(National Security Agency, 簡稱 NSA)是成立於五十年代初的組織，隸屬於國防部，依據法律它的責任是監聽與監察國外的各類諮詢，雖在成立之初係為軍事運用為主，後改組為聯合譯密與資訊安全服務部門，隸屬國防部，但在實際命令執行上，更趨近於直屬白宮之情治單位，而其監控範圍與能量更是遍布全球。主要管轄之下屬單位有，信號情報處(Signals Intelligence Directorate, SID) 負責情報收集、資訊保障處(Information Assurance Directorate, IAD)負責保護美國通訊系統、國家安全戰情中心(National Security Operations Center, NSOC)、網路威脅戰情中心(NSA/CSS Threat Operations Center, NTOC)及研究處(Research

Directorate)。

而美國國家資訊保證合作組織(The National Information Assurance Partnership；簡稱 NIAP)係由美國國家標準與技術院(National Institute of Standards and Technology，簡稱 NIST)及國家安全局(NSA)合作組成，為一個共通準則評估與驗證體制下的驗證機構，目前由國家安全局(NSA)所管理。

1.Mobility Security Guide v2.3

行動安全指引(Mobility Security Guide，簡稱 MSG)用於描述一個組織的安全行動裝置架構，透過安全分級的方法，將其應用於作為商用產品、服務、裝置、網路之分類，使行動使用者得以安全的連接到美國政府組織。為國家安全局(National Security Agency)的資訊安全保證部門(National Security Agency Information Assurance Directorate，簡稱 NSA/ IAD)所產出的指引標準。目的是為了讓技術與客戶高階需求能並駕齊驅，此外 NSA/ IAD 發展出一種方法與相關架構，使商業化的產品和服務能被適用於不同層級的解決方案。

美國政府使用此安全指引以建立各部門所擁有的行動式方案特色外，也必須出示一個解決方案，該方案除了提供該組織官方的授權委託(Delegated Authorizing Official，簡稱 DAO)，還必須遵守所有在使用、儲存與管理行動裝置，以及基礎建設元件的政策。此外美國政府的使用者還必須遵循現有且適當的認證與認可(Certification & Accreditation，簡稱 C&A)要求，這些要求將被使用於組織提供的 DAO 中，其中包含從將可接受的控制需求描述 (例如：NIST SP 800-53 第四版。)加入。此外，如果 MSG 與 DAO 因產品多樣性造成條文衝突，則應以 MSG 為優先。

此指引的目的在於秉持指引中的要求---行動化組織要能提供使

用者在不受時空限制的前提下，取得資料、服務與聯繫他人，以安全的完成任務。

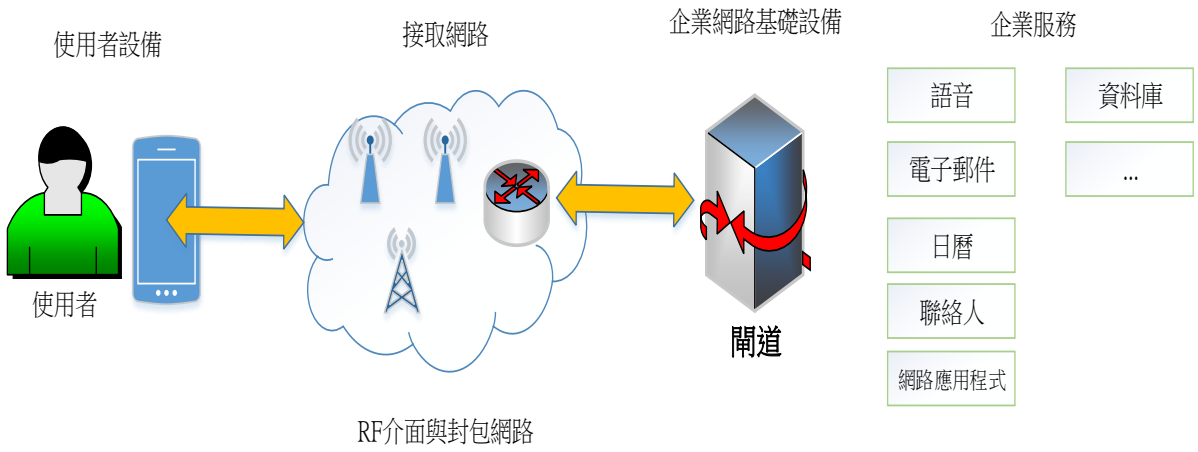


圖8　組成政府組織行動化架構的各個基本區塊

資料來源：NSA/IAD

(1)使用者設備

一般市售行動裝置在使用上需要考慮機密性，雖然能夠有效降低單位採購的成本，且永遠保持使用最新的技術，但迄今對於政府運作相關的安全考量仍未能完全獲得解決，因此需要透過政府的行動化基礎建設架構加以彌補以降低風險。為了要能完全的導入此指引，引用之機構需要完全遵守指引中所有的要求，其中包含國家信息安全保障合作組織(NIAP)指定的所有相關之保護剖繪，以及需要接受如 NIST 800-53 及更重要 NIST SP800-164 所提的要求。

(2)行動應用與服務

此部分將對於將會被使用者裝置所使用的應用與服務加以描述，首先使用者將可能需要透過兩種主要的加密驗證方法，以連接到政府組織網路，分別是 IPsec VPN 與應用程式本身的資料加密機制。以及所使用加密驗證方法需要符合 NIAP

所認可的保護剖繪。因此，不論在語音或資料的傳遞，廣泛的採用 IPSec VPN 在此指引中，以對於提供足夠的安全保護，此外針對應用程式或服務則採用 TLS 並運用適當的金鑰交換管理機制加強資料安全。

(3)網路的接取策略

在此強調以行動電話蜂巢通訊服務為主，政府組織行動基礎設施和商業蜂巢式網路之間的相互作用，蜂巢式網路包括使用無線接取網路(RAN)分碼多工接取網路-2000(CDMA-2000)、通用行動電話服務(UMTS)、高速封包接取(HSPA)/演進 HSPA(HSPA+)或長期演進技術(LTE)，其連接到封包核心網路。政府組織行動基礎設施幾乎無法控制運營商的行動電話服務，政府組織需進一步導入並整合在蜂巢式系統的專業知識，以了解系統工程問題、選項與權衡。

(4)行動化政府組織的基礎架構

行動化政府組織的資訊基礎建設主要是用於行動裝置在存取服務時，保護所提供的服務之安全。因此，本指引透過下列項目增加防禦縱深，以確保服務的安全無虞。

- 組織內網路與網路邊界防禦:藉由佈署防火牆與入侵偵測/防禦系統達成。
- 多層次的認證與加密保護:使用兩層式認證、加密與授權作因應。
- 行動應用服務:提供行動裝置存取使用。
- 行動閘道:管制使用者與組織內的資料交換。
- 預防與管理措施:適當的設定組織內資訊基礎建設，以提供

安全的作業環境。

(5)行動化之威脅、風險與如何降低造成之損害

由於使用蜂巢式網路行動裝置、語音和數據等服務，均含有若干風險待解，這些風險包括惡意或意外動機下被敵人或授權用戶進行操作，目前有許多方法能用以降低損害並減少行動裝置所導致的風險，並且其中大多數是透過組織內資訊基礎建設裝置之間相互搭配而成。尤其是組織內資訊基礎建設和現有功能提供了用戶設備和用戶流量強大的安全保護。

2.Security Requirements for Mobile Operating Systems v1.0 (NIAP)

現在行動裝置安全與傳統物理上的防護完全沒有關聯，不僅是無線通訊通道更容易遭到攻擊，由於裝置本身也希望可以進行更多用途與多功能而帶來新的安全挑戰。資訊保障處(Information Assurance Directorate)打算藉由擬訂第一代的行動裝置保護剖繪(Protection Profile，簡稱 PP) 以管理存在於行動裝置上的風險或弱點。所以此份 2013 年發佈於國家資訊保證合作組織 (National Information Assurance Partnership；NIAP)的共同準則(Common Criteria)之行動裝置保護剖繪，在於行動裝置使用者(在此指 IAD)依據共同準則(Common Criteria)之框架並透過 Protection Profiles (PPs)的使用，以具體描述他們對安全功能要求(SFRs)與安全保證要求(SARs)；而廠商依此 PP 實作他們所宣稱具有相關安全屬性的產品，主要是作為供應商生產智慧型裝置的一致性標準，依此製作供單位使用之智慧型裝置。因此共同準則(Common Criteria)的目標在於

- 確保評估的 IT 產品和保護剖繪(Protection Profile，簡稱 PP)的一致標準；
- 要增進評估的有效性、安全性更高的 IT 產品及保護剖繪；

- 消除重複評估 IT 產品和保護剖繪的負擔；
- 不斷提高評估和認證/驗證處理 IT 產品及保護剖繪的效率和成本效益。

(1)評估目標(Target of Evaluation；簡稱 TOE)之定義

現代的智慧型手機如同一部可隨手攜帶的微型電腦，但就安全性而言，智慧型手機本身設計與預設組態上卻存在不少潛在的弱點，從資訊安全的觀點來看，資訊安全的目的無非在於確保或提供私密性(Confidentiality)、完整性(Integrity)與可用性(Availability)、不可否認性(Non-Repudiation)等目標，因此評估目標的主要目的是驗證標地的完整性及一致性，並可以作為評估一個資訊產品的基礎。在這個原則範圍內，企業可以管理與控制一部分行動作業系統執行的工作空間。

(2)資訊安全問題描述

安全性問題將會被定義為符合評估目標(TOE)的威脅描述，而該評估目標通常就是指一個通用的行動裝置作業系統。在共通準則上所定義的風險是指在一個資產上執行有安全威脅程式所可能產生的危害行為。因此在這一個版本保護剖繪的對象是儲存為本地端(手機)儲存裝置內使用者驗證資訊與密鑰等內容，被用在對使用者驗證與確認驗證資訊與密鑰等內容更新符合需求，以此保護主要資產的安全。以避免攻擊者或惡意軟體藉由取得上述內容後，對企業內部網路發動攻擊。故此保護剖繪將依據上述準則，將問題描述如下：

- 遺失風險
- 網頁與網路攻擊
- 發送用戶資料到不相關的目的地

●惡意程式的威脅

●未經授權更新(Unauthorized Updates)

●不安全的工作區

●評估目標的安全功能失效

(3)對安全目的之定義

符合此規範的受評估目標，所提供的安全功能需要能對付威脅，且實現其安全政策是能由額外的法律或法規加以深化。以下將提供一個功能性的敘述，使先前討論的威脅能更為明確。此外安全功能也提供包含評估目標元件之間受保護的通訊、評估目標存取管理與設定功能、評估目標更新來源能夠被驗證。

●可驗證的更新

●安全儲存

●安全工作區

●評估標的管理

●殘留資料清除

●標的安全功能自我測試

(4)對安全要求之定義

共同準則(Common Criteria，簡稱 CC)就是被期許當成一個安全分析的利器，他提供許多適當的資訊產品的評鑑項目以及用來表示評估資訊安全要求的評鑑準則。這樣的準則更有助於跨廠商，跨國際的認證不僅節省廠商再次作認證的手續，也給予消費者一個通用的準則，來判斷所使用的產品是否合

乎自身要求。

三、歐盟

(一)歐盟網路資訊安全局

歐洲網路與資訊安全機構(European Network and Information Security Agency，簡稱 ENISA)，是由歐盟於 2004 年所成立的機構，目的是提高歐盟的網路和資訊安全，該機構具有發展網路資訊安全的使命，並有為公民、消費者、企業和公部門組織利益把關的責任。

1.Smartphone secure development guidelines for APP developers & Top Ten Smartphone Risks

此二份標準分別針對廠商(Smartphone secure development guidelines for APP developers)與使用者(Top Ten Smartphone Risks 文件參考到 Smartphones: Information security risks, opportunities and recommendations for users)提供自主性測試指引，作為歐盟地區行動裝置資訊安全評測之參考。藉由歸納出的 10 個重要的風險項目，引申出開發期間相對應的處理方式以消除常見的漏洞。對應處理策略概述如下：

- 識別與保護行動裝置上的機敏資料
- 安全的掌握行動裝置的密碼與識別
- 確認機敏資料在傳輸過程得以受到妥善保護
- 正確的實現使用者認證、授權與設備之間對話管理
- 維護應用程式界面與伺服器平台之間的安全機制
- 與第三方服務及應用程式之間良好的資料安全整合機制

- 用戶端的資料儲存與收集需特別關注並取得用戶認可
- 實現控制作為以避免未經授權的訪問
- 確保所有應用程式能被安全的發佈與安裝
- 詳細檢查所有運行過程中因程式錯誤所產生的代碼

(二)歐盟執行委員會

歐盟執行委員會(European Commission)是歐盟政治體系的執行機構，負責貫徹執行歐盟理事會和歐洲議會的決策。此外，委員會可以通過行使其主動權就法律規定、政策措施和項目提出建議。歐盟執行委員會是一個獨立於成員國的超國家機構，其委員效力於整個歐盟而不是各自的成員國。

1.Opinion 02/2013 on APPs on smart devices

為了向最終用戶提供嶄新和創新的服務，這些應用程式能夠從設備中獲取大量資訊(例如：用戶儲存在設備中的資訊以及不同感應器中的資訊，其中包括位置資訊)，並對這些資訊進行處理。然而，來源相同的資料還能夠被進一步處理，通常是透過一種用戶可能不知道或不希望的方式而提供了收入來源。但也因此沒有意識到資料保護要求的應用程式開發商可能會為智慧型裝置使用者的私人生活和名譽帶來重大的風險。在可能沒有得到最終用戶的有效同意前，資料已被進行處理；缺乏透明度，以及缺乏對處理類別的認知構成了最終用戶在資料保護方面的關鍵風險。拙劣的安全措施和彈性的收集目的助長了存在當前應用程式環境中的資料保護風險。從此觀點出發，此文件係歐洲聯盟第二十九條資料保護工作小組(ARTICLE 29 DATA PROTECTION WORKING PARTY)所訂，在此文件中闡明了在開發、經銷和使用智慧型裝置應用程式過程中處理個人資料時

所適用的法律框架，此框架著重於對同意的要求、目的限制和資料最簡化原則、採取充分安全措施的需要、正確地向最終用戶告知其權利和合理保存期的義務。

此外 API 還能夠提供與其他已安裝應用程式相關的資訊，並且通過一個或多個獨一識別碼來提供有關設備本身的資訊，而且這些透過 API 獲取的資料還能夠被用作進一步處理與應用，其中包括使用在惡意行為上。

本規範旨在闡明經銷和使用智慧型手機的應用程式進行個人資料的處理時適用的法律框架，以及在應用程式範圍外作進一步處理時適用的法律框架，此外對資料保護的主要風險作分析，描述所涉及的不同各方的各種法律責任，其中包括：應用程式開發商、應用程式擁有人、應用程式商店、作業系統和設備製造商(OS 和設備製造商)、以及其他可能參與從智慧型裝置中收集及處理個人資料的第三方，如分析和廣告的提供商。

本規範還著重對使用者同意的要求、目的限制和資料最簡化原則、採取充分安全措施的需要、正確地向最終用戶告知其權利和合理保存期的義務。此框架適用於各種不同的智慧型裝置，但尤其以智慧型手機中的應用程式為核心。

基於以上原則，此標準從下列兩個層面加以說明並引用相關法源佐證，彙整說明如下：

(1)資料保護風險

由於作業系統之間的密切互動使應用程式能夠比傳統網頁瀏覽器獲取更多的資料。應用程式能夠從設備中收集並處理大量的資料(如位置資訊、使用者儲存在設備中的資訊以及不同感應設備所取得的資訊)，以便向最終使用者提供新穎及創新的服務。單一的資料項目能夠即時地從設備中傳輸出去，然

後在世界各地進行處理，或者在鏈條式的第三方之間相互複製。缺乏透明度、在可能沒有得到最終用戶的有效同意前，資料已被進行處理，以及缺乏對處理資料類別的認知構成了最終用戶在資料保護方面的關鍵風險。基於上述資訊，將可能造成的風險歸納為下列四點項目：

- 缺乏透明度是資料保護面臨的高風險。
- 缺乏透明度與缺乏自由及知情的同意有密切的關係。
- 拙劣的安全措施可能會導致(敏感)個人資料在未經授權的情況下被處理。
- 對目的限制原則的無視(基於忽視或故意)，該原則規定個人資料的收集和處理只能基於特定且正當的目的。

(2)資料保護原則

資料保護指令是歐盟相關的法律框架。該指令適用於任何使用智慧型裝置中的應用程式處理個人資料的情況。為了明確適用法律，首先有必要明確所涉及的各方的身分角色，透過手機應用程式的處理識別出掌控者的身分，這對於適用法律的問題尤其重要。因此，涉及應用程式的開發、經銷和操作的任一方被視為是掌控者時，其有責任單獨或與其它方共同確保所有與資料保護指令相關規定確實被遵守。

在安全性方面，資料掌控者和處理者必須採取必要的組織和技術措施以確保其所處理的個人資料的安全。因此各方有必要根據各自的角色和職責採取對應措施。安全義務的遵守具有雙重目的。它使用戶更具自主性地對其資料進行嚴格的控制，並且提高了對其資料進行實際處理的實體的信任度。為了各自遵守作為資料掌控者承擔的安全義務，應用程式開發

商、應用程式商店、OS 和設備製造商和第三方必須考慮採用“從設計著手保護私隱”原則和“預設私隱”原則。這要求對現有的以及未來的資料保護風險不斷進行評估，且要求實施並評估有效的補救措施，包括資料最簡化。且在第三方基於其本身的目的收集並處理個人資料時，他們還必須使用上述安全功能和事項，其中最主要的是廣告商和分析提供商。這包括安全傳輸和加密存放裝置獨一的識別碼、應用程式使用者的獨一識別碼及其他個人資料。

四、中國大陸

(一)大陸工業和信息化部

1.移動智能終端安全能力技術要求(YD/T2407-2013)及移動智能終端安全能力測試方法(YD/T2408-2013)

大陸工業和信息化部(簡稱工信部)，是行業管理部門，主要是規劃、政策、標準，指導行業發展，但不干預企業生產經營活動。

對於手機安全因具備廣大內需市場，故制定國內行動裝置資訊安全基準法規，以作為要求遵循之目的。主要是促使企業通過穩固智能終端作業系統，加強預置應用軟體安全審查，來達到保護移動智能終端機安全目的，為此針對移動智能終端分別發佈了移動智能終端安全能力技術要求(YD/T 2407-2013)及移動智能終端安全能力測試方法(YD/T 2408-2013)兩份相互配套的遵循文件。

文件中將移動智能終端設備的測試方法與技術要求基於安全能力框架將其分為五大類，分別為硬體(未有具體測項)、作業系統、外圍接口、應用層安全目標與用戶端數據安全保護，據此加以定義適當的安全能力要求以及相對應之測試項目。

<table>
<tr><td colspan="2">应用层安全要求</td><td rowspan="3">用户数据保护安全能力</td></tr>
<tr><td>操作系统安全能力</td><td rowspan="2">外围接口安全能力</td></tr>
<tr><td>硬件安全能力</td></tr>
</table>

圖9　行動式智慧型終端安全能力框架

資料來源：大陸工業和信息化部

上述五大類要求分別制訂欲達成之安全目標說明如下：

(1)硬體安全目標

在晶片端保證移動通信終端內部儲存媒介與基本安全，以確保晶片內系統程序、終端參數、安全數據、用戶數據不會被竄改或非法存取。

(2)作業系統安全目標

目的在達到作業系統對於系統資源使用的監控、保護和提醒機制，確保涉及系統安全的行為都是在可監控的狀態下，且不會出現用戶在不知情的前提下某種行為被執行，或者用戶不可控制行為的執行。另外，操作系統還應保證本身的升級是受到控制的。

(3)外部界面安全目標

外部界面包含有線與無線兩種型式，主要是用以確保用戶對外界接與進行數據傳輸的過程，是可以被控制並告知使用者。

(4)應用層安全目標

目的在保證要安裝於移動智能終端之應用程式軟體可以識別來源，並且對於已經安裝的應用程式軟體可以進行敏感行為的控制。此外，要確保移動智能終端出廠預置的應用軟體不會對用戶權益造成損害並且產生危害網路的行為，例如:惡意

收費、未經授權狀況下對用戶資料進行刪除、修改或對外傳送用戶資料等行為。

(5)應用數據保護安全目標

目的在保證用戶資料能被安全的儲存，確保用戶資料不會被非法訪問、存取或竄改，並且能透過備份還原的機制保證用戶資料能完整恢復。

此外，在移動智能終端完成測試後將依據所達成之測試項目多寡，對該移動智能終端進行分等以提供廠商於包裝上標示安全級別與功能等級。

本計畫依據 YD/T 2408-2013 公告之相關技術細節，分析彙整如下以作為後續檢測項目編寫之參考。

五、英國

(一)英國通訊電子安全局

英國通訊電子安全局 (Communications-Electronics Security Group，簡稱 CESG)，為英國政府機關中負責訂定通訊安全的機構，確保產品符合安全標準及規範。該機構針對手機訂定較歐盟標準更嚴謹之指引與控制方法，並列出實作與對應之參考標準。此外亦提供民眾相關參考辦法。

1.End User Device Strategy: Security Framework & Controls

在 End User Device Strategy: Security Framework & Control 主要在說明安全框架最終用戶設備與使用於進行官方資料處理工作，並也一併定義用於官方和官方敏感資料的筆記型電腦管控。所選用的標準目標在優化技術、安全保證、低成本和複雜度、最小第三方軟體、良好的用戶體驗、更多競爭和選擇，針

對消費者和商品 IT 市場之改進。其使用範圍是中央政府部門機構和相關機構。更廣泛的公共部門機構將可以利用這個安全框架作為其更廣泛的遵守方面的公共服務網絡(PSN)代碼的一部分。此一安全框架的目標在於：

- 最大限度地利用原生安全功能，並盡可能避免第三方產品。
- 更妥善利用各地的數據和服務控制，而不是增加額外的複雜設備。
- 允許負擔更大的用戶的責任，以降低安全複雜性，保持用戶體驗。
- 日誌和審查紀錄優於預防和控制，以保持用戶體驗和靈活性。
- 發展單一且足以透過服務端進行識別與更多控制行為的規範，以用於存取政府機關資料包括敏感資料之保護。
- 提供明確且全面的安全要求，以擴大潛在供應商的市場，避免過於繁雜的規範安全性。
- 啟動風險管理和透過追蹤威脅與攻擊手法，藉此提出緩解措施作為進行安全控制。
- 藉由使用普遍和一致的方法使 IT 系統之間有更好的互用性，以確保官方資料之安全。

此外亦藉由提出一個高層次的安全體系結構，以說明用戶設備與公共服務之間的關係與特性，做為配置與架構環境之指引。

(二)英國資訊委員辦公室

英國資訊委員辦公室(Information Commissioner's Office;簡稱 ICO)是英國為維護公眾資訊權而設立之獨立政府機關，致力於提倡政

府資訊公開及個人資料與隱私保護，為英國 1998 年資料保護法(Data Protection Act 1998)之主管機關。

1.Personal information online small business checklist

英國資訊委員辦公室為了幫助網路上的中小企業，並確保他們能妥當的收集與處理客戶資料，提供此一列表作為企業在處理客戶資訊參考之用。

- 考慮確實的需要收集的客戶資訊。
- 資訊收集後之目的。
- 有基於法律義務保護客戶資料之安全。
- 如借助資訊外包處理廠商,則需要有書面合約以保障資訊安全。
- 發送廣告信應遵守法律規範。
- 委由第三方公司發送廣告信時，需有適當的告知。
- 停止收集不必要的資訊。
- 客戶有權要求存取屬於自己的資訊。
- 鼓勵客戶檢查定期檢查並更新資料。

(三)英國通訊傳播管理局

鑒於傳統通訊業的多頭分散管理體制已不足以因應電信、資訊、電視廣播產業的快速變遷所帶來的衝擊，英國於 2003 年 12 月成立英國通訊傳播管理局(Office of Communication；Ofcom)，以統一監督、管理該國資通訊產業。

2000 年 12 月，英國政府發表通訊政策白皮書《通訊新未來》(Communication White Paper：A New Future for Communication)，

提出成立 Ofcom 的構想；2001 年 6 月，關於成立 Ofcom 的法案提交到英國議會，並於 2002 年 3 月獲得通過，開始進入籌備階段。2003 年 7 月，英國議會通過《2003 年英國通訊法》(Communications Act 2003)，分為：Ofcom 的職權、網路業務和無線頻率、電視和電台業務、電視接收的許可、通訊市場的競爭、附則等六大部分，共 411 條。該法案取代了 1984 年英國電信法而成為英國電信管制的根本大法，也確立了 Ofcom 的法律地位，賦予該機構全面監管英國資訊及傳播領域的權利。

2004 年 1 月 1 日起，Ofcom 正式取代包括 Broadcasting Standards Commission(BSC)、Independent Television Commission(ITC)、Office of Telecommunications(Oftel) 、 Radio Authority 及 Radiocommunications Agency 共五個管理機構的全部職權，成為英國橫跨資訊、大眾傳播及通訊領域的唯一且獨立的監督管制機構。此機構被定位成英國通訊傳播產業的「管制者」，與我國 NCC 相同的是，身為獨立機關的 Ofcom 管制涵蓋結構、行為與內容品質的多元性，其主要核心價值為公民福祉，得依法執行權力維護並促進市場競爭以利廣大的公民消費者。就其立法宗旨而言，在必要之時，國家對於媒體的管制與介入是必要的。當重要媒介議題發生時，Ofcom 下轄的各部會應依照法律授權、以最低社會成本，透過公開透明並經過風險評估的方式執行管制。

1.Safer smart phones–keeping your device secure

英國通訊傳播管理局為了協助國人避免因遺失/遭竊或惡意程式所造成的威脅，並藉此確保智慧型行動裝置的安全，製作並發佈此指引，透過 9 項說明對國人進行宣導。相關內容如下。

(1)設定 PIN 碼與手機密碼。

(2)手機被盜用時應使用 IMEI 碼進行相應之通報，以維護個人權

益。

(3)不任意調整預設的手機安全設定。

(4)定期備份手機之資料於安全的本地端裝置，

(5)僅安裝來自可信任來源提供之 APPs。

(6)使用防毒軟體

(7)安裝能遠端定位智慧型裝置並刪除裝置上資料之 APPs。

(8)在進行回收、出售、贈送舊有行動裝置前，應確實清除所有的資料。

(9)保持智慧型裝置的系統或軟體更新或修補程式為最新狀態，並允許修補。

六、日本

(一)日本智慧型手機安全協會

日本智慧型手機安全協會(一般社団法人日本スマートフォンセキュリティ協会; 簡稱 JSSEC)，於 2011 年 5 月由業界成立之志願性組織，2012 年 4 月成為正式社團法人組織，以提昇智慧型手機的使用安全為目標。

1.Security Guideline for using Smart phones and Tablets

對於企業與組織資訊安全為前提下，提供企業或組織在導入智慧型手機(含 BYOD)時規劃，管理策略與安全管制參考。目的主要是當企業和組織需要在使用智慧手機作為基本營運需求，以有助於提高勞動生產率和創新的工作前提下，找出安全威脅和對策，並促進在工作場所安全地使用智慧手機的健全環境。

由作業系統廠商為他們自家產品的安全性功能進行標準化並實

作，但設備供應商和電信運營商在這方面是沒辦法有進行太多的處置。因此管理和控制對商業用途來說，智慧型手機仍然在一些方面中言之過早，並在有限措施的前提下要進行全面強加，這些問題將需要被考慮。此外，也有導致新舊裝置混合以及複雜頻繁的版本更新在管理上也需要進一步討論。

相對而言，因 PC 更加的標準化，這是個很難將智慧型手機強行加入 PC 的安全系統的問題點，因此各種對策需要從一個設備本身、網路、系統和服務的訪問，數據儲存的角度組合，與管理方面等詳加考量的。

由於智慧型裝置設備和作業系統將能繼續升級藉以得到更高的功能性並提高其使用能力。例如，一個額外的訂閱智慧型手機用戶可以使用雲端存取服務進行自動數據同步，但該服務不了解其性質可能造成個人資料洩漏，非法訪問和安全威脅。此外，損失可能由於網路的強大數據交換率變得更嚴重，並且電池通過 USB 線從 PC 充電也可能因此洩漏資料，實必須研究如何維護智慧型裝置使用之資訊安全。

有鑑於上述的考量，此份資料提出以下的 Use Case 作為未來發展相關策略的參考依據。分別為電話簿、手機通話、電子郵件、排程管理、瀏覽管理、網路連接、企業網路使用考量、企業使用雲端 SaaS 服務時的參考、應用程式使用、裝置基礎功能、儲存媒體與備份同步機制等，再逐一檢查企業的安全要求目標，並有選擇地使用和實施適合組織需求的對策，在使用智慧型手機與安全性的目的間取得平衡。

(二)資訊技術促進機構

資訊技術促進機構(Information-Technology Promotion Agency; 簡稱 IPA)為日本資訊技術政策之實施機關，負責推動資訊安全、軟

體可靠性和人才培育等事業。在日本的 IT 國家戰略的技術方面，從人力資源，經濟，貿易和工業管轄權部額外獨立的行政機構，目標在全面加強在日本軟體領域的競爭力。

1.10 Major Security Threats

此份報告主要用以介紹近年來資訊系統安全威脅，依據各領域匯集的意見所判定 10 大安全威脅委員，因此希望藉由此份報告，讓企業、組織與個人用戶都能充分認識/意識到目前面臨的威脅，以採取相對應的措施。以下將依次排序 10 個主要安全威脅之項目。

(1)利用使用者端安裝之軟體弱點進行攻擊

(2)對特定目標進行間諜攻擊

(3)針對智慧型裝置的惡意程式

(4)透過病毒遠端控制受病毒劫持個人電腦

(5)進行金錢詐騙的惡意軟體

(6)無法預期的系統斷線

(7)對具有大量資料的網站進行攻擊

(8)破解使用者密碼並盜用身分

(9)利用合法使用者從企業內部發動攻擊

(10)冒充銀行進行網路釣魚攻擊

並進一步預測未來可能排名迅速竄升的三大威脅，分別為：

(1)雲端服務所面臨的挑戰與風險

(2)對於民生基礎建設發動攻擊(例如:水利、輸配電)

(3)透過擴散式攻擊避開既有的安全防禦措施

七、新加坡

(一)新加坡金融管理局

1.Technology Risk Management Guidelines

新加坡金融管理局(Monetary Authority of Singapore，簡稱MAS)，是新加坡共和國行使中央銀行職能的政府機構，同時也是負責監控金融機構的主管部門。該機構針對手機安全從金融資訊安全角度全盤考量資訊安全需求並分析可能造成的風險與對應管理策略之指引。該準則是金融機構應當採用行業最佳實踐範例，以實現以下三點安全準則。

(1)建立健全和強大的技術風險管理框架

科技風險管理框架應建立在系統和一致的方式來管理技術風險。該框架應該包括以下屬性：

- 角色和責任管理中的技術風險
- 優先識別和資訊系統資產
- 識別和當前出現的威脅、風險和脆弱性影響及可能性的評估
- 適當的做法和控制，以降低風險
- 定期更新和監測風險，包括改變系統、環境或工作條件

(2)加強系統的安全性，可靠性，靈活性和可恢復性

(3)部署強大的身分驗證，以保護客戶數據，交易和系統。

該準則不影響也不應被視為金融機構欠缺對客戶標準的聲明。在適當情況下，考慮到他們從事各種活動和他們進行交易的市場，金融機構能自行調整這些準則，並且金融機構應

閱讀指導與相關監管相結合要求和行業標準，其中強調金融機構應該要充分認識整個系統中風險規模並強化防禦技術。他們也應該適當和穩健的風險管理系統，以及操作流程來管理這些風險。

八、韓國

(一)大韓民國廣播通信委員會

大韓民國廣播通信委員會(Korea Communications Commission，簡稱 KCC)是韓國有關通訊與廣播事務的最高主管機關，也是韓國總統直屬機關之一。其機構是仿照美國聯邦通訊委員會(FCC)的架構，除了研究、管理廣播、通訊、頻譜，也是建立相關政策的機構(2012/2 因應政府組織改組更名為科學與資訊科技未來規劃部(Ministry of Science, ICT & Future Planning，簡稱 MSIP)。

1.Comprehensive Plans for Smart Mobile Security

此文件為該機構於改組前公告對手機安全，提供英文版政策性說明與宣示作用文件。未來將以達成下列三個目標為前提，分別為：

(1)改善未來的移動服務基礎設施安全品質

(2)建立行動用戶隱私保護基礎

(3)建立行動資訊安全基礎

該機構並透過以下 10 項重點任務以達成上述目標：

(1)強化智慧手機與平板安全與建立環境安全應用程式的散佈，以識別惡意程序和加強無線網路安全管理。

(2)確保無線網路安全性與執行系統檢測，藉以掌握有線與無線網路入侵關聯。

(3)透過探索進行環境建立和宣傳移動辦公，與介紹給安全考慮案件示範推廣使用的移動辦公，準備推動行動雲計算標準之SLA 指導方針，並支持智能電視設備與內容安全解決方案的發展。

(4)強化保護措施的提供與管理職責，如個人信息加密，以提高行動服務的個人信息和位置信息的安全性，並促進實現應用程式隱私安全驗證系統和個人的定位信息。

(5)自我控制系統，通過分析新服務的 SPAM 風險和加強反垃圾郵件服務，如智能過濾，並盡量減少行動垃圾郵件數量。

(6)防止藉由行動裝置分發有害信息，將藉由促進發展應用程式商店監測系統，以阻斷行動應用有害信息散佈。

(7)加強對發展原生性安全技術支援，如低功耗且嚴謹的加密技術，終端和平台的保護，無線網絡保護和移動內容保護。

(8)建立大、小企業的安全性之間的雙贏環境，以形成手機安全市場的生態系統，支持商業化和新的安全技術轉移到私營部門，藉由建立“移動安全標準研究中心”租用全球化的手機安全等機制，促進核心人力資源的開發。

(9)加強國內和國際合作，以預防和處理事故手機，支持研究機構專門從事行動安全領域和促進擴大的行動裝置訊息安全文化。

(10)推動使用新的移動服務和智慧型設備，藉由組織「智慧型手機安全立法研究(暫定名)協會」完善法律體系以確保安全。

參、各國標準研析與比較

本計畫首先依據各標準發佈之目的，將其區分為下列幾種類型，各類型依據其強制性及影響範圍由高至低依序說明如下：

一、全國強制性之標準規範

國家政府以立法方式，由單位把關，強制要求規範所涵蓋之對象遵守，建立條列式的測試項目作為判定之依據。

目前中國大陸是唯一全國強制性規範實施的國家，對欲連上網路之行動裝置，要求需符合最高安全標準。

二、政府組織內部規範

基於保護國家安全的立場，針對一般的單位訂定通用的遵循規範，以及特定的單位針對其特殊性質予以強化之規範，後者通常使用在與國家安全相關之政府單位。

三、組織與企業指引

提供政府組織與企業內部在導入行動裝置與方案之參考，在以資訊安全為考量之前提，協助導入單位透過定義與評估風險、建立框架、參照現有 ISO 標準，以此建立安全的行動裝置作業環境。

四、使用者/開發者指引

提供一般使用者/開發者強化對於行動裝置使用或程式開發之參考，或，通常以宣導加強安全觀念並輔以簡易的操作設定或觀念說明。

五、風險評估

主要提供目前行動裝置安全問題之統計與客觀評估。通常被前述四項用來做為設計防禦重點的參考依據。

依據上述分類說明中，本計畫將所收集標準依據同質性加以分類並針對互異之處加以彙整說明如下。

表3　各國規範綜合研析比較表

編號	地區	發佈單位	相關發佈文件	類型	分類/分層	檢驗分級	簡述
1	國際組織	OWASP	1. OWASP Mobile Security Project - Top Ten Mobile Risks(2014)	風險評估	6 類威脅, 10 項弱點	無	藉由每年度收集之資料，分析相關行動裝置 APP 之風險與威脅。採用行動威脅模型研究方法，將可攜式裝置遭受的威脅分 6 類，並將 6 類依造成的衝擊之嚴重性定義出十大弱點。
2	美國	Federal CIO Council	1. Government Mobile and Wireless Security Baseline(2013/5)	組織與企業指引	4 類威脅(其中包含 2 類屬於基礎設施受到之威脅)	無	本指引用以協助政府的各部門局處，透過使用行動運算決策框架(MCDF)定訂出各自適當的安全相關要求與風險容忍指標，選擇出適合政府的各部門局處行動安全架構，以及應用行動安全基準在所定義的安全控制措施上。主要目標在於引導政府的各部門局處導入行動安全方案於各自的資訊安全作業程序，但本文件不能被用來取代其他用於保護聯邦訊息及資訊系統的強制性要求。
		NIST	1. SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations(2013/4)	組織與企業指引	3 種初始化控制等級, 4 種優先等級	無	以類似 ISO 27001 風險管控方式，聯邦資訊系統與組織在基於資訊系統的安全類別上，制訂安全與隱私控制的最低限度之集合。實現組織範圍內，資訊安全和隱私風險管理流程的一部分，並提供機構用一致性方法來管理組織風險及共

編號	地區	發佈單位	相關發佈文件	類型	分類/分層	檢驗分級	簡述
							同的方法來做安全評估、授權與連續監測，作為管理組織及各種安全控制之依據。
			2. SP-800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise(2013/6)	組織與企業指引	無	無	目的是為了幫助企業集中管理行動裝置的安全性。因為是用最少的計算能力的行動裝置，提供建議、選擇、實施和使用集中管理技術，並解釋了固有的行動裝置使用的安全問題，並提供整個生命週期保護行動裝置的建議。
			3. SP 800-142, Practical Combinatorial Testing(2010/10)	使用者/開發者指引	無	無	介紹軟體開發過程的組合測試，並說明如何有效地使用此指引，降低開發成本、提升軟體有效性，藉由概念引導與模型方法，保障資訊系統及系統重要組成部份之安全性。
			4. SP 800-164, DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices(2012/10)	組織與企業指引	使用者端裝置 5 層架構	無	為了加速產業導入安全防護的能力，以提供具備高度資訊安全信賴保證的產品，制定此指引以定義行動裝置基本安全能力之需求。其目的在協助企業環境開放使用個人自帶設備時，所依循的泛用行動裝置資訊安全技術基準。
			5. SP 800-163,Vetting the Security of Mobile APPlications (2015/1)	組織與企業指引	7 種威脅類別 4 類威脅	無	目的是為了協助企業避免因員工將自己的裝置帶到工作場所，忽略資訊安全導致的問題。因此發佈此文件主要是在幫助企業判定風險並建立審批流程。依據

編號	地區	發佈單位	相關發佈文件	類型	分類/分層	檢驗分級	簡述
					等級		自行定義的應用程式弱點進行分類與分級，且內容並不包含行動裝置硬體與網路行為的部分。
		DHS, US-CERT	1. Cyber Threats to Mobile Phones(2011)	使用者/開發者指引	無	無	提供民眾在選購與使用智慧型手機時，選擇並應用適當的安全機制，使其資訊安全能夠受到充分的保護。
		DoD	1. Commercial Mobile Device Implementation Plan(2013)	組織與企業指引	無	無	此備忘錄是提供商業行動裝置(CMD)分階段導入計畫，以做為促進在國防部內，發展與使用行動裝置在非戰略方面應用
			2. Mobile Device Strategy(2012)	組織與企業指引	無	無	目標在不受時空限制前提下，建立一個高度行動化的特定組織(此指國防部)，在此組織內能提供安全存取資訊與運算資源。
			3. Mobile Operating System Security Requirements Guide Version 1, Release 3 (2013/6)(DISA)	政府組織內部規範	無	無	美國國防資訊系統局(DISA)為國防部內部相關機構發布安全需求指南(SRG)以作為提升國防部資訊系統安全性的程序。在依據 SRG 需求所開發的安全性技術實作指南(STIG)則是用以記載特定產品的原則、需求以及最佳設定作法的實作方式。並經由描述性的方式提列要求，以及該要求對應能避免的風險。

編號	地區	發佈單位	相關發佈文件	類型	分類/分層	檢驗分級	簡述
		FCC	1. Ten Steps to Smartphone Security(2012/12)	使用者/開發者指引	無	無	透過線上工具與行動裝置作業系統的安全設定步驟教學，以協助消費者抵禦不斷增長的風險、病毒、惡意程式與行動裝置被盜/遺失所衍生的風險。
			2. Ten Steps to Smartphone Security (Android)(2012/12)		無	無	
			3. Ten Steps to Smartphone Security (iOS)(2012/12)		無	無	
			4. Ten Steps to Smartphone Security (Windows Phone)(2012/12)		無	無	
			5. Ten Steps to Smartphone Security (BlackBerry)(2012/12)		無	無	
		NSA	1. Mobility Security Guide v2.3(2013/11)	政府組織內部規範	無	無	行動安全指引(Mobility Security Guide，簡稱 MSG)用於描述一個組織的安全行動裝置架構，依據此架構劃分不同的安全範圍，將其應用於作為商用產品、服務、裝置、網路之分類，使行動使用者得以安全的連接到美國政府組織。並要求符合 NIST 800-53、NIST 800-164 與 Security Requirements for Mobile Operating Systems。

編號	地區	發佈單位	相關發佈文件	類型	分類/分層	檢驗分級	簡述
			2. Security Requirements for Mobile Operating Systems v1.0 (2013/1) (NIAP)	政府組織內部規範	無	依據 ISO 15408 安全評估共通準則(Common Criteria)之分級標準	藉由擬訂行動裝置保護剖繪(Protection Profile) 以管理存在於行動裝置上的風險或弱點。IA 透過 PP 具體描述他們對安全功能要求(SFRs)與安全保證要求(SARs)；而廠商依此 PP 實作他們所宣稱具有相關安全屬性的產品，主要是作為供應商生產智慧型裝置的一致性標準，依此製作供單位使用之智慧型裝置。
3	歐盟	ENISA	1. Smartphone secure development guidelines for APP developers(2011/11)	使用者/開發者指引	無	無	提供廠商自主性測試指引
			2. Top Ten Smartphone Risks(2014)	使用者/開發者指引	無	無	提供使用者自主性測試指引
		EC	1. Opinion 02/2013 on APPs on smart devices(2013/02)	使用者/開發者指引	無	無	在此文件中說明了在開發、經銷和使用智慧型裝置應用程式過程中處理個人資料時所適用的法律框架，此框架著重於對同意的要求、目的限制和資料最簡化原則、採取充分安全措施的需要、正確地向最終用戶告知其權利和合理保存期的義務。

編號	地區	發佈單位	相關發佈文件	類型	分類/分層	檢驗分級	簡述
4	中國	工業和資訊化部	1. YD/T 2407-2013 移動智能終端機安全能力技術要求(2013/4)	全國強制性之標準規範	使用者端裝置 5 層架構	5 級安全能力，5 級安全功能	因具備廣大內需市場，故制定硬性國內行動裝置資訊安全基準法規，以作為要求遵循之目的。主要是促使企業通過穩固智能終端作業系統，加強預置應用軟體安全審查，來達到保護移動智能終端機安全目的與 YD/T 2408-2013 是為相互配套的遵循文件。欲上網之行動裝置需通過最高等級之審驗。
			2. YD/T2408-2013 移動智能終端機安全能力測試方法(2013/4)		無	無	條列各項安全測試方法
5	英國	CESG	1. End User Device Strategy: Security Framework & Controls(2013/2) (ERG)	政府組織內部規範	12 項安全控制領域	無	針對用於政府官方與接觸官方敏感資訊之筆記電腦，這類使用標準作業系統之行動裝置所制訂；而使用簡易型作業系統之智慧型手機與平板未來亦極有可能適用此標準。並採用既有之國際標準提供最佳化安全保證。
		ICO	1. Personal information online small business checklist	使用者/開發者指引	無	無	為了幫助網路上的中小企業，並確保他們能妥當的收集與處理客戶資料，提供此一列表作為企業在處理客戶資訊參考之用。
		Ofcom	1. Safer smartphones–keeping your device secure(2013/10)	使用者/開發者指引	無	無	為了協助國人避免因遺失/遭竊或惡意程式所造成的威脅，並藉此確保智慧型行動裝置的安全，製作並發佈此指引，

編號	地區	發佈單位	相關發佈文件	類型	分類/分層	檢驗分級	簡述
							透過 9 項說明對國人進行宣導。
6	日本	JSSEC	1. Security Guideline for using Smartphones and Tablets(2011/12)	使用者/開發者指引	無	無	行動裝置提供更多的便利與業務效率，也因此研究如何使用連續的對策加以維護資訊安全將會是必需被考量的。JESSEC 提出以 Use Case 方式作為未來發展相關策略的參考依據，以滿足企業的安全要求之目標。
		IPA	1. 10 Major Security Threats (2013/3)	風險評估	無	無	10 大安全威脅委員會，依據各領域匯集的意見所匯集之報告，讓企業、組織與個人用戶都能充分認識/意識到目前面臨的威脅，以採取相對應的措施。
7	新加坡	MAS	1. Technology Risk Management Guidelines(2013/6)	組織與企業指引	無	無	該機構針對手機安全從金融資訊安全角度全盤考量資訊安全需求並分析可能造成的風險與對應管理策略之指引。
8	韓國	KCC	1. KCC announces 'Comprehensive Plans for Smart Mobile Security'(2010/12)	使用者/開發者指引	無	無	此文件為該機構對於手機安全，所提供之政策宣示之文件。

資料來源：本計畫整理

此外，本計畫也將目前唯一具有智慧型行動裝置檢測項目細節之中國標準與 OWASP 提列之風險項目，依據 YD/T 2407-2013 使用者端裝置類別差異進行對應，相關分析比較結果如下。

表4　OWASP 與 YD/T 2407-2013 分類對應表

對應標準 使用者端類別 (YD/T 2407-2013)	OWASP Mobile Security Project - Top Ten Mobile Risks	YD/T 2407-2013 移動智能終端機安全能力技術要求
硬體安全	**M2:** 不安全的資料儲存 **M4**: 非故意或意外造成的資料外洩 **M5**: 粗糙的授權與認證 **M6**: 加密失效	確保手機內基頻晶片與記憶體晶片的安全，確保晶片內系統程式、手機內參數、安全數據、及用戶數據不被竄改或非法取得。如手機硬體具遠端遙控功能時，手機應保護遠端遙控功能，以防止遠端遙控功能被惡意利用。(安全能力測試項目: 1)
操作系統		確保作業系統行為均於受控狀態，不會出現在使用者不知情或不可控制的情況下，執行某種行為。如應用軟體使用定位、通話錄音、一般錄音、拍照、錄影或使用者資料存取時，作業系統應主動告知使用者，及讓使用者選擇確認或取消。另作業系統應保證其版本升級是受控制的。 (安全能力測試項目: 2~21)
外圍接口	**M3:** 傳輸層保護不足 **M6**: 加密失效 **M9**: 不適當的會話	週邊介面包含有線及無線介面。週邊介面的安全目標是確保週邊介面的連接及資料傳輸，應告知使用者和可受使用者控制。如啟動無線連結(藍

對應標準 使用者端類別 (YD/T 2407-2013)	OWASP Mobile Security Project - Top Ten Mobile Risks	YD/T 2407-2013 移動智能終端機安全能力技術要求
	處理	芽、NFC)或有線連結(USB)，作業系統應主動告知使用者，及讓使用者選擇確認或取消。 (安全能力測試項目: 22~27)
應用層	**M1:** 脆弱的伺服器端控制 **M4**: 非故意或意外造成的資料外洩 **M5**: 粗糙的授權與認證 **M8**: 安全決策是經由不受信任的輸入 **M10**: 封裝檔案保護不足	保證手機能對安裝之應用軟體進行來源識別，及對已安裝在手機上的應用軟體控制敏感行為。另須確保手機系統內建軟體無損害使用者權益及危害網路安全行為，例如:惡意收費、未經授權修改、刪除或對外傳輸使用者資料等行為。 (安全能力測試項目: 28~36)
用戶數據	**M2:** 不安全的資料儲存 **M7:** 客戶端注入	確保使用者資料安全儲存、不被非法存取、不被非法讀取、不被非法竄改，同時能以備份機制確保使用者資料恢復可靠性。如智慧型手機須可設定開機及螢幕保護時解鎖功能，及使用者資料權限控制、儲存加密、完全刪除、遺失時遠端遙控清除及備份功能。(安全能力測試項目:37~42)

資料來源：本計畫整理

最後，本計畫依據國際組織與各國規範所公告之相關技術細節，進行深入的研究分析並彙整如下，以作為後續檢測項目撰擬之參考。

表5　國際組織與各國規範所公告之相關技術細節彙整對應表

類別	技術細節內容
資料授權、儲存與保護	● **OWASP Mobile Top 10 Risk** ➢ M2:應避免使用 NSUserDefaults 的儲存敏感資訊，例如:避免使用 NSManagedObject 所有資料將儲存在未加密的資料庫文件中。 ➢ M2:機密資訊的儲存或暫存有必要考慮使用一個標準的加密函式庫，如 CommonCrypto。但對於特殊敏感的資訊應用，則可考慮使用白箱加密，以避免數位簽名在通用加密函式庫中被找到而造成洩漏。 ➢ M2:Android 可用“setStorageEncryption”以強制加密本地端文件的儲存。而對於 SD 卡儲存某些安全函式可以透過 javax.crypto 中的函式庫實現。 ➢ M2:儲存敏感訊息時，完全依賴於編碼加密或解密密鑰，應考慮提供操作系統預設加密機制外的附加加密。 ➢ M5:當行動裝置軟體之資料需要從行動裝置匯出時，則該資料需要用使用者金鑰進行加密，以確保僅持正確金鑰者方可存取該資料。 ● **NIST SP 800-164** ➢ 受保護的儲存裝置：保護儲存在設備上資料的機密性和完整性，並當使用中的資料發生未授權的應用程式試圖存取被保護的項目時，應撤銷其存取權限。 ➢ 避免當行動裝置遭竊而導致機敏資料洩露，需要有足夠強健的 Data at Rest (DAR)機制，可參考下列標準：

類別	技術細節內容
	• NIST SP 800-111 敘述有關環境風險和注意事項兩大類設備的資訊、儲存加密技術為終端使用者設備參考指南。 • FIPS-140 敘述有關 DAR 加密保護機制之標準，並保證使用標準化和普遍接受的機制進行加密操作，以及完成獨立的驗證。 • FIPS-199 為了有效的應用基於策略的受保護的儲存媒體，資訊的所有者需要明確定義出資料的保護需求和政策。其中資訊將被進行機密等級分類，並依據使用分類的標準作為處理的依據。 • NIST SP800-60 用以協助對應資訊安全類別，關於醫療資訊、財務或個人資訊之保護，則可進一步參考 NIST SP800-122。 ➢ 加密機制的強健性由加密演算法與密鑰長度所共構，可參考下列標準： • NIST SP800-133 密鑰的生成的準則。 • NIST SP800-90A 建議透過使用確定性隨機變數產生器，來產生具有足夠熵值的隨機變數以提升安全強度。 • NIST SP800-132 建議提供密鑰導出函數，並可用於推導從密碼密鑰對資料加密之密鑰或密鑰的保護的準則。 • ISO / IEC11889 提供重點服務保護加載密鑰用於確保機密性和完整性。此服務可以實現為一個純粹基於軟體服務或與硬體支援的可信平台模組。 • NIST SP800-88rev1，提供媒體清除原則，確立了

類別	技術細節內容
	消除數據的三種方法，以提供不同級別的保護。 ● **NIST SP 800-163** ➢ 啟用已獲得使用者授權功能：應用程式必須描述所有工作、按鈕，選項和其他介面連接所必需的作業並得到使用者確認。 ➢ 避免啟用未授權功能：權限可能透過隱式授予，使應用程式能在未經使用者同意的前提下，擅自使用相關功能。 ➢ 限制權限：應用程式應該只有最小的必要權限，且應避免與使用者授權聲明不一致。需要被加以考量應用程式所獲取權限的如下： • File input/output (I/O) and removable storage • Privileged commands • APIs ➢ 測試應用程式更新：應用程式的新版本都必須經過測試，以確定任何可能產生的新弱點。 ➢ 避免應用程式共謀：避免應用程式可能透過彼此之間的資訊交換，而獲得原本未被使用者授權資料之取得。 ➢ 保護敏感資料：應導入被證明足夠強健的加密機制(參考經 FIPS 140-2 驗證核可之加密機制)，以保護所蒐集/儲存/傳輸敏感資料的機密性和完整性。在隱私處理時也需要被考慮如位置數據、車載攝影照片，及設備身分的應用程式等，也需要被加以保護避免洩露。 ● **YD/T 2408-2013** ➢ 4.6.3 用戶資料的加密儲存：未經授權的軟體無法存取加密儲存區之電話簿資料。

類別	技術細節內容
	➢ 4.6.5.1 用戶資料遠端鎖定：受測之行動裝置經鎖定後，在尚未解鎖前，行動裝置持有者無法進行操作。 ➢ 4.6.5.2 用戶資料遠端刪除：受測之行動裝置資料經刪除後，用戶資料無法再被讀取。 ➢ 4.6.6.1 用戶資料的本地備份：透過備份功能進行使用者電話簿、簡訊、多媒體簡訊、郵件與多媒體資料之備份，並產生相關提示。
傳輸協定與保護	● **OWASP Mobile Top 10 Risk** ➢ M2:強制用戶使用標準的 Web API 或登錄方案（通過 HTTPS）進行身分驗證。 ➢ M2：應用程式可應用 SSL / TLS 傳輸機敏資訊，網路會談層或其他敏感數據傳輸到後端 API 或 Web 服務通道之加密保護。 ➢ M3：考慮未來安全弱點發生在 SSL 執行發現的情況下，額外提供數據加密將提供資料保密有效的二次防禦。較新的威脅允許攻擊者在資料通過行動裝置 SSL 庫加密之前截取行動裝置內傳輸中的敏感資訊，並竊聽網路流量後發送到目標伺服器。 ➢ M3:使用 SSL/TLS 傳輸時，應避免網路會談層的混雜，進而造成使用者 session ID 的洩露。 ➢ M6:不應使用被證明有明顯弱點的演算法與通訊協定，例如:RC2, MD4, MD5, SHA1。 ● **NIST SP 800-164** ➢ 透過建立身分，產生連線、維護、共享、蒐集、宣告及處理六個方面已完成整個管理的生命週期。 ➢ 發出服務請求的一方，應對遠端的裝置進行評估，並

類別	技術細節內容
	參與設備上的軟體所使用的通訊協定，以保證機密性、完整性及簽章的正確性，並完成設備驗證。 ● **NIST SP 800-163** ➢ 未加密通訊：當應用程式之間進行內部通訊，則將可能讓應用程式收集額外資訊，並注入惡意資訊。而當使用在對外通訊時(Data network, Wi-Fi, Bluetooth, NFC, etc.)則可能招致中間人攻擊之威脅。 ● **YD/T 2408-2013** ➢ 4.4.1.1.1 藍牙接口開啟/關閉之開關 ➢ 4.4.1.1.2 藍牙接口開啟之受控機制 ➢ 4.4.1.1.3 NFC 接口開啟/關閉之開關 ➢ 4.4.1.1.4 NFC 接口開啟之受控機制 ➢ 4.4.1.2 藍牙配對連接的受控機制 ➢ 4.4.1.3.1 藍牙接口連接狀態顯示 ➢ 4.4.1.3.2 NFC 接口連接提示 ➢ 4.4.1.4.1 藍牙接口數據傳輸受控機制 ➢ 4.4.1.4.2 NFC 接口數據傳輸受控機制 ➢ 4.4.2.1 有線外圍接口連接建立確認機制:在未發出提示，並獲得使用者授權之前，行動裝置資料無法被存取，僅能進入充電模式。
應用程式執行與安全	● **OWASP Mobile Top 10 Risk** ➢ M5：確保所有身分驗證請求都需要在伺服器端進行。一旦驗證成功，資料將被載入到行動裝置。以確保資料只在認證成功後才可使用。 ➢ M5：如果需要的數據的客戶端儲存時，資料將需要被安全地從使用者之登錄憑證所得之加密密鑰進行加

類別	技術細節內容
	密。 ➢ M2：資料庫應考慮使用 SQLcipher 進行資料加密 ➢ M2：對於存儲在 keychain 的項目應利用安全的 API 加以保護。 ➢ M3：使用受信任的 CA 提供商簽署的證書及要求 SSL 驗證程序的完整。避免使用自簽憑證，作為安全應用程序的一部分 ➢ M3：唯有在確認金鑰使用受信任且有效憑證，並且與伺服器的確認身分後才可建立安全連線。 ➢ M3：在 Android 系統上，移除開發期間所有可能允許應用程序接受所有憑證，如 org.apache.http.conn.ssl.AllowAllHostnameVerifier 或 SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER。如果使用延伸 SSLSocketFactory 的類別，則應確保 checkServerTrusted 方法正確的被實作，使伺服器能有效核對憑證之正確性。 ➢ M3：在 iOS 系統使用 CFNetwork 時，可以考慮使用安全傳輸 API 來指定受信任的客戶端憑證。幾乎在所有情況下，使用 NSStream 通訊連結 SECURITYLEVEL 的 TLSv1 應使用具備更高標準的密碼強度。以確保（NSURL 或包裝）NSURL 通訊不允許自簽或無效憑證，如 NSURL 類方法 setAllowsAnyHTTPSCertificate。 ➢ M10：行動裝置應用程式在編譯時應針對其完整性檢測，須能夠發現程式碼被新增或修改。應用程式必須能在執行時對完整性衝突做出反應。 ➢ M7：避免行動裝置應用程式遭注入威脅，伺服器應該

類別	技術細節內容
	對下列可能的注入威脅，做適當的處理，包含: SQLite Injection, JavaScript Injection, Local File Inclusion, XML Injection, Format String Injection, Classic C Attacks, Intent Injection/Fuzzing。
系統執行與安全	● **OWASP Mobile Top 10 Risk** ➢ M9：行動裝置應該具備適當的超時保護，以避免未經授權的惡意存取。良好的超時週期根據應用程式的安全敏感性、既有的風險狀況等有很大的不同，建議的方針是： • 15 分鐘的高安全性應用 • 30 分鐘中等安全應用 • 1 小時低安全應用 ➢ M5：行動裝置應用程式中之持久性認證功能，用戶密碼不應該在裝置上儲存。 ➢ M5：理想情況下，行動裝置應用程式應使用能夠讓用戶自行撤銷已安裝特定於裝置之憑證，以確保可避免裝置被盜或遺失時，遭到未經授權的存取。 ➢ M8：避免使用不合時宜的 handleOpenURL 方法處理 URL 的呼叫；應採用 openURL: sourceApplication: annotation 這類的方式與透過安全參數驗證受信任的應用程式白名單。 ➢ M6：避免使用行動裝置應用程式內建加密程序，以防止攻擊者透過逆向工程或繞道的方式，取得機敏資料。 ● **NIST SP 800-164** ➢ 隔離並防止在同一設備上的應用程式和資訊意外交互存取。

類別	技術細節內容
	➢ 參考 NIST SP800-88rev1 媒體清除原則，以提供不同級別的保護。 ● **YD/T 2408-2013** ➢ 4.6.1.1 開機密碼保護：行動裝置開啟身分認證功能，以確保唯有持正確密碼方可令行動裝置開機。 ➢ 4.6.1.2 開機後鎖定狀態的密碼保護：行動裝置開啟身分認證功能，以確保唯有持正確密碼方可使用行動裝置。

資料來源：本計畫彙整

肆、現行國際行動終端硬體晶片檢測說明

就本研究案國際手機安全發展與現況的論述中，我們可瞭解美國於 NIST Special Publication 800-164 規範中，將行動裝置基架構分為硬體、韌體、作業系統、應用程式及資訊內容，特別針對手機硬體的密碼模組功能的區塊的檢測措施與管理辦法，可參考 NIST「聯邦資訊處理標準」 FIPS-140-2 標準來加強手機密碼模組安全功能。

密碼模組是指由硬體、軟體及韌體組合成的模組，用來實現密碼邏輯、程序及密碼演算法，例如智慧卡內的加密模組、虛擬私密網路內的加密演算法、電子憑證中心(CA)及加密傳真機等。目前對密碼模組檢驗的國家有美國、加拿大與英國，其他國家則將其納入資訊安全的領域中。在共同準則(Common Criteria, CC)安全評估的保護剖繪(protection profile, PP)中，密碼模組有些也會要求通過 FIPS 140-2 的驗證，所以共同準則安全評估與密碼模組安全需求兩者有互補關係，依據不同的檢測概念執行各自的產品檢驗。

目前由美國及加拿大訂定密碼模組驗證的相關標準，即 FIPS 140-2。美國 NIST 於 1994 年 1 月 11 日公布「密碼模組安全需求規範 FIPS 140-1」，將密碼模組產品安全等級分為四級，於 1994 年 6 月 30 日正式生效。同時美國 NIST 與加拿大通訊安全組織(Communication Security Establishment, CSE)於 1995 年 7 月 17 日共同宣佈了美國/加拿大「密碼模組核可計畫」(Cryptographic Module Validation Program, CMVP)。

美國聯邦政府規定 1997 年 6 月 30 日後採購的密碼模組產品必須通過 CMVP FIPS 140-1 測試；加拿大政府雖然沒有強制規定，但是強烈建議政府採購的密碼模組產品要通過 CMVP FIPS 140-1 測試。NIST/CSE 於 2001 年 5 月 25 日公布 FIPS 140-2，為 FIPS 140-1 的修訂版，並宣布於 2002 年 5 月 25 日正式生效。從 2002 年 5 月 26 日之後，美國聯邦政府與加拿大政府只准購買通過 CMVP FIPS 140-2 測試通過的密碼模組產

品。

就上述密碼模組檢驗從提出申請至取得美國 NIST 發證，最快時間約八個月，因此許多資通訊系統廠商，都會要求密碼模組設計與研發商，於開發期間就提出認證申請工作，待取得認證後，再將該通過認證之密碼模組整合至資通訊系統產品，以宣告產品符合國際安全標準。另外，2015 年第 16 屆國際共同準則研討會（ICCC）中，由韓國國家安全研究院(NSRI) Keunwoo Rhee 先生主講「Developing the Security Functional Requirements of Mobile Devices for the Korean Government」提到，為了解決行動裝置安全議題，韓國從 2014 年 8 月起集結產官學各單位人馬針對行動裝置安全議題進行討論，以共同準則(Common Criteria, CC)架構並列出行動裝置安全功能要求，包含資料保護、身分認證、安全管理、存取控管、可信賴路徑，以及延伸定義組件平台與應用管理保護。本計畫依據 Common Cretia 最近一版公告的行動裝置基礎保護規範(Mobile Device Fundamentals Protection Profile, MDFPP)，有關硬體安全技術資訊彙整如下表所示。

表6　共通準則硬體安全深度彙整分析表

序號	項目	技術要求與檢測說明
1	受信任的傳輸通道	行動裝置能提供建立與通訊目標之可信任安全連線，且在傳輸期間對通訊資料加以保護，傳輸過程應符合 IEEE、RFC 發佈之信任通道建立標準。相關參考標準如下列所示： IEEE 802.11-2012, IEEE 802.11ac-2013 IEEE 802.1X, RFC 5280, 2560, 5759
2	開機自我測試	行動裝置開機過程，需通過所有與密碼有關之功能及系統軟體完整性檢測。
3	連續認證失敗	應具備正整數次之驗證錯誤計數機制，當嘗試錯誤

序號	項目	技術要求與檢測說明
	次數監測	超過門檻值，需抹除受應保護之資訊。
4	金鑰管理	加密金鑰及通訊密鑰之產生、交換、合併與銷毀。 應符合 NIST、ANSI 及 IEEE 發佈之金鑰使用及管理標準。相關參考標準如下列所示: ANSI X9.31-1998, IEEE 802.11-2012, IEEE 802.11ac-2013, IEEE 802.1X, NIST SP 800-38A, 38C~F, 56A~B, 57, 90B
5	金鑰儲存保護	所有的儲存於行動裝置之金鑰，都需要對其機密性與完整性，透過金鑰額外保護。故行動裝置應具備適當之機制，以對存放於行動裝置之金鑰保證其機密性與完整性。
6	金鑰傳輸保護	行動裝置之金鑰應具備適當的存放與管理機制，且明文金鑰不得存放於非揮發性之記憶體、不得用任何方式匯出或直接對外傳輸。
7	演算法要求	行動裝置使用之加/解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發佈之金鑰演算法標準。相關參考標準如下列所示: ANSI X9.31-1998, IEEE 802.11-2012 IEEE 802.11ac-2013, IEEE 802.1X NIST SP 800-38A, 38C~F, 56A~B, 57, 90B
8	產生初始化向量	行動裝置所有使用之加密模式，應各自對其初使化向量產生要求。因此加密模式應符合 NIST 發佈之初始化向量要求。相關參考標準如下列所示: NIST SP 800-38A, 38C~F, 56A~B, 57, 90B
9	產生隨機位元	使用熵源種子以確定性方式產生隨機位元。 符合 NIST、ANSI 發佈之隨機位元產生規範要求。 相關參考標準如下列所示:ANSI X9.31-1998,

序號	項目	技術要求與檢測說明
		NIST SP 800-38A, 38C~F, 56A~B, 57, 90B

反觀國內手機資安檢測也會遭遇到測試時程與晶片掌握度等問題，就研究團隊了解目前國內手機業者亦向各專業廠商採購硬體零件進行組裝，硬體(例如：手機晶片)相關安全性，實掌握在該硬體製造商而非手機原廠中。若強制要求進行硬體晶片的安全檢測工作，除產品認證須耗費較長時間，同時也影響產品上市時間，也降低廠商送檢驗意願，而失去安全檢測的目的。因此建議參考國際手機資安的檢測管理模式，由主管機關將晶片硬體功能檢測獨立並訂定相關檢測規範，並利用手機產品的分層架構特性及對應的檢測要求規範做法，以提升國內手機資安檢測規範實施的可行性。

伍、結論

依據前一章節分析說明，本計畫基於對使用者資料之保護，歸納出可為規範訂定之指標文件，及原因說明如下:

一、OWASP Mobile Security Project - Top Ten Mobile Risks

數個風險評估文件中，相較於其他國家所發佈的分析報告，長期以來 OWASP 在資訊安全領域,不斷累積並具備持續收集分析威脅與風險之專業能力，且能夠持續進行更新，故本計畫在風險評估文件中以 OWASP 為最適風險參考標準。

二、SP 800-164, DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices 及 YD/T 2407-2013 移動智能終端機安全能力技術要求(包含配套文件 YD/T 2408-2013 移動智能終端機安全能力測試方法)

經由明確定義使用者端裝置相關要求，以及將使用者端裝置由硬體至使用者資訊分為五個不同的層級，有助於在訂定規範時將測試項目依據不同的層級加以深化。

三、Security Requirements for Mobile Operating Systems

則是藉由國際共通的 ISO 15408 安全評估共通準則(Common Criteria)標準，透過擬訂行動裝置保護剖繪(Protection Profile) 以作為單位使用之智慧型裝置的一致性標準。對本計畫所訂定之規範內容上，能從宏觀的角度，以朝向國際共通陳述方式撰寫。

四、Commercial Mobile Device Implementation Plan、Mobile Device Strategy、Mobile Operating System Security Requirements Guide 、Mobility Security Guide

由於政府組織內部規範通常為了確保資訊安全，及基於國防與國家

安全，相對於一般企業使用之架構考量更為縝密，且均透過引述及比較既有安全之標準，達到強化安全之目的。因行動裝置應用程式安全除了從行動裝置本身外，本計畫也希望藉由審視從外部環境對行動裝置所造成之威脅，以研擬相對應之檢測細節，以與前述二項針對裝置本身做出完整的配套策略。

五、SP 800-163, Vetting the Security of Mobile APPlications

最後則是希望透過參考此規範所提出的審批與檢視方法，以期避免風險與實際檢測之間造成疏漏，使規範更臻完整。

由於目前收集到的規範多數均以使用者資料安全以及行動裝置應用程式為主要考量，因此本計畫藉由上述條件歸納彙整出 10 份主要標準，作為後續規範與檢測執行之主要參考依據，藉此提升整體與全面性考量。

以及本研究基於排除風險評估與使用者指引之各規範共通性內容加以歸納，可明確得出以下結論:首先透過資料收集與分析，事先評估所可能遭遇之風險。其次是將各種風險依據智慧型行動裝置之特性，進行適當之分級分類(例如: YD/T 2407-2013、YD/T 2408-2013 及 SP800-164)以達到風險管理之目的，以及 YD/T 2407-2013 對於分級分類後進一步深化訂定檢測內容。最後，則是依據各企業/政府組織內部的資訊安全政策(例如:美國國防部、美國國家安全局)或規範安全評估共通準則，進行實作及預防資訊安全風險之相關管制措施，以期達到全面性的防護成效。

此外，基於對民眾宣導智慧型行動裝置資訊安全之概念，多數國家均在協助使用者的立場，藉由正確的設定智慧型行動裝置之相關安全機制，達到初期對於智慧型行動裝置基本使用安全之保護，因此本計畫歸納前述所有關於保護使用者資料安全之相關指引，將其彙整如下列 10 項使用者指引，以期防範資訊安全問題於未然。

表7　使用者指引參考表

項次	項目	說明
1	設定 PIN 碼、行動裝置密碼與多重身分驗證機制(例如:指紋辨識)。	避免行動裝置因送修或失竊而遭到未授權的存取內部資訊。
2	定期檢查並安裝原廠提供之更新與修補程式。	藉由原廠提供的修補機制，提升行動裝置安全性。
3	不移除行動裝置預設的安全機制。	不應對行動裝置進行”破解”、”越獄”或”取得 root 權限”，卸除行動裝置預設安全機制。
4	僅從受信任的來源安裝應用程式。	避免安裝來源不明的程式造成安全威脅，應從正式的官方管道取得 APPs。如: APPle APP Store, BlackBerry World or Google Play。
5	不使用之行動裝置應刪除所有儲存之資料並恢復出廠預設值。	當不使用的行動裝置要移轉他人使用、廢棄、捐贈、轉賣、送修前，應刪除所有行動裝置上之資料，並恢復出廠預設值。
6	應透過建立信任安全的連線與機制傳送機敏資料。	使用點對點的安全通道(例如:SSL/TLS/HTTPS)與金鑰加密機制，對欲傳送之機敏資料(如:網路銀行之帳號、密碼)加以保護。
7	所有介面在不使用的狀況下應關閉，並避免建立不信任連線。	防止不經意的狀況下，在公共場合主動連線或被不明連線。例如:藍芽的探索模式應於使用後立即關閉，並盡可能避免使用。以及不連線到公共場合中不明的無線基地台(或無線熱點)。
8	特別留意軟體蒐集使用者資料之要求。	在行動裝置軟體提示並要求時，應注意盡可能避免不必要之資訊之上傳。例如: 不任意依據軟體指示上傳通訊錄資訊。

項次	項目	說明
9	不任意相信並點選可疑的郵件或簡訊所提供之連結位址。	對不明簡訊內容應提高警覺，以防範簡訊詐騙與避免遭受安裝惡意程式之威脅。
10	對於任何應用程式執行過程所產生的錯誤代碼應加以求證。	那有可能是惡意程式欲繞過系統防禦機制所導致，應對不明訊息代碼向原始供應商進一步求證。

資料來源：本計畫整理

附件 2 智慧型手機資安風險評估報告

智慧型手機資安風險評估報告

附件 2

目 次

壹、 智慧型手機資安風險評估 ..... 附件 2-1
一、 安全目標 ..... 附件 2-1
二、 風險之定義 ..... 附件 2-1
三、 風險評鑑技術與方法 ..... 附件 2-1
(一) 高階風險評鑑作法 ..... 附件 2-4
(二) 詳細風險評鑑作法 ..... 附件 2-6
四、 行動裝置風險評估流程 ..... 附件 2-10
(一) NIST 行動裝置安全管理參考指引 ..... 附件 2-10
(二) OWASP 行動安全專案(Mobile Security Project)..... 附件 2-14
五、 智慧型手機風險評估框架 ..... 附件 2-25
(一) 檢測單元區分 ..... 附件 2-25
(二) 安全等級 ..... 附件 2-26
(三) 智慧型手機風險評估矩陣 ..... 附件 2-27

圖 目 次

圖 1　預先定義值矩陣範例(一) ..... 附件 2-7
圖 2　預先定義值矩陣範例(二) ..... 附件 2-8
圖 3　依風險之量測排序威脅之範例 ..... 附件 2-9
圖 4　行動裝置威脅分析示意圖 ..... 附件 2-19
圖 5　行動裝置 10 大風險 ..... 附件 2-20
圖 6　智慧型手機風險評估框架 ..... 附件 2-25

表 目 次

表 1　風險評鑑方法 ..... 附件 2-2
表 2　資訊系統營運衝擊分析範例 ..... 附件 2-4
表 3　安全等級說明 ..... 附件 2-26
表 4　智慧型手機風險評估矩陣表 ..... 附件 2-27

壹、智慧型手機資安風險評估

參考國際之智慧型手機資安相關評估文件，針對智慧型手機之韌體、作業系統及出廠時內建應用軟體等風險，提出智慧型手機資安風險評估報告，內容包括資安風險評估方法、流程、範圍、面向、等級及結果等。

一、安全目標

行動裝置需要支援多元的安全目標，典型的作法是整合許多的安全功能在裝置裡，通常的安全目標如下：

- 機密性：確保傳輸或是儲存的資料，不會遭到未獲授權者的讀取
- 完整性：偵測傳輸或是儲存的資料，遭到故意或是非故意的改變
- 可用性：確保使用者可以利用行動裝置，在需要時存取所需資源

二、風險之定義

風險的定義，參考 ISO 31000:2009 係指：對於組織目標之不確定影響(effect of uncertainty on objectives)。所謂影響：係指對於預期結果的誤差，包括正向與負向的結果。

另參考 ISO/IEC 27000:2009 係指：事故發生的潛在可能性及其後果。

三、風險評鑑技術與方法

ISO 31010:2009 風險管理—風險評鑑技術(Risk management -- Risk assessment techniques)提供系統化的風險評鑑方法選擇及應用的指引文件，摘列適用於各個層級的風險評鑑方法，詳見表 1 所示。

以下所列風險評鑑方法，依據風險評鑑之過程，區分為風險識別、風險分析(含衝擊後果、發生可能性、風險等級)及風險評估等階

段，標示所列風險評鑑方法之適用性，SA：表強烈建議　NA：表不適用　A：表適用。

表1　風險評鑑方法

方法名稱	風險評鑑過程					註記
	風險識別	風險分析			風險評估	
		衝擊後果	發生可能性	風險等級		
腦力激盪法	SA	NA	NA	NA	NA	
結構或非結構化訪談法	SA	NA	NA	NA	NA	
Delphi 德爾非法	SA	NA	NA	NA	NA	
檢查表法	SA	NA	NA	NA	NA	
主要危險分析法(PHA)	SA	NA	NA	NA	NA	
危害與可操作性分析法（HAZOP）	SA	SA	A	A	A	
危害分析重要管制點法（HACCP）	SA	SA	NA	NA	SA	
環境風險評鑑法	SA	SA	SA	SA	SA	
結構化 SWIFT 法	SA	SA	SA	SA	SA	
情境分析法	SA	SA	A	A	A	
營運衝擊分析法	A	SA	A	A	A	●
根本原因分析法(RCA)	NA	SA	SA	SA	SA	
失效模式與影響分析法(FMEA)	SA	SA	SA	SA	SA	
故障樹分析法	A	NA	SA	A	A	
事件樹分析法	A	SA	A	A	NA	
原因及後果分析	A	SA	SA	A	A	
原因及影響分析法	SA	SA	NA	NA	NA	
保護層及分析法(LOPA)	A	SA	A	A	NA	
決策樹分析法	NA	SA	SA	A	A	
人員可靠性分析法	SA	SA	SA	SA	A	

方法名稱	風險評鑑過程					註記
	風險識別	風險分析			風險評估	
		衝擊後果	發生可能性	風險等級		
Bow tie analysis	NA	A	SA	SA	A	
可靠性為中心的維修(RCM)	SA	SA	SA	SA	SA	
潛行迴路分析法(Sneak circuit analysis)	A	NA	NA	NA	NA	
馬爾可夫轉移矩陣法(Markov analysis)	A	SA	NA	NA	NA	
蒙特卡羅方法(Monte Carlo simulation)	NA	NA	NA	NA	SA	
貝氏網路法(Bayesian statistics and Bayes Nets)	NA	NA	NA	NA	SA	
ROC 曲線(FN curves)	A	SA	SA	A	SA	
風險指標法(Risk indices)	A	SA	SA	A	SA	
後果可能性矩陣(Consequence/probability matrix)	SA	SA	SA	SA	A	●
成本利潤分析法(Cost/benefit analysis)	A	SA	A	A	A	
多目標決策分析(Multi-criteria decision analysis)	A	SA	A	SA	A	
註記	SA：強烈建議 Strongly applicable NA：不適用 Not applicable. A：適用 Applicable ●：CNS/ISO/IEC 27005:2011 建議之資訊安全風險評鑑風法 高階風險評鑑法=營運衝擊分析法 詳細風險評鑑法=後果可能性矩陣					
資料來源：整理自 ISO 31010 附錄 A						

CNS/ISO/IEC 27005：2011 該文件之附錄 E 建議之二項資訊安全風

險評鑑作法，摘述如後：

(一)高階風險評鑑作法

高階風險評鑑允許定義行動之優先順序及時間表，基於各種理由例如：預算，機關可能無法同時實作所有的控制措施，故應將最關鍵之風險優先處理。同樣的，若實作風險管理僅一、二年，便要求開始進行詳細之風險評鑑作業，可能為時過早。為達成此目標，高階風險評鑑可由營運衝擊後果開始，而非以威脅、脆弱性、資產及衝擊後果之系統化分析開始，例如：行政院頒布之「資訊系統分類分級與鑑別機制參考手冊」所描述之「安全等級設定原則」，其所採用的便是如 ISO 31010 述之營運衝擊分析法，綜整考量在「資料保護受到損害」、「影響業務運作」、「影響法律規章遵循」、「人員傷亡」、「損害組織信譽」及「其他」等構面，評鑑對於機關之衝擊程度，而不考量其發生之可能性，以評定資訊系統之安全等級，便是符合本標準所稱之高階風險評鑑作法之一，詳見表 2 所示。

表2　資訊系統營運衝擊分析範例

安全等級 / 影響構面	普	中		高	
	0	1	2	3	4
1. 資料保護受到損害	▪一般性資料 ▪資料若外洩或遭竄改，不致影響個人權益或僅導致個人權益輕微受損	▪敏感性資料 ▪資料若外洩或遭竄改，將導致個人權益嚴重受損之資料		▪機密性資料 ▪資料若外洩或遭竄改，將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損	
2. 影響業務運作	▪系統容許中斷時間較長	▪系統容許中斷時間短		▪系統容許中斷時間非常短	

安全等級 影響構面	普	中		高	
	0	1	2	3	4
	▪ 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響 ▪ 系統故障僅影響機關非核心業務執行效能，或造成核心業務執行效能輕微降低	▪ 系統故障對社會秩序、民生體系運作將造成嚴重影響 ▪ 系統故障將造成機關核心業務執行效能嚴重降低		▪ 系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全 ▪ 系統故障將造成機關核心業務執行效能非常嚴重降低，甚至業務停頓	
3. 影響法律規章之遵循程度	系統運作、資料保護、資訊資產使用等若未依循相關規範辦理，將導致機關違反法律規章並伴隨輕微後果	系統運作、資料保護、資訊資產使用等若未依循相關規範辦理，將導致機關違反法律規章並伴隨嚴重後果		系統運作、資料保護、資訊資產使用等若未依循相關規範辦理，將導致機關從根本上違反法律規章	
4. 人員傷亡		若系統發生資訊安全事故，無法完全排除造成人員傷亡的可能性		若系統發生資訊安全事故，非常可能造成生命及肢體傷害的危險	
5. 損害組織信譽	若系統發生資訊安全事故，將導致機關形象、信譽受到輕微損害	若系統發生資訊安全事故，將導致機關形象、信譽受到嚴重損害		若系統發生資訊安全事故，將導致機關形象、信譽受到非常嚴重損害	
6. 其他	由機關視本身業務特性考量可能遭遇衝擊之其他影響構面（如：財物損失），並依需求和本質自行設定測量基準				

高階風險評鑑作業之優點如下：

- 一開始採用較簡單之作法，容易獲得風險評鑑參與人員之接受。
- 可做為良好之輔助規劃，以建構機關資訊安全之策略藍圖。
- 可將資源及預算運用於最有利之處。

惟由於初始採用高階風險評鑑，潛在地存在評鑑結果較不精確，可能未識別某些營運過程或系統，可視需要針對高安全等級之資產，進行詳細風險評鑑作業。

(二)詳細風險評鑑作法

詳細風險評鑑對於資產進行深度之識別與鑑別作業，並針對資產詳細列出其可能面臨之威脅與可能存在之脆弱性，以做為評鑑其風險與風險處理方法之依據。詳細之步驟需考慮時間、耗費程度及專家意見等。

詳細風險評鑑作法可以是定量或是定性的方法，或是二者之結合。宜根據資產之價值，或需被保護之特性，以評鑑威脅發生之可能性。

CNS/ISO/IEC 27005 於該文件之附錄 E 中，列舉了符合 ISO 31010 所示之後果可能性矩陣(Consequence/probability matrix)法之實務範例，但不以此為限，摘述如後：

1.預先定義值之矩陣

預先定義值矩陣主要考量資產之價值、威脅發生之可能性及脆弱性被利用之程度，以排序待因應之風險，範例詳見圖 1 所示，摘述說明如後：

	發生可能性－威脅	低			中			高		
	易被利用	低	中	高	低	中	高	低	中	高
資產價值	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

資料來源：CNS 27005

圖1　預先定義值矩陣範例(一)

(1)資產價值

依據資產之建置成本或是置換成本加以估價，再轉換成相同性尺度。

資產之價值可以經由與資料擁有者之晤談，依據不利之營運後果可合理預期發生之最壞情境加以估計，可以參考「資訊系統分類分級鑑別機制」的作法，例如對於資料保護受到損害或是影響業務運作之情境，經訪談後設定置換成本，以表 2 範例中所示資產安全等級區分為普、中、高三級，可以再轉換成相同性尺度，細分為 0~4 之五等級區分，以表示資產之價值，另實務當中對於資訊資產之衡量，亦會採用評估「機密性 C」、「完整性 I」與「可用性 A」之組合[CIA]加以衡量。

部分機關會將資產價值之[CIA]組合表示成以下二種模式：

資產價值[CIA]＝C + I + A 或是

資產價值[CIA]＝C x I x A

(若採用相乘之方式，建議將以上所述之相同性尺度修訂為

1~5 等級區分，以避免相乘之後，產生資產價值為 0 之情形)

不論機關採用相加或是相乘之計算模式，經轉換成相同性尺度之後，所代表之意義均是排序後之結果，代表機關待因應風險的優先順序，至於要採用相加或是相乘的方法，可以視機關之需求與尺度範圍而定，並無優劣之分。

(2)發生可能性—威脅

將威脅發生之可能性，區分為低、中、高三級。

(3)脆弱性易被利用之程度。

再將威脅利用脆弱性之容易程度，區分為低、中、高三級。

經由以上方法識別風險之相關量測組合，尺度由 0~8，填入於矩陣之內。

另一範例顯示類似之矩陣，分析營運衝擊之程度，另考量事故情境發生之可能性，以排序風險處理之優先順序。

	事故情境之可能性	非常低 (非常不可能)	低 (不可能)	中 (有可能)	高 (可能)	非常高 (經常)
營運衝擊	非常低	0	1	2	3	4
	低	1	2	3	4	5
	中	2	3	4	5	6
	高	3	4	5	6	7
	非常高	4	5	6	7	8

資料來源： CNS 27005

圖2　預先定義值矩陣範例(二)

縱軸將營運衝擊程度由非常低至非常高，區分為五個尺度，分別為 0~4。

橫軸將事故情境之可能性由非常低至非常高，區分為五個尺度，分別為 0~4。再將兩軸之尺度值相加，產生 0~8 尺度，詳見圖 2 所示。

以上範例所列示之 0~8 尺度，可以再簡化成為整體風險等級，例如：

- 低風險：0~2。
- 中風險：3~5。
- 高風險：6~8。

2.依風險之量測排序威脅

本方法將後果(資產價值)之因素與威脅發生之可能性(將脆弱性層面納入考量)相關聯，詳見圖 3 所示。

威脅描述詞 (a)	後果(資產) 值 (b)	威脅發生 可能性 (c)	風險量測 (d)	威脅排序 (e)
威脅 A	5	2	10	2
威脅 B	2	4	8	3
威脅 C	3	5	15	1
威脅 D	1	3	3	5
威脅 E	4	1	4	4
威脅 F	2	4	8	3

資料來源： CNS 27005

圖3　依風險之量測排序威脅之範例

- 首先依據預先定義之尺度，範例中採用的是 1~5，評估各受威脅資產之後果(資產價值) (b 欄位)。

- 同樣依預先定義之尺度 1~5，評估各威脅發生之可能性(c 欄位)。
- 藉由相乘(bxc)計算風險之量測。
- 最後再依風險相關之量測順序排序威脅(e 欄位)。

四、行動裝置風險評估流程

參酌以上風險評鑑技術所描述之高階風險評鑑作法及詳細風險評鑑作法，以下各列舉國際規範中所適用之行動裝置風險評鑑作法，摘述如後：

(一)NIST 行動裝置安全管理參考指引

美國國家標準局 NIST SP 800-124r1「機關行動裝置安全管理參考指引」(Guidelines for Managing the Security of Mobile Devices in the Enterprise)，當前行動裝置主要資安風險來源列舉七大面向，並建議在設計與建置行動裝置之安全控制措施時，須針對行動裝置以及經由行動裝置接取的資源，發展系統威脅模型(threat models)。

威脅模型包括確認利益相關的資源、威脅與漏洞以及這些資源的安全管控，然後進行成功攻擊與影響的量化工作，藉以分析相關資訊，以作為安全管控的改進或強化的決策參考。威脅模型幫助組織確認安全要項，以協助設計行動裝置的解決方案，期所有管控均能符合相關的安全要求。

NIST 在該指引中提出了七項：行動裝置的高階威脅與弱點(High-Level Threats and Vulnerabilities)，依據風險評鑑方法之區分，屬於「高階風險評鑑作法」，摘述如後：

1. 欠缺實體安全保護(Lack of Physical Security Controls)

行動裝置通常使用於組織能控制以外的不同地點，如員工家中、

咖啡飲店、飯店、研討會場等。比起其他裝置，行動裝置較容易遺失或被偷而增添許多風險。因此，當規劃行動裝置安全政策與管控時，組織應假設行動裝置被惡意人士利用，意圖恢復敏感資料時之情境，而不僅是考量直接從裝置本身或間接使用行動裝置以接取組織遠端的資源之情形。

緩解策略乃採分層方式。首先，對機敏資料進行保護，其作法是對儲存於行動裝置的機敏資料進行加密，讓未受授權的協力廠商，無法回復機敏資料；另一種方式是完全不允許機敏資料儲存於行動裝置中。縱使行動裝置一直由所有者持有，沒有任何實體安全上的顧慮，然而有心人士仍可經由偷窺行動裝置螢幕或盜用帳號密碼的方式進行惡意行為。

其次，在使用行動裝置或接取組織資源時均需進行認證。一般而言，行動裝置通常是單一的認證，即假設行動裝置僅有一位使用者，故不將行動裝置的使用者再用帳號予以區別，因此僅會使用PIN(Personal Identity Number)予以認證識別。此外，網域的認證識別，也可利用藉以強化行動裝置的認證能力。

2.使用不可信任之行動裝置(Use of Untrusted Mobile Devices)

許多行動裝置，特別是個人所有的行動裝置，並不必然值得信任。現在的行動裝置普遍缺乏已內建於筆記型電腦與其他型式主機的可信任的功能(如 TPM)，所以時有越獄(jailbreaking)與取得原始管控權力(rooting)的事件發生，亦即內建於行動裝置的安全性、作業系統使用的限制已被技術性跳過，發揮不了實質的功能。因此，組織應假設所有的行動裝置都是不可信任的，除非該組織織已妥適進行資訊安全的防護，並持續監控行動裝置使用機關內部的應用與資料。

減少不可信任行動裝置影響的策略為限制或禁止使用 BYOD 設備，從而使用組織所配發的行動裝置。另一有效的方法是確認組織所配發行動裝置的安全性，利用差異的監控與處理上，盡可能讓行動裝置維持在配發初時的狀態。例如在安全、隔離的行動裝置環境中執行組織軟體，或者使用裝置的完整掃描應用程式，以確認行動裝置維持在配發原始狀態。

3.使用不可信任之網路(Use of Untrusted Networks)

行動裝置主要是使用非組織的網路以接取網際網路，故組織通常對行動裝置所使用的外部網路的安全沒有任何的管控權利。通訊系統可能包括寬頻網路，如有線電視寬頻網路、WiFi 與行動通訊網路等。這些通訊系統很容易受到竊聽，而中間人攻擊的手法也可能出現，而進行監聽或修改之惡意行為。組織於規劃行動裝置安全性時應假設行動裝置與組織之間的網路是不可信任的。

使用加密技術可以減少不安全網路的使用風險，藉以保護通訊的機密性與完整性，同時，使用成熟的認證機制，用以確認傳輸資料的兩端的身分識別，更能保障通訊的安全性。

4.使用不可信任之軟體(Use of Untrusted Applications)

行動裝置的設計通常須符合易於尋找、取得、安裝與使用協力廠商應用軟體。這會帶來明顯的安全隱憂，特別是對於那些不會對協力廠商應用程式發布安全限制或其他限制的行動設備平臺。因此，組織規劃行動裝置使用的安全性時，應假設使用者可以下載的協力廠商應用軟體是不可信任的。

我們可以數種方式來減低這些應用軟體所帶來的風險，比如禁止協力廠商應用軟體的安裝；實施白名單策略，禁止安裝未經授

權允許的應用程式；或者建置安全的隔離區，將組織的資料與應用跟行動裝置的其他資料與應用予以隔離。另一建議是針對協力廠商的應用在核准用於行動裝置之前，均需進行風險評估，以降低風險。

重要的是，縱使採用減輕協力廠商應用程式風險的策略，使用者仍有可能利用行動裝置內建的網頁瀏覽器接取不可信任的網頁應用，或者經由隔離的網頁瀏覽器接取不當的應用內容。

5.與其他系統之交互作用(Interaction with Other Systems)

在資料同步與儲存方面，行動裝置可能須與其他系統互動。本地系統的互動一般包括利用一條充電用或同步用的纜線，連結行動裝置與桌上型電腦或筆記型電腦，而遠端系統最常見的互動包括資料備份到雲端儲存。倘若這些元件設備均在組織的管控之下，一般而言風險應是可接受的，但常常是其中一項或多項的設備是屬外部的，無法予以管控。例如：利用個人的行動裝置連結到組織配發的筆記型電腦、或使用組織配發的行動裝置連結到個人的筆記型電腦、或利用組織配發的行動裝置連結到遠端的備份服務等。在這些情境下，組織的資料均處在將資料儲存於組織外不安全環境的風險之中，讓惡意程式有機會藉以在設備與設備之間傳播。

為降低與其他系統互動的風險，組織配發的行動裝置應避免與個人所有的電腦進行同步動作，並對行動裝置可以同步的資料或設備進行安全管控。反之，也應避免個人的行動裝置與組織配發的電腦進行動同步，且在組織的電腦中限制可以連線接取的行動裝置。最後，為避免備份服務不當使用所產生的風險，可以終止該項服務或藉由行動裝置的組態設定來判別能否使用該服務。

6.使用不可信任之內容(Use of Untrusted Content)

行動裝置有可能使用不可信任的內容，例如 QR 碼的使用。每一個 QR 碼，會被轉譯成相關的 URL，所以惡意 QR 碼有可能直接將行動裝置導到惡意的網頁。此舉有可能引發目標式攻擊(targeted attacking)，例如放置惡意 QR 碼在目標用戶所聚集的地方。

減少風險的主要策略包括教育使用者且不鼓勵使用者在工作時，使用行動裝置接取不可信任的內容。然而卻可能限制行動裝置週邊使用，例如為了避免 QR 碼所產生的風險而關閉相機功能。

7.使用定位服務(Use of Location Services)

內建 GPS 功能的智慧型行動裝置通常可以執行在地化服務(Location services)，亦即依據 GPS 的地理資訊，提供與現在所在位置相關的商業服務。在地化服務通常與社群媒體、導航、網頁瀏覽及其他行動化主軸的應用服務。在組織安全方面，具在地化服務功能的行動裝置面臨更大的目標性攻擊的風險，因為使用者與行動裝置的所在位置的資訊，讓攻擊者易於利用這些資訊發動攻擊。

為了降低行動裝置定位服務的風險，可以將社群網路或相片的地理資訊去除，可也以在機敏的地區將在地服務關閉，以維持資訊安全。然而，即使關閉 GPS 的功能，類似的問題仍有可能發生，例如，接取網際網路時，IP 位址或 WiFi 的所在位置，仍有可能讓使用者的地理位置曝光。因此，最可行的方式是盡可能不要使用在地化服務，尤其是該行動裝置涉及重要公務時。

(二)OWASP 行動安全專案(Mobile Security Project)

開放網路軟體安全計畫，簡稱 OWASP（Open Web Application

Security Project）是一個開放社群、非營利性組織，全球目前有 82 個分會，其主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善應用程式的安全性。美國聯邦貿易委員會(FTC)更強烈建議所有企業務必遵循 OWASP 所發佈的十大網路弱點防護守則，美國國防部亦將此守則列為最佳實務[1]。

此網站每年度收集之資料分析相關行動裝置 APP 之風險與威脅並公告，目前已知歐盟在 2011 年 11 月所發表的 Smartphones secure development guidelines for app developers 文件中，亦參考此資料做為制定指引之基礎。

1.OWASP 行動應用威脅模型(Mobile Application Threat Model)

因應雲端技術快速的發展，不論是使用者或應用程式開發者，資訊的操作模式已逐漸地從主機平台移至可攜式行動裝置或智慧型手機，即使平台不同，既然是由人所開發的應用程式，必定會產生一定程度的弱點風險。

OWASP 採用行動應用威脅模型(Mobile Application Threat Model)作為詳細風險評鑑作法之依據，分從以下五個方面，分別說明應用程式可能的威脅：

- 行動應用架構：此部分內容描述如何根據行動裝置的特定功能，來設計應用程式，包含無線傳輸協定，數據傳輸介質，

[1] Simplifying Application Security andCompliance with the OWASP Top10

http://web.securityinnovation.com/Portals/49125/docs/OWASP%20Top%20Ten.pdf

硬體組件和其他應用程序的交互運作。

- 行動數據：內容包含數據應用程序之儲存和處理？數據工作流程為何？
- 威脅代理人鑑定：行動應用程序的威脅為何，定義何種威脅代理人適用於行動應用。
- 攻擊方法：何者是威脅代理人最常使用的攻擊。攻擊方法乃是定義這些攻擊，並利控制被侵入並減輕攻擊。
- 控制措施：定義防止攻擊元件。

另該研究方法將行動裝置遭受的威脅分成 6 大分類，分別為：

(1)詐欺(Spoofing)

是一種技術用以取得非經授權的存取電腦，其手法主要以偽裝發送訊息、郵件的位址或偽裝成為已被授權的使用者，在未經許可下進入安全的電腦系統，以進行任何不法的行為。Spoofing 多為垃圾郵件發送者、駭客或網路詐騙者所使用，藉以達到犯罪行為而不被發現。

(2)拒絕/否認(Repudiation)

讓沒有修改權利的人或系統能夠竄改他人資訊或否認某些事實，其目的在破壞資料的完整性。否認的反面為不可否認(non-repudiation)，是指藉由提供原本的證據，使發件人不能否認曾發出信息，而收件人也不能否認曾收到信息。例如在網路上購物，商家有時不只要求消費者提供信用卡號，還要信用卡的 PIN。藉由消費者的身分確認，商家就有不可否認的證據來進行交易。

(3)阻斷服務(Denial of Service)

亦稱洪水攻擊，是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其對目標客戶不可用。當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時，其稱為分散式阻斷服務攻擊(Distributed Denial of Service attack，縮寫：DDoS)。攻擊發起者一般針對重要服務進行攻擊，如銀行，信用卡支付閘道器，甚至根網域名稱伺服器。該類攻擊也常見於部分遊戲，被心懷不滿的玩家或是競爭對手廣泛使用。DDoS 攻擊可以具體分成兩種形式：頻寬消耗型以及資源消耗型。它們都是透過大量合法或偽造的請求占用大量網路以及器材資源，以達到癱瘓網路以及系統的目的。

A.頻寬消耗型

可以又分為兩個不同的層次；洪泛攻擊或放大攻擊。洪泛攻擊的特點是利用殭屍程式傳送大量流量至受損的受害者系統，目的在於堵塞其頻寬。放大攻擊與其類似，是通過惡意放大流量限制受害者系統的頻寬；其特點是利用殭屍程式傳送資訊，但是資訊卻是傳送至廣播 IP 位址，導致系統子網路被廣播 IP 位址連線上之後再傳送資訊至受害系統。

B.資源消耗型攻擊

協定分析攻擊(SYN flood，SYN 洪水)傳送控制協定(以下簡稱 TCP)同步(以下簡稱 SYN)攻擊。TCP 行程通常包括傳送者和接受者之間在封包傳送之前建立的完全訊號交換。啟動系統傳送一個 SYN 請求，接收系統返回一個帶有自己 SYN 請求的確認(以下簡稱 ACK)作為交換。傳送系統接著

傳回自己的 ACK 來授權兩個系統間的通訊。若接收系統傳送了 SYN 封包，但沒接收到 ACK，接受者經過一段時間後會再次傳送新的 SYN 封包。接受系統中的處理器和記憶體資源將儲存該 TCP SYN 的請求直至超時。

DDoS TCP SYN 攻擊也被稱為「資源耗盡攻擊」，它利用 TCP 功能將殭屍程式偽裝的 TCP SYN 請求傳送給受害伺服器，從而飽和服務處理器資源並阻止其有效地處理合法請求。它專門利用傳送系統和接收系統間的三向訊號交換來傳送大量欺騙性的原 IP 位址 TCP SYN 封包給受害系統。最終，大量 TCP SYN 攻擊請求反覆傳送，導致受害系統記憶體和處理器資源耗盡，致使其無法處理任何合法用戶的請求。

(4)篡改(Tampering)

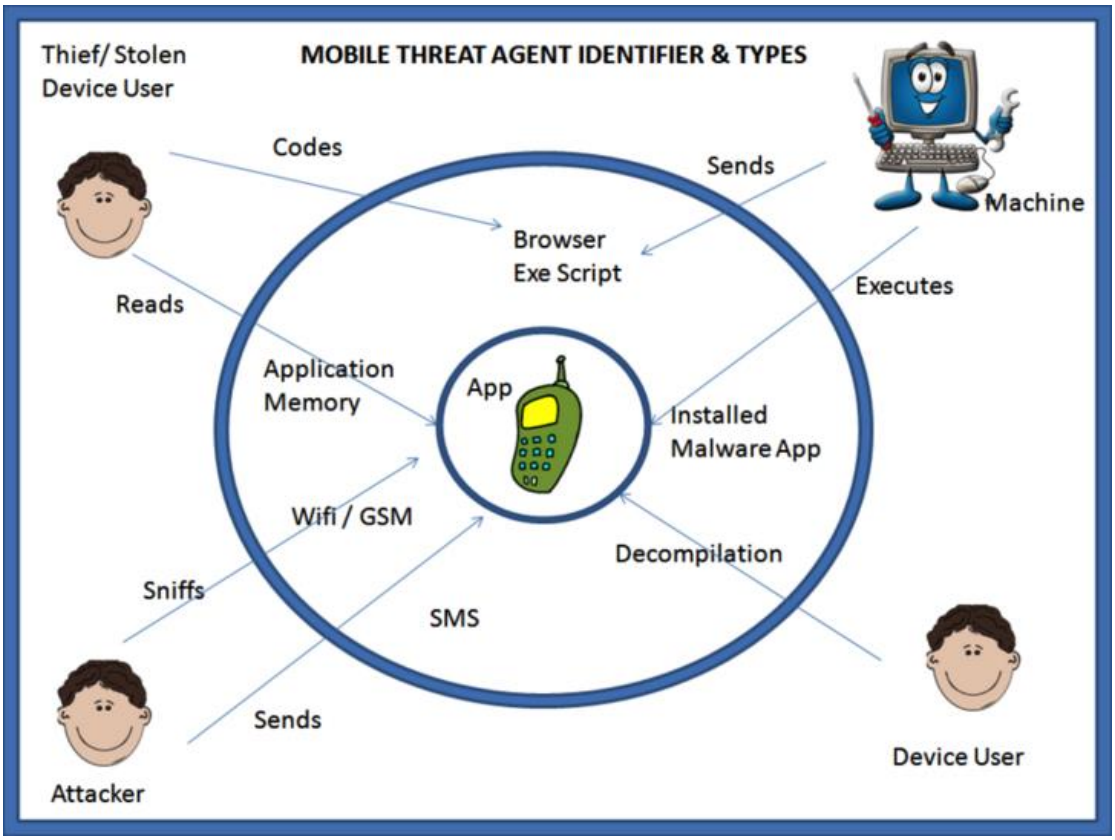
是指未經授權的刪除、插入、或更改資訊，並期望別人無法察覺。例如學生更改考試成績，或是駭客進銀行網路刪除信用卡消費紀錄等。

(5)資訊洩漏(Information Disclosure)

將資料洩漏給不該接收的使用者，例如，攻擊者在沒有存取權的情況下，讀取機密性的檔案。

(6)提升權限(Elevation of Privilege)

讓一個遠端一般使用者,透過非正常的管道，提升權限能夠執行一些只有系統管理員才能使用的指令集。



資料來源： OWASP Mobile Application Threat Model

圖4　行動裝置威脅分析示意圖

2.行動裝置 10 大風險

OWASP 再將上述分類依照風險所造成嚴重性衝擊(例如：機密性、完整性、可用性)加以定出行動裝置十大風險。概略說明如下：

資料來源： OWASP Top Ten Mobile Risks : 2014

圖5　行動裝置 10 大風險

(1) M1 伺服器端的控制薄弱(M1:Weak Server Side Controls)

主要是說明 Mobile 的弱點並不只單存在於 Mobile 端，所開發的 APP 應用程式或雲端系統的程式亦有可能存在弱點，例如：OWASP Cloud Top 10。

【建議防護措施】人員於伺服器端開發應用程式時，應避免產生 OWASP Web Top 10 或 OWASP Cloud Top 10 相關弱點。

(2) M2 不安全的資料儲存(M2:Insecure Data Storage)

意指敏感性資料未受到適當的保護，一般常見如敏感性資料未加密，或是一些不常用到的暫存資料可能含有敏感訊息(例如：登入帳號與密碼)，可能會造成機密性資料損失、憑證外洩、侵犯隱私權等衝擊。

【建議防護措施】只儲存必要資訊，不將敏感資料存放於開放式的儲存媒體(例如：SD 卡)，採用安全的檔案加密應用程式介面，設定檔案的讀取與寫入設定權限等。

(3) M3 傳輸層保護不足(M3:Insufficient Transport Layer Protection)

可攜式行動裝置於傳輸機敏性資料時，很常發生未加密情況，例如：瀏覽器本身不支援 HTTPS 功能，或是使用的 APP 應用程式未採用加密方式進行資料的傳輸(如：登入系統、交易資料等)，因此可能會造成駭客使用中間人攻擊(Man-in-the middle attacks)，從中竄改或竊取封包資料，進而造成機敏資料的洩漏。

【建議防護措施】程式開發者應確保所有敏感性資料有採用加密方式進行傳輸，傳輸媒介可包含網路連線、Wifi 連線，甚至是近場通訊(Near Field Communication, NFC)連線等，若只採用明文方式傳遞，攻擊者可輕易透過網路監聽方式(Sniffer)竊取機敏性資料。

(4) M4 非故意的資料外洩(M4:Unintended Data Leakage)

可攜式行動裝置中的第三方應用程式可能會自動幫使用者儲存一些敏感性資訊，例如：網頁暫存(Web Cache)、按鍵側錄(Keystorke Logging)、擷取畫面(Screenshots)、日誌檔(Logs)或暫存目錄(Temp Directories)等，一但攻擊者成功取得行動裝置權限時，將會侵犯使用者隱私，甚至導致資料洩漏情形。

【建議防護措施】一些較敏感性的資料應避免自動儲存於可攜式行動裝置內(例如：憑證資訊、帳號、密碼等)，檢查部分應用程式是否會儲存敏感性資訊，建議加以手動移除，或是選

擇不自動儲存功能。

(5) M5 粗糙的授權與認證(M5:Poor Authorization and Authentication)

部分可攜式行動裝置的網頁應用程式僅採用永不變的數值來執行身分驗證與授權階段，例如：國際移動設備識別碼(International Mobile Equipment Identify Number, IMEI)、國際移動用戶識別碼(InternationalMobile Susscriber Identify, IMSI)或通用唯一識別碼(Universally Unique Identifier, UUID)。

【建議防護措施】使用嚴謹的身分驗證與授權(例如：雙因素認證)，避免使用可攜式行動裝置的硬體 ID 標籤或永不變的 ID 識別碼做為身分驗證的因素。

(6) M6 加密失效(M6:Broken Cryptography)

所謂加密失效分為兩種情況，一種是使用強健的加密演算法卻遭到破解，另一種為使用過於簡單的加密演算法遭到破解。前者要實現的困難度較高，後者則是相當常見。OWASP 提出幾個對於加密方法的謬誤，例如：編碼(Encoding)、混淆(Obfuscation)、序列化(Serialization)，上述嚴格說起來，並非為嚴謹加密方式，攻擊者能輕易破解簡單的加密演算法後，取得可攜式行動裝置的完整資訊，同樣也可做到提升權限或機敏資料遭洩漏等情況。

【建議防護措施】開發應用程式建議使用強健的加密演算法，並不斷進行反覆測試，直到應用程式開發完成時，仍需執行嚴格的挑戰測試(Battle-Tested)。

(7) M7 客戶端注入(M7:Client Side Injection)

Injection 攻擊即使從傳統電腦轉移到了可攜式行動裝置上的網頁應用程式，若網頁應用程式存有 Injection 弱點，攻擊者仍可利用 SQL Injection 或 XSS 攻擊手法來提升可攜式行動裝置的權限，或是利用網路盜打市話(Toll Fraud)的情況發生。

【建議防護措施】網頁應用程式傳遞參數給雲端資料庫的內容，需過濾不受信任或不應該接受的內容，例如：SQL 執行語法、特殊字元等，同樣可採用 prepared statement 功能進行過濾。

(8) M8 不受信任的輸入(M8:Security Decisions Via Untrusted Inputs)

在各種可攜式行動裝置的平台均會發生(例如：iOS、Andriod)，應用程式可能經由惡意攻擊者精心設計，或是應用程式遭攻擊者透過 Client Side Injection 攻擊方式來消耗可攜式行動裝置的硬體資源或提升權限情形。舉例來說，假設 Skype 應用程式具有 HTML 或 Script Injection 弱點，攻擊者只要事先把具有惡意連結的 iframe 寫入某個特定網頁，一但可攜式行動裝置的瀏覽器讀取到此段程式碼時，則應用程式將無需使用者授權，自動開始播號給指定的電話號碼。

【建議防護措施】每個應用程式在設計時應注意身分認證與授權的問題，以確保可攜式行動裝置需經過使用者的身分驗證後才允許執行特殊的行為或功能。

(9) M9 不適當的會話處理(M9:Improper Session Handling)

可攜式行動裝置的應用程式 session 過期時間，一般而言會設定的比較長，原因是對使用者方便存取或使用，通常這些

session 經由 HTTP Cookies、Oauth Token、Single Sign-on 等方式來進行維護，建議避免使用裝置的硬體識別碼來當作 session 值，很容易讓攻擊者猜到 session 內的機密性內容(例如：帳號或密碼)，進而造成提升攻擊者於可攜式行動裝置的權限，進行非授權的存取。

【建議防護措施】若需要提高安全性，相對其軟硬體設計(演算法或操作方式)的複雜度亦會增高，只要 session 值的過期時間應設定在一個可接受範圍內，就無需擔心讓使用者太頻繁的重新驗證；另外可攜式行動裝置遭遺失或竊取時，應有能夠快速撤銷 Token 的機制，使裝置無法更近一步遭受到濫用情況。

(10) M10 封裝檔案保護不足(M10:Lack of Binary Protections)

此弱點的洩漏方式，乃是指應用程式原始碼中，把輸入或輸出的相關參數直接寫入在程式碼當中，因此只要攻擊者能夠取得應用程式的原始碼(例如：透過逆向工程手法)，若原始程式碼內容含有敏感資訊，像是 API 金鑰、帳號或密碼等，可能會造成企業內部的智慧財產暴露或個人憑證洩漏等情況。

【建議防護措施】程式開發者應避免將敏感資訊寫入於原始程式碼中。

以上所述之 OWASP Mobile Top 10 Risk 係採用詳細風險評鑑之作法，蒐集大數據之後所進行威脅分析之結果，對於其他之機構，例如：美國國防部及歐盟：美國國防部(US DoD)及歐盟網路及資訊安全署(ENISA -the European Union Agency for Network and Information Security)，均將 OWASP 所公布之 Top 10 Risk 作為其國家或是機關之高階風險評鑑作法之參考，適兼具效能與效

率之聰明作法。

五、智慧型手機風險評估框架

本案遵循高階風險評鑑作法，並參考 OWASP Mobile Top 10 Risk，作為風險評鑑之威脅分析依據，以評估智慧型手機在資料層、應用程式層、通信協定(介面)層、作業系統層及硬體層，作為智慧型手機風險評估框架，評估當「機密性」、「完整性」及「可用性」喪失，可能造成之衝擊程度，區分為以下三級：

- 初級：基本隱私保護
- 中級：進階資料保護
- 高級：機密型資料保護

資料來源：本計畫彙整

圖6　智慧型手機風險評估框架

(一)檢測單元區分

依據國際間對智慧型手機安全之分層概念，本規範將智慧型手機安全區分為資料層、應用程式層、通訊協定層、作業系統層及硬體

層五個層別，主要考量不同層別可能面臨的資訊安全風險有所不同，並對各層別訂定技術要求。智慧型手機通過所屬技術要求之檢測項目，即表示達到該檢測安全需求與安全期望。

- 資料層(Information/Data)：主要包含資料的傳送、儲存或使用等相關安全。
- 應用程式層(APPs)：主要包含手機系統內建軟體等相關安全。
- 通訊協定層(Protocol)：主要包含有線介面、無線介面及通訊協定等相關安全。
- 作業系統層(Operating System)：主要包含作業系統相關服務與各硬體元件存取等相關安全。
- 硬體層(Hardware)：主要包含金鑰與演算模組等安全。

(二)安全等級

本規範之智慧型手機系統內建軟體安全規劃初級至高級共 3 個安全等級，主要依據智慧型手機可能面臨之資安風險有所不同，以及所支援的安全能力程度來劃分，訂定所需符合之安全等級；而各安全等級內之檢測項目採累加式，即高級除了滿足自身安全等級內之檢測項目外，也必須滿足初級與中級所有檢測項目。

初級為智慧型手機基本隱私保護最低要求，所有智慧型手機應通過初級之技術要求內檢測項目，中級與高級則採自願性檢測。中級則對資料做進階之保護、高級則確保智慧型手機之核心底層不會被遭到竄改或不正當地擷取資訊。安全等級說明詳表 3。

表3　安全等級說明

項次	安全等級	要求	說明
1	初級	基本隱私保護	智慧型手機提供個人使用者隱私相關的資料安全，包含手機安全性功能和個人資料相關保護，如蒐集個人資料的行為必須明確告知使用者。
2	中級	進階資料保護	智慧型手機提供完整資料保護機制，包含使用中、儲存及傳輸中的資料，確保所有資料在各狀態下可被安全使用。
3	高級	機密型資料保護	智慧型手機須確保核心底層不被篡改或被不正當的獲取資訊。

(三)智慧型手機風險評估矩陣

綜上所述之風險評估框架，彙整智慧型手機風險評估矩陣，以供後續檢測規範發展之參考，詳見表 4 所示。

表4　智慧型手機風險評估矩陣表

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
M4：Unintended Data Leakage(非故意的資料洩漏)	D.1	D.1.1.B	資料使用授權	手機系統內建軟體於存取敏感性資料前，應取得使用者同意	初
M5：Poor Authorization and Authentication(不	D.1	D.1.2.M(+)	資料使用授權	手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。	中

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
安全的授權與鑑別)					
M2：Insecure Data Storage(不安全的資料儲存)	D.2	D.2.1.B	資料儲存保護	手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。	初
M2：Insecure Data Storage(不安全的資料儲存)	D.2	D.2.2.M(+)	資料儲存保護	手機系統內建軟體於儲存敏感性資料時提供資料加密功能，以避免遭不正當方式取得敏感性資料。	中
M2：Insecure Data Storage(不安全的資料儲存)	D.2	D.2.3.M(+)	資料儲存保護	手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於程式碼中，以避免遭不正當的方式存取。	中
M2：Insecure Data Storage(不安全的資料儲存)	D.3	D.3.1.B	資料遺失保護	手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，讓使用者可在遠端啟動鎖定。	初
M2：Insecure Data Storage(不安全的資料儲存)	D.3	D.3.2.B	資料遺失保護	手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，讓使用者可在遠端移除資料。	初

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
M2：Insecure Data Storage(不安全的資料儲存)	D.3	D.3.3.B	資料遺失保護	手機系統應提供資訊備份功能。	初
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.1	A.1.1.B	程式身分辨識	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。	初
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.2	A.2.1.B	程式信任來源	手機系統內建軟體具備付費服務時，應使用有效期間之伺服器憑證，以避免使用過期的憑證。(A.2.1.B(+)適用無圖示軟體)	初
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.2	A.2.2.B	程式信任來源	手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。	初
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.3	A.3.1.B	程式執行授權	手機系統內建軟體在使用付費服務前，應提示並取得使用者同意後才可執行。	初
M5：Poor Authorization and Authentication(不	A.3	A.3.2.B	程式執行授權	手機系統內建軟體應僅使用其所需之權限，且權限須與「廠商自我宣告表」所宣告之「功	初

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
安全的授權與鑑別)				能說明」與「權限說明」相符。	
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	A.3	A.3.3.M	程式執行授權	手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路服務連接埠(本地服務)」相符。(A.3.3.M(+)適用無圖示軟體)	中
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.3	A.3.4.M(+)	程式執行授權	手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。	中
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	A.3	A.3.5.M(+)	程式執行授權	手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。	中
M7：Client Side Injection(使用者端注入)	A.4	A.4.1.B	程式執行安全	手機系統內建軟體應提供回報安全性問題之管道	初
M7：Client Side Injection(使用者端注入)	A.4	A.4.2.M	程式執行安全	手機系統內建軟體應具隱碼攻擊字串的處理能力。	中
M7：Client Side Injection(使用者端注入)	A.4	A.4.3.M	程式執行安全	手機系統內建軟體應具延伸標記語言攻擊字串的處理能力。	中

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	P.1	P.1.1.B	協定使用授權	手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。	初
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	P.1	P.1.2.B	協定使用授權	當手機之無線傳輸技術功能確認開啟時，應給予使用者相對應的提示狀態。	初
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	P.1	P.1.3.B	協定使用授權	手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。	初
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	P.2	P.2.1.B	協定傳輸保護	手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。(P.2.1.B(+)適用無圖示軟體)	初
M9：Improper Session Handling(不適當的通訊控制)	P.2	P.2.2.M	協定傳輸保護	手機系統內建軟體應避免交談識別碼遭重送攻擊。	中
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	P.2	P.2.3.M	協定傳輸保護	手機系統內建軟體與付費服務伺服器間之資料加密傳輸，應使用安全之加密演算法。	中

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
				(P.2.3.M(+)適用無圖示軟體)	
M9：Improper Session Handling(不適當的通訊控制)	P.3	P.3.1.M	協定執行安全	手機系統內建軟體應具通訊協定內容的錯誤處理能力。	中
M4：Unintended Data Leakage(非故意的資料洩漏)	O.3	O.3.2.M	系統執行安全	手機之作業系統應具位址空間配置隨機化功能，以避免程式與參考函式在記憶體中的位址為固定值。	中
M3：Insufficient Transport Layer Protection(不充分的傳輸層保護)	O.3	O.3.3.H	系統執行安全	手機之作業系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。	高
M4：Unintended Data Leakage(非故意的資料洩漏)	O.3	O.3.4.H	系統執行安全	手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。	高
M5：Poor Authorization and Authentication(不安全的授權與鑑別)	O.3	O.3.5.H	系統執行安全	手機之作業系統應具備驗證錯誤計數機制，當嘗試錯誤超過門檻值，應抹除受保護之資訊。	高
M6：Broken Cryptography(不安全的加密保護)	H.1	H.1.1.H	金鑰管理保護	手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀。應符合 NIST、ANSI 及	高

OWASP Mobile TOP 10	檢測項目編號	檢測編號	檢測項目	檢測細項	安全等級
				IEEE 發布之金鑰使用及管理標準。	
M6：Broken Cryptography(不安全的加密保護)	H.1	H.1.2.H	金鑰管理保護	手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。	高
M6：Broken Cryptography(不安全的加密保護)	H.1	H.1.3.H	金鑰管理保護	金鑰不得以明文方式存放於非揮發性之記憶體、且不得用任何方式匯出或直接對外傳輸。	高
M6：Broken Cryptography(不安全的加密保護)	H.2	H.2.1.H	演算法強度要求	手機實作之加/解密及簽章演算法，應符合NIST、ANSI 及 IEEE 發布之金鑰演算法標準。	高
M6：Broken Cryptography(不安全的加密保護)	H.2	H.2.2.H	演算法強度要求	手機實作之演算法，應依據各模式要求，產生初始化向量，並符合NIST 發布之初始化向量要求。	高
M6：Broken Cryptography(不安全的加密保護)	H.2	H.2.3.H	演算法強度要求	金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。	高

附件 3 智慧型手機系統內建軟體資通安全檢測技術規範草案

國家通訊傳播委員會

智慧型手機系統內建軟體資通安全檢測

技術規範草案

(V0.9)

執行單位：中華民國資訊軟體協會

日 期 ：１０５ 年 ０６ 月

目 次

1. 概說.....附件 3-1-1
2. 目的.....附件 3-1-1
3. 適用範圍.....附件 3-1-1
4. 用語釋義.....附件 3-1-2
5. 檢測要求.....附件 3-1-10
6. 檢測項目.....附件 3-1-13
7. 附件.....附件 3-1-48

1. 概說

網路無遠弗屆，智慧型手機基於高度可攜性與便利性，有效提升生產力與工作效率，但隨之而來，使用者也必須面對智慧型手機所帶來的資安威脅。有鑒於此，行政院國家資通安全會報於 103 年 6 月 24 日第 26 次會議決議，參考各國手機管制機制及協調我國相關政府機關分工，由經濟部主管手機與電腦之應用軟體基本資安規範，另智慧型手機屬電信法第 42 條規定之電信終端設備，其出廠時已內建之軟體基本資安規範，則由國家通訊傳播委員會主管，故而國家通訊傳播委員會制訂「智慧型手機系統內建軟體安全檢測技術規範」（以下簡稱「本規範」），作為智慧型手機製造商、代理商或是行動通信服務業者等辦理檢測之依據。

2. 目的

本規範旨在提供業界依循標準，在智慧型手機出廠至消費者使用前，加強智慧型手機資安防護，強化我國對於智慧型手機之資安品質要求、提升消費者對於智慧型手機信賴度與使用意願。

惟資訊安全本質為風險控管概念，智慧型手機系統內建軟體經本規範檢測通過後，並不能完全保證受測後的智慧型手機不會被惡意破解或遭到駭客攻擊，使用者應搭配良好的使用習慣，並隨時提高資安警覺，以降低資安問題所帶來的風險與影響程度。

3. 適用範圍

本規範適用於智慧型手機系統及其內建軟體，以確保其符合現階段資訊安全要求，但不包含使用者於內建軟體中自行付費下載之附加服務或內容。

為配合不同安全需求，本規範將智慧型手機系統內建軟體安全等級區分為初級、中級及高級 3 種：初級為智慧型手機基本隱私保護最低要求；中級必須符合初級所有檢測細項並增加資料進階保護

之檢測細項；高級主要為確保智慧型手機之核心底層不會被竄改或不正當地擷取資訊，因此須符合初級與中級所有檢測細項，並納入手機設計相關安全性文件審定之檢測細項。

安全等級說明如表 1，安全等級、檢測項目與檢測細項對應關係如附件 6。

表 1　安全等級說明

安全等級 (編號代碼)	要求	說明
初 (B)	基本隱私保護	智慧型手機提供個人隱私相關的資料安全，包含手機安全性功能和敏感性資料相關保護，如蒐集敏感性資料的行為必須明確告知使用者。
中 (M)	進階資料保護	智慧型手機提供完整資料保護機制，包含所有資料在使用、儲存及傳輸時，皆可被安全保護。
高 (H)	機密型資料保護	智慧型手機確保核心底層不被竄改或被不正當的獲取資訊。

4. 用語釋義

4.1 加密（Encryption）

係指利用數學演算法處理電子資料，使資料不會以原來的形式呈現，達到保密的目的，並且可透過解密方式取得加密資料原文內容。

4.2 本地服務（Local Port）

係指系統內建軟體因服務需求，綁定並開啟固定之網路埠號(端口)。

4.3 交談識別碼（Session Identification，Session ID）

係指在建立連接時，指派給每個使用者連接的唯一工作階段識別碼。當連接結束時，即釋出該識別碼，讓伺服器重新指派給新的使用者連接。

4.4 近場通訊技術（Near Field Communication，NFC）

係指一種近距離（通常小於 10 公分）的無線通訊技術，主要運作頻率是 13.56 MHz，資料傳輸速度每秒最高可達 424 Kbps。NFC 包含三種模式，分別為點對點模式（Peer-to-Peer Mode）、讀寫模式（Read/Write Mode）及卡片模擬模式（Card Emulation Mode），其中卡片模擬模式可模擬多種實體卡片功能，如信用卡、悠遊卡等，當近場通訊技術使用卡片模擬模式時，可在無電力供應情況下使用。

4.5 非作業系統保護區（Non-Operating System Protection Area）

係指使用者透過外部裝置（如電腦）連接手機，在非管理者權限下可存取之空間，包含手機本身儲存空間和出廠時提供的外接記憶卡。

4.6 隱碼攻擊（Injection）

係指利用應用程式的漏洞執行非預期之外部程式或指令，進而取得未經授權之資料或控制整個應用程式與系統，常見的型態例如資料庫的語法（SQL Injection）或作業系統相關的指令（OS Command Injection）等攻擊。

4.7 延伸標記語言 隱碼攻擊（XML Injection）

係指一種網路攻擊手法，XML 格式的檔案常用來作為應用程式的輸入和輸出，當應用程式以 XML 格式作為執行作業的輸入時，攻擊者可能透過變更 XML 格式的結構或資料，以此來篡改重要檔案

或資料之內容，達到入侵目的。

4.8 個人資料（Personal Data）

指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

4.9 敏感性資料（Sensitive Data）

指內容遭外洩或竄改將可能導致個人或資料擁有者的權益受損之個人資料或手機相關資訊。

4.10 資料型別 （Data Type）

本規範依資料之敏感性與是否為使用者輸入等兩個因素分成第 1 型、第 2 型、第 3 型及第 4 型(如表 2 **錯誤! 找不到參照來源。**)，其中第 1 型及第 2 型為敏感性資料。

表 2 資料型別分類表

型別	判斷標準		範例
	是否屬於敏感性資料	是否為使用者輸入	
第 1 型	是	是	1.本規範用語釋義之個人資料。 2.手機相關資訊：簡訊內容、通話錄音、裝置密碼、帳號密碼、相片。
第 2 型	是	否	IMEI、IMSI[註]、定位資訊。
第 3 型	否	否	APP 列表、音樂播放資訊、手機作業系統、手機型號、手機韌體版本、MCC、MNC、行動通信業者、網路傳送方式、設

型別	判斷標準		範例
	是否屬於敏感性資料	是否為使用者輸入	
			定檔。
第 4 型	N/A	N/A	資料加密、協定加密、無加密但內容未知。
[註]IMEI 碼及 IMSI 碼須與行動通信業者或手機廠商之銷售保固連結，該 IMEI 碼及 IMSI 碼才具備個資識別性，但使用人與登錄人可能不同，故歸類為第 2 型。			

4.11 強健性測試（Robustness Testing）

係指透過製造錯誤或不可預期的輸入來驗證程式的強健性，主要對於作業系統、行動應用程式或網路服務在執行過程中，遭遇輸入、運算等異常時，其錯誤處理程序或演算法繼續正常執行能力的測試。

4.12 國際行動用戶識別碼（International Mobile Subscriber Identity，IMSI）

係指結合所有 GSM 與 UMTS 網路行動裝置用戶的唯一識別碼。IMSI 由一串 10 進位數組成，最大長度為 15 位，在行動電話裡面的 SIM 卡上所標示前三位數代表行動裝置國碼（Mobile Country Code， MCC)；接續是行動裝置網路碼（Mobile Network Code，MNC)，它是 3 位數（北美標準式）或 2 位數（歐洲標準式)；其餘的位數代表行動訂閱辨識碼（Mobile Subscription Identification Number，MSIN)，該數值由營運商自行分配，因此 IMSI 是由 MCC、MNC 及 MSIN 三種代表碼依次連接而成。

4.13 國際行動設備識別碼（International Mobile Equipment

Identity，IMEI）

係指行動網路中識別每一部獨立的行動通訊裝置，相當於該裝置之身分證。序列號共有 15 位數字，前 6 位（Type Approval Code，TAC）是型號核准號碼，代表手機類型；接著 2 位（Final Assembly Code，FAC）是最後裝配號，代表產地；後 6 位（Serial Number, SNR）是序號，代表生產順序號；最後 1 位（SP）是檢驗碼，一般為 0。國際行動設備識別碼一般貼於機身背面與外包裝上，同時也存在於手機記憶體中。

4.14 密碼（Password）

係指為特定應用中，用於保護特定資料的一組字串，通常用於身分識別及資料加密。

4.15 使用者同意 （User Agrees）

使用者同意機制係指系統透過訊息提示方式提供使用者選擇「同意」或「不同意」的機制。

使用者同意則係指包含使用者主動操作之行為和系統透過使用者同意機制取得使用者同意之情況。

4.16 無線傳輸技術（Wireless Transfer Technology ）

係指透過無線通訊標準的連接，讓智慧型手機透過網路或點對點等連線方式來傳輸資料，手機使用的無線傳輸技術如藍牙、WLAN、NFC、行動通訊網路、GPS（定位服務）、紅外線及無線充電等。

4.17 無線區域網路（Wireless Local Network，WLAN）

係指透過無線電波、雷射光或紅外線作為傳輸資料的媒介與網路連線，其功能與有線區域網路相同。

4.18 智慧型手機系統內建軟體（Internal Mobile Applications）

係指手機製造商、行動通信服務業者或應用軟體開發商，於使用者初次使用智慧型手機或初次啟用網路服務時，強制安裝之軟體。

4.19 網際網路通訊協定位址（Internet Protocol Address，IP Address）

係指一組 32 位元的數字，該位址可唯一識別 TCP/IP 網路上的主機，簡稱為 IP 位址，一般使用「.」來分隔 4 個 10 進位數字來表示。

4.20 網域名稱（Domain Name ）

係指用以與網際網路位址相對映，便於網際網路使用者記憶 TCP/IP 主機所在位址（即 IP 位址）之文字或數字組合。

4.21 數位簽章（Digital Signature）

係指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，再以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰進行驗證。

4.22 緩衝區溢位攻擊（Buffer Overflow）

係指一種攻擊手法，惡意攻擊者利用程式設計漏洞，輸入超過預定長度的字串或資料，造成程式發生非預期情況，產生緩衝區溢位問題；惡意攻擊者以帶有惡意目的之程式語法或資料插入原有程式碼中，可能導致程式異常停止、執行任意程式碼或取得系統權限等影響。

4.23 憑證（Certificate）

係指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。

4.24 憑證機構（Certification Authority，CA）

係指簽發憑證之機關、法人，為使用者所信任之公正機構，其業務為簽發並管理 X.509 格式之公開金鑰憑證、憑證機構註銷清冊及憑證廢止清冊。

4.25 位址空間配置隨機化（Address Space Layout Randomization，ASLR）

係指於執行程序中將關鍵元件的記憶體位置打亂，使得攻擊方難以定位執行的基址、函式庫、記憶體堆疊（stack）及堆積（heap）等關鍵位址，使其難以正確地執行惡意程式。

4.26 共同準則（Common Criteria，CC）

係指國際資通安全產品評估及驗證之標準（ISO/IEC 15408），依其定義之評估保證等級（Evaluation Assurance Level，簡稱 EAL） 判定產品之安全等級，EAL 共有 7 個等級，最低等級為 EAL 1，最高等級為 EAL 7，提供申請者/贊助者、檢測實驗室與驗證機關（構）評估及驗證資通安全產品安全與功能性，參考網址 http://www.commoncriteriaportal.org。

4.27 評估標的（Target of Evaluation，TOE）

係指申請資通安全評估及驗證之產品及其相關使用手冊。

4.28 保護剖繪（Protection Profile，PP）

係指滿足資通安全產品評估標的(TOE)製作之安全基本需求文件。

4.29 安全標的（Security Target，ST）

係指資通安全產品能符合保護剖繪(PP)或特定安全需求製作之規格文件。

4.30 安全功能需求（Security Functional Requirement，SFR）

係指共同準則第二部分（Common Criteria，Part 2）所定義之安全

相關需求條文，用以描述一資通安全產品之安全功能（TSF）所需滿足的各項要求。此要求條文會被引用於保護剖繪及安全標的中，用以具體陳述該產品功能於安全方面的需求。

4.31 安全功能（TOE Security Functions，TSF）

係指資通安全產品用於實現安全標的（ST）所要求安全功能需求（Security Functional Requirement，SFR）之相關功能。

4.32 安全功能介面（TOE Security Functions Interface，TSFI）

係指評估標的（TOE）用於實現安全功能需求（SFR）之對外溝通介面。

4.33 安全領域（Security Domain）

係指一主動式個體（人或機器）被授權存取的資源集合，為安全架構的屬性之一。

4.34 自我保護（Self-Protection）

係指安全功能可以自動識別自身並加以保護，無法被無關的程式碼或設施破壞，為安全架構的屬性之一。

4.35 防止繞道（Non-Bypassibility）

係指防止避開待測物安全功能檢查之技巧（如：未經過身分鑑別，無法進入稽核功能介面）。

5. 檢測要求

本規範檢測要求包括書面檢視與實機測試兩個部分。書面檢視主要為申請檢測者（以下簡稱申請者）提供書面文件，以利檢測實驗室透過審查書面文件，據以執行檢測項目；實機測試則為檢測實驗室依據檢測項目之檢測方法，對待測之智慧型手機執行實機操作測試。

申請者提出檢測申請後，檢測實驗室應依據本規範所說明之適用範圍進行書面檢視與實機測試。

5.1 內建軟體屬性

智慧型手機系統內建軟體（以下簡稱系統內建軟體）包含出廠預載軟體、銷售商加載軟體及無圖示軟體 3 種屬性，其中無圖示軟體得由申請者自行選擇是否檢測：

(1)出廠預載軟體：智慧型手機出廠時預設搭載安裝之應用程式，且使用者可透過圖示啟動。

(2)銷售商加載軟體：智慧型手機銷售時預設搭載或首次連結網路後自動安裝之應用程式，且使用者可透過圖示啟動。

(3)無圖示軟體：於上述兩種情況所安裝之應用程式，使用者無法透過圖示啟動，且該軟體會將資料回傳至遠端伺服器。

5.2 檢測層別

本規範依據國際間對智慧型手機安全之分層概念，將智慧型手機區分為資料層、應用程式層、通訊協定層、作業系統層及硬體層五個層別，考量不同層別可能面臨的資訊安全風險有所不同，故對各層別分別訂定檢測項目。各檢測層別之主要包含內容如下：

- 資料層（Information/Data）：主要包含資料的傳送、儲存或使

用等相關安全。

- 應用程式層（APPs）：主要包含手機系統內建軟體等相關安全。
- 通訊協定層（Protocol）：主要包含無線傳輸技術及通訊協定等相關安全。
- 作業系統層（Operating System）：主要包含作業系統相關服務與身分辨識等相關安全。
- 硬體層（Hardware）：主要包含金鑰與演算模組等安全。

5.3 資料型別

本規範依資料之敏感性與是否為使用者輸入等兩個因素將資料分成第1型、第2型、第3型及第4型，詳細分類參考表2**錯誤! 找不到參照來源。**。

5.4 書面檢視資料

申請者應填具檢測申請書（詳附件1）及廠商自我宣告表（詳附件2）；申請檢測之安全等級為高級者，應額外填具安全功能規格表（詳附件3）、設計安全性表（詳附件1）及安全架構表（詳附件5）。

5.4.1 檢測申請書

內容包括申請者、製造商相關資訊、送測智慧型手機相關規格，包含廠牌、型號、名稱、作業系統版本、定位功能、無線傳輸技術、生物辨識、外接記憶體等。

5.4.2 廠商自我宣告表

內容包括系統內建軟體名稱、發行商、版本、套件名稱、屬性、功能說明、權限說明、存取資料類型、網路連接埠（本地服務）等。

5.4.3 安全功能規格表

內容包括安全功能介面（TSFI）之名稱、目的、可實現的安全功能需求、操作方式、參數、執行的動作以及錯誤訊息。申請者應完整填列及說明，俾檢測實驗室檢視安全功能介面是否可確實實現安全功能（TSF）需求。

5.4.4 設計安全性表

內容包括如何以子系統組成安全功能規格之安全功能介面，以及安全功能子系統之名稱、目的、子系統隸屬之安全功能介面、子系統行為說明。

5.4.5 安全架構表

內容應依據安全功能規格表、設計安全性表之內容，說明送測設備安全架構如何滿足安全功能需求（SFR），並針對安全功能介面及子系統，提出安全架構的設計概念與操作安全建議。安全架構應說明送測設備因執行安全功能區隔的安全領域、安全功能的安全初始程序、安全功能的自我保護機制，以及安全功能執行如何避免被繞道。

6. 檢測項目

本規範依據檢測層別訂定檢測項目，再依各檢測項目之安全需求訂定檢測細項。檢測項目及安全需求說明如表 3，檢測項目與檢測細項說明如表 4。檢測項目與檢測細項之編碼原則如下：

- 檢測項目編碼：層別代碼.檢測項目編號
- 檢測細項編碼：層別代碼.檢測項目編號.檢測細項編號.安全等級代碼 (+)
- 說明：

(1)層別代碼：

層別	代碼
資料層	D
應用程式層	A
通訊協定層	P
作業系統層	O
硬體層	H

(2)安全等級代碼：

安全等級	代碼
初級	B
中級	M
高級	H

(3)檢測細項編碼標記(+)符號者，為選測項目，由申請者自行選擇是否檢測。

- 範例：

(1)資料層的第 1 個檢測項目編碼為 D.1，其中第 1 個檢測細項為初級，且為必測項目，是以該檢測細項編碼為 D.1.1.B。

(2)資料層的第 2 個檢測項目編碼為 D.2，其中第 2 個檢測細項為中級，且為選測項目，是以該檢測細項編碼為 D.2.2.M(+)。

表 3 檢測項目及安全需求說明

層別	檢測項目	安全需求
資料層	D.1 資料使用授權	手機系統內建軟體對敏感性資料進行存取前，應取得使用者同意。
	D.2 資料儲存保護	手機系統內建軟體應將敏感性資料儲存於作業系統保護區域，並提供資料

層別	檢測項目	安全需求
		加密功能，以避免敏感性資料遭不正當方式存取。
	D.3 資料遺失保護	手機系統應提供資料保護與備份功能，以避免資料外洩和防止資料損失。
應用程式層	A.1 程式身分辨識	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。
	A.2 程式信任來源	手機系統內建軟體應確認付費功能機制與資料來源的安全。
	A.3 程式執行授權	手機系統內建軟體所執行的行為，應取得使用者同意，並與其宣告之內容相符。
	A.4 程式執行安全	手機系統內建軟體應具備惡意字串輸入時的處理能力。
通訊協定層	P.1 協定使用授權	手機與外部設備進行連接時，應給予使用者相對應的提示，並提供開啟及關閉無線傳輸技術之功能。
	P.2 協定傳輸保護	手機系統內建軟體與伺服器間之資料加密傳輸，應使用安全之加密演算法，並避免可能的傳輸攻擊。
	P.3 協定執行安全	手機系統應具備通訊協定內容的錯誤處理能力。
作業系統	O.1 系統操作授權	手機系統所執行的行為，應取得使用者同意，必要時並提供風險提示。
	O.2 系統身分辨識	手機系統應提供安全的身分辨識及保護機制。

層別	檢測項目	安全需求
層	O.3 系統執行安全	手機系統應具備程式執行期的記憶體保護機制，並提供安全回報之管道。
硬體層	H.1 金鑰管理保護	手機之金鑰管理，應符合金鑰使用及管理標準。
	H.2 演算法強度要求	手機實作之加密、解密及簽章演算法，應符合金鑰演算法標準與初始化向量要求。

表 4 檢測項目與檢測細項說明

檢測項目	檢測編號	檢測細項
D.1 資料使用授權	D.1.1.B	手機系統內建軟體於存取敏感性資料前，應取得使用者同意。
	D.1.2.M(+)	手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。
D.2 資料儲存保護	D.2.1.B	手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。
	D.2.2.M(+)	手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。
	D.2.3.M(+)	手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。
D.3 資料遺失保護	D.3.1.B	手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。

檢測項目	檢測編號	檢測細項
	D.3.2.B	手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。
	D.3.3.B	手機系統應提供資料備份功能。
A.1 程式身分辨識	A.1.1.B	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。
A.2 程式信任來源	A.2.1.B	手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。
	A.2.2.B	手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。
A.3 程式執行授權	A.3.1.B	手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。
	A.3.2.B	手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。
	A.3.3.M	手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路連接埠(本地服務)」相符。
	A.3.4.M(+)	手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。
	A.3.5.M(+)	手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。

檢測項目	檢測編號	檢測細項
A.4 程式執行安全	A.4.1.B	手機系統內建軟體應提供回報安全性問題之管道。
	A.4.2.M	手機系統內建軟體應具備隱碼攻擊字串的處理能力。
	A.4.3.M	手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。
P.1 協定使用授權	P.1.1.B	手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。
	P.1.2.B	當手機之無線傳輸技術功能確認開啟時，應給予使用者相對應的提示狀態。
	P.1.3.B	手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。
P.2 協定傳輸保護	P.2.1.B	手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。
	P.2.2.M	手機系統內建軟體應避免交談識別碼遭重送攻擊。
	P.2.3.M	手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。
P.3 協定執行安全	P.3.1.M	手機系統應具備通訊協定內容的錯誤處理能力。
O.1 系統操作授權	O.1.1.B	手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。

檢測項目	檢測編號	檢測細項
	O.1.2.B	手機系統於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。
O.2 系統身分辨識	O.2.1.B	手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。
	O.2.2.B	手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。
	O.2.3.B	手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。
	O.2.4.M	手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。
O.3 系統執行安全	O.3.1.B	手機系統應提供回報安全性問題之管道。
	O.3.2.M	手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。
	O.3.3.H	手機系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。
	O.3.4.H	手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。
	O.3.5.H	手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。

檢測項目	檢測編號	檢測細項
H.1 金鑰管理保護	H.1.1.H	手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。
	H.1.2.H	手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。
	H.1.3.H	金鑰不得以明文方式存放於非揮發性之記憶體，且不得用任何方式匯出或直接對外傳輸。
H.2 演算法強度要求	H.2.1.H	手機實作之加密、解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發布之金鑰演算法標準。
	H.2.2.H	手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。
	H.2.3.H	金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。

6.1 必測項目

以下檢測方法與判定標準說明中，統一將手機系統稱為受測系統，手機系統內建軟體簡稱為受測軟體。檢測實驗室應依下列檢測細項對智慧型手機進行測試，以確保符合本規範之檢測項目。

6.1.1 資料層（Information/Data）

資料之安全性應確保使用者資料避免遭系統內建軟體未經授權之蒐集、分享、使用、刪除、竄改及儲存。

D.1資料使用授權	
D.1.1 .B 手機系統內建軟體於存取敏感性資料前,應取得使用者同意。	
檢測條件： ■ 受測軟體具備存取敏感性資料的功能 ■ 資料型別：第 1 型資料及第 2 型資料 ■ 受測軟體屬性：出廠預載、銷售商加載	
檢測方法	判定標準
(1)開啟受測系統。 (2)檢查受測系統之隱私權政策或使用聲明中，是否提供受測軟體存取敏感性資料之相對應說明和使用者同意機制。 (3)如未符合步驟(2)，則執行受測軟體，並存取使用者敏感性資料。 (4)檢查受測軟體是否提供相對應的使用者同意機制。	步驟(2)中，隱私權政策或使用聲明中有提供受測軟體存取敏感性資料之相對應說明和使用者同意機制。 或步驟(4)中，受測軟體有提供相對應的使用者同意機制。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

D.2資料儲存保護	
D.2.1 .B 手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。	
檢測條件： ■ 受測軟體具備帳號密碼登入功能 ■ 資料型別：帳號密碼 ■ 受測軟體屬性：出廠預載、銷售商加載	
檢測方法	判定標準

(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)執行受測軟體，輸入帳號密碼、同意儲存帳號密碼並成功登入。 (4)使用資料讀取工具對受測軟體在非作業系統保護區內所存放的檔案進行資料讀取。 (5)檢查受測軟體是否將明文帳號密碼存放於非作業系統保護區內。	步驟(5)中，受測軟體未將明文帳號密碼存放於非作業系統保護區內。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

D.3資料遺失保護	
D.3.1 .B 手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。	
檢測條件： ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)開啟受測系統。 (2)設定並執行受測系統的遠端鎖定功能。 (3)檢查受測系統是否被遠端鎖定。	步驟(3)中，受測系統已被遠端鎖定。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
D.3.2 .B 手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。	

<table>
<tr><td colspan="2">檢測條件：
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)輸入測試資料後並儲存。
(3)執行受測系統的遠端刪除功能，並執行遠端刪除步驟(2)輸入之測試資料。
(4)檢查步驟(2)輸入之測試資料是否被刪除。</td><td>步驟(4)中，測試資料已被遠端刪除。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">D.3.3 .B 手機系統應提供資料備份功能。</td></tr>
<tr><td colspan="2">檢測條件：
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)檢查受測系統是否有提供資料備份功能。</td><td>步驟(2)中，受測系統有提供資料備份功能。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
</table>

6.1.2 應用程式層（APPs）

應用程式之安全性應確保系統內建軟體避免未經授權存取系統資源。

<table>
<tr><td colspan="2">A.1 程式身分辨識</td></tr>
<tr><td colspan="2">A.1.1 .B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。</td></tr>
<tr><td colspan="2">檢測條件：
■ 受測軟體具備連接使用者帳戶的功能
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)執行受測軟體之使用者帳戶認證功能。
(4)檢查受測軟體是否提供使用者登入確認並取得授權之機制。</td><td>步驟(4)中，受測軟體於存取使用者帳戶時，有提示使用者認證與授權機制。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
</table>

<table>
<tr><td colspan="2">A.2 程式信任來源</td></tr>
<tr><td colspan="2">A.2.1 .B 手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。</td></tr>
<tr><td colspan="2">檢測條件：
■ 伺服器類型：付費功能的主機
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。</td><td>步驟(4)中，伺服器端提供給受測</td></tr>
</table>

(2)確認已符合檢測條件。 (3)受測軟體透過網路傳輸資料至遠端伺服器。 (4)檢查伺服器端提供給受測軟體的憑證資料是否過期。	軟體的憑證資料未過期。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
A.2.2 .B 手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。	
檢測條件： ■ 資料型別：無 ■ 受測軟體屬性：出廠預載、銷售商加載	
檢測方法	判定標準
(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)檢查受測軟體或廠商自我宣告表是否提供受測軟體的發行商和版本資訊。	步驟(3)中，受測軟體或廠商自我宣告表有提供受測軟體的發行商和版本資訊。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

A.3 程式執行授權
A.3.1 .B 手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。
檢測條件： ■ 受測軟體具備付費功能 ■ 資料型別：無

<table>
<tr><td colspan="2">■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)執行受測軟體，並開啟付費功能。
(4)檢查受測系統或受測軟體是否經使用者同意才執行付費。</td><td>步驟(4)中，受測系統或受測軟體經使用者同意才執行付費。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">A.3.2 .B 手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。</td></tr>
<tr><td colspan="2">檢測條件：
■ 申請者須填寫「廠商自我宣告表」中之「功能說明」與「權限說明」欄位
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)執行及操作受測軟體，並列舉受測軟體所使用的功能及存取權限。
(4)比對步驟(3)列舉之內容是否與廠商自我宣告之內容相符。</td><td>步驟(4)中，步驟(3)列舉之內容與廠商自我宣告之內容相符。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">A.3.3 .M 手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路連接埠(本地服務)」相符。</td></tr>
<tr><td colspan="2">檢測條件：</td></tr>
</table>

■ 受測軟體具備開啟網路連接埠，以提供被連線的功能 ■ 申請者須填寫「廠商自我宣告表」中之「網路連接埠(本地服務)」欄位 ■ 資料型別：無 ■ 受測軟體屬性：出廠預載、銷售商加載	
檢測方法	判定標準
(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)執行受測軟體，並透過檢測工具取得該受測軟體開啟之網路埠號。 (4)檢查步驟(3)取得之網路埠號是否與廠商自我宣告表所宣告之「網路連接埠(本地服務)」相符。	步驟(4)中，取得之網路埠號與廠商自我宣告表所宣告之「網路連接埠(本地服務)」相符。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

A.4 程式執行安全	
A.4.1 .B 手機系統內建軟體應提供回報安全性問題之管道。	
檢測條件： ■ 資料型別：無 ■ 受測軟體屬性：銷售商加載	
檢測方法	判定標準
(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)檢查受測軟體、官方網站或使用說明書是否提供問題回報管道。	步驟(3)中，受測軟體發現的問題可透過問題回報管道回報。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

<table>
<tr><td colspan="2">A.4.2 .M 手機系統內建軟體應具備隱碼攻擊字串的處理能力。</td></tr>
<tr><td colspan="2">檢測條件：
■ 受測軟體具備可供使用者輸入資料之欄位
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)執行受測軟體，並輸入資料隱碼攻擊字串。
(4)檢查步驟(3)之受測軟體是否執行隱碼攻擊字串。</td><td>步驟(4)中，受測軟體未執行資料隱碼攻擊字串。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">A.4.3 .M 手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。</td></tr>
<tr><td colspan="2">檢測條件：
■ 受測軟體可接收延伸標記語言
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)執行受測軟體之網路傳輸功能。
(4)使用檢測工具攔截遠端主機至受測軟體間之通訊封包。
(5)將延伸標記語言攻擊字串注入步驟(4)攔截之通訊封包中後，傳送</td><td>步驟(6)中，受測軟體未執行注入攻擊字串。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
</table>

至受測軟體。 (6)檢查受測軟體是否執行注入攻擊字串。	

6.1.3 通訊協定層（Protocol）

通訊協定之安全性應確保使用者對資料之傳輸、周邊設備之連接的可控管性。

P.1 協定使用授權	
P.1.1 .B 手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。	
檢測條件： ■ 受測的無線傳輸技術：藍牙、WLAN、NFC(Peer-to-Peer 模式和 Read/Write 模式)、行動通訊網路及 GPS(定位服務) ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)檢查手機是否提供無線傳輸技術功能的開啟及關閉介面，並確認手機狀態是否與顯示狀態相符。	步驟(3)中，手機有提供無線傳輸技術功能的開啟及關閉介面，且手機狀態與顯示狀態相符。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
P.1.2 .B 當手機之無線傳輸技術功能確認開啟時，應給予使用者相對應的提示狀態。	
檢測條件： ■ 受測的無線傳輸技術：藍牙、WLAN、NFC(Peer-to-Peer 模式和	

<table>
<tr><td colspan="2">Read/Write 模式)、行動通訊網路及 GPS(定位服務)
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)開啟手機之無線傳輸技術功能。
(4)檢查手機是否提供相對應的提示狀態。</td><td>步驟(4)中，手機有提供使用者相對應的提示狀態。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">P.1.3 .B 手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。</td></tr>
<tr><td colspan="2">檢測條件：
■ 受測的無線傳輸技術：藍牙及 WLAN
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)開啟手機之無線傳輸技術功能。
(4)開啟另一臺具備無線傳輸技術對應可被連線之設備，並與手機連接。
(5)於受測系統選擇拒絕或不接受連線功能。
(6)檢查受測系統是否能與步驟(4)之設備建立連線。</td><td>在步驟(6)中，受測系統無法與步驟(4)之設備建立連線。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
</table>

<table>
<tr><td colspan="2">P.2 協定傳輸保護</td></tr>
<tr><td colspan="2">P.2.1 .B 手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。</td></tr>
<tr><td colspan="2">檢測條件：
■ 無線傳輸技術：藍牙、WLAN 及行動通訊網路
■ 資料型別：第 1 型資料(不包含相片)及定位資訊
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)執行受測軟體，並以無線傳輸技術功能傳輸敏感性資料。
(4)檢查受測軟體是否以明文方式傳輸敏感性資料。</td><td>步驟(4)中，受測軟體未以明文方式傳輸敏感性資料。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">P.2.2 .M 手機系統內建軟體應避免交談識別碼遭重送攻擊。</td></tr>
<tr><td colspan="2">檢測條件：
■ 受測軟體透過網路傳輸資料時具備交談識別碼
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)執行受測軟體之網路傳輸功能。
(4)使用檢測工具側錄受測軟體與遠端主機間之通訊封包，並擷取交</td><td>步驟(5)中，電腦主機使用交談識別碼執行重送攻擊並無效果。

若「符合」判定標準，則本檢測細項通過；</td></tr>
</table>

談識別碼。 (5)將步驟(4)中之交談識別碼，透過電腦主機執行重送攻擊。	若「不符合」判定標準，則本檢測細項不通過。
P.2.3 .M 手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。	
檢測條件： ■ 伺服器類型：付費功能的主機 ■ 申請者須提供書面資料作為審查依據 ■ 必要時，檢測實驗室得請申請者進行功能示範 ■ 資料型別：無 ■ 受測軟體屬性：出廠預載、銷售商加載	
檢測方法	判定標準
(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)執行受測軟體之網路傳輸功能。 (4)使用通訊加密演算法檢測軟體，檢查受測軟體所存取之伺服器，其使用之加密演算法為 FIPS 140 核准之加密編譯演算法或由申請者提供同等安全性之佐證資料。	步驟(4)中，受測軟體與伺服器端之通訊加密演算法為 FIPS 140 核准之加密編譯演算法或申請者提供足以證明達同等安全性之佐證資料。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

P.3 協定執行安全
P.3.1 .M 手機系統應具備通訊協定內容的錯誤處理能力。
檢測條件： ■ 受測的無線傳輸技術：藍牙及 WLAN

■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)針對手機之無線傳輸技術介面，在通訊連線交涉(Negotiation)階段，使用檢測工具針對使用的通訊協定發送超過一萬個不同測試封包。 (4)檢查無線傳輸技術介面或受測系統是否仍正常運作。	步驟(4)中，受測系統均可正常進行通訊連線與資料傳輸，且正常運作。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

6.1.4 作業系統（Operating System）

作業系統之安全性應確保作業系統對系統資源之保護、提醒，並讓使用者於知情的狀況下進行更新。

O.1系統操作授權	
O.1.1 .B 手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。	
檢測條件： ■ 受測系統具備作業系統更新功能 ■ 申請者須填寫「廠商自我宣告表」中之「資料連結伺服器之 IP/DN/公司主機名稱」欄位 ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準

(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)透過受測系統內建作業系統更新功能執行作業系統更新。 (4)透過檢測工具取得作業系統更新之連線目的地位址。 (5)檢查步驟(4)中目的地位址是否與廠商自我宣告之內容相符。	步驟(5)中，目的地位址與廠商自我宣告之內容相符。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
O.1.2 .B 手機系統於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。	
檢測條件： ■ 受測系統具備作業系統更新功能 ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)檢查受測系統或官網是否提供作業系統更新資訊，並告知使用者更新之內容或未更新可能造成安全風險之資訊。	步驟(3)中，受測系統或官網有提供作業系統更新資訊及相關安全風險之訊息。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

O.2系統身分辨識
O.2.1 .B 手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。

檢測條件： ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)開啟受測系統。 (2)開啟受測系統之螢幕鎖定設定功能介面，並設定螢幕鎖定方式及解鎖資料。 (3)鎖定受測系統(包含關閉螢幕及關閉受測系統)。 (4)喚醒受測系統(包含開啟螢幕及開啟受測系統)，並操作解鎖方式。 (5)檢查是否可以步驟(3)所設定的解鎖資料喚醒受測系統。	步驟(5)中，可以步驟(2)所設定之密碼喚醒受測系統。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
O.2.2 .B 手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。	
檢測條件： ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)開啟受測系統。 (2)開啟螢幕鎖定設定功能介面並設定螢幕鎖定方式及解鎖資料。 (3)鎖定受測系統。 (4)喚醒受測系統，並重複輸入數次錯誤的解鎖資料。 (5)檢查受測系統是否顯示強制鎖定的訊息。	步驟(5)中，受測系統有顯示強制鎖定的訊息。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

<table>
<tr><td colspan="2">O.2.3 .B 手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。</td></tr>
<tr><td colspan="2">檢測條件：
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)開啟輸入密碼設定介面。
(3)檢查受測系統提供之密碼輸入值，是否包含英文大寫、英文小寫、數字及特殊符號，且達 72 種以上。
(4)檢查密碼長度是否可達 14 碼以上。</td><td>步驟(3)中，受測系統提供之密碼輸入值有包含英文大寫、英文小寫、數字及特殊符號，且達 72 種以上。
且步驟(4)中，密碼長度可達 14 碼以上。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">O.2.4 .M 手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。</td></tr>
<tr><td colspan="2">檢測條件：
■ 申請者須提供智慧型手機管理者權限
■ 螢幕鎖定功能：圖形、密碼及生物特徵
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。</td><td>步驟(4-1)或(4-2)中，未以明文方式將螢幕鎖定解鎖資料儲存於手機上。</td></tr>
</table>

(3)開啟螢幕鎖定設定功能介面並設定螢幕鎖定方式及解鎖資料。 (4-1)以管理者權限身分確認解鎖資料是否以明文方式儲存於手機上。 (4-2)未能提供管理者權限者，得提供足以證明符合本測試細項之詳細說明、畫面及截圖等佐證資料，必要時檢測實驗室得要求申請者做功能示範。	若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

O.3系統執行安全	
O.3.1 .B 手機系統應提供回報安全性問題之管道。	
檢測條件： ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)開啟受測系統。 (2)檢查受測系統、官方網站或使用說明書是否提供問題回報管道。	步驟(2)中，受測系統發現的問題可透過問題回報管道回報。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
O.3.2 .M 手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。	
檢測條件： ■ 申請者須提供書面資料作為審查依據 ■ 必要時請申請者進行功能示範	

■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)依書面資料審查是否具備此功能。 (2)當無充分資料顯示具備此功能時，則請申請者做功能示範。	於步驟(1)或(2)中，受測系統具備記憶體配置保護機制。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
O.3.3 .H 手機系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。	
檢測條件： ■ 申請者須提供書面資料作為審查依據 ■ 必要時請申請者進行功能示範 ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)依書面資料審查是否具備此功能。 (2)當無充分資料顯示具備此功能時，則請申請者做功能示範。	於步驟(1)或(2)中，受測系統之傳輸過程具備安全通道。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
O.3.4 .H 手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。	

<table>
<tr><td colspan="2">檢測條件：
■ 申請者須提供書面資料作為審查依據
■ 必要時請申請者進行功能示範
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)依書面資料審查是否具備此功能。
(2)當無充分資料顯示具備此功能時，則請申請者做功能示範。</td><td>於步驟(1)或(2)中，受測系統之開機過程具備自我安全功能測試。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">O.3.5 .H 手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。</td></tr>
<tr><td colspan="2">檢測條件：
■ 申請者須提供書面資料作為審查依據
■ 必要時請申請者進行功能示範
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)依書面資料審查是否具備此功能。
(2)當無充分資料顯示具備此功能時，則請申請者做功能示範。</td><td>於步驟(1)或(2)中，受測系統之認證失敗處理方式符合資料覆蓋方式安全抹除受保護之資料。

若「符合」判定標準，則本檢測細項通過；</td></tr>
</table>

	若「不符合」判定標準，則本檢測細項不通過。

6.1.5 硬體層（Hardware）

硬體之安全性應確保金鑰管理、存放之保護，並確保演算法之安全強度符合國際規範，並確保使用者於知情的狀況下進行更新。

H.1金鑰管理保護	
H.1.1.H 手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。相關標準臚列如下： ANSI X9.31-1998、 IEEE 802.11-2012、 IEEE 802.11ac-2013、 IEEE 802.1X、 NIST SP 800-38A, 38C~F, 56A~B, 57, 90B	
檢測條件： ■ 申請者須提供書面資料作為審查依據 ■ 必要時請申請者進行功能示範 ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)依書面資料審查是否具備此功能。 (2)當無充分資料顯示具備此功能時，則請申請者做功能示範。	於步驟(1)或(2)中，受測硬體之金鑰管理符合機密性與完整性之要求。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢

	測細項不通過。
H.1.2.H 手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。	
檢測條件： ■ 申請者須提供書面資料作為審查依據 ■ 必要時請廠商進行功能示範 ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)依書面資料審查是否具備此功能。 (2)當無充分資料顯示具備此功能時，則請申請者做功能示範。	於步驟(1)或(2)中，受測硬體之金鑰儲存保護機密性與完整性之要求。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
H.1.3.H 金鑰不得以明文方式存放於非揮發性之記憶體，且不得用任何方式匯出或直接對外傳輸。	
檢測條件： ■ 申請者須提供書面資料作為審查依據 ■ 必要時請申請者進行功能示範 ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)依書面資料審查是否具備此功能。 (2)當無充分資料顯示具備此功能	於步驟(1)或(2)中，受測硬體之金鑰傳輸保護符合不匯出或傳輸之要求。

時，則請申請者做功能示範。	若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

H.2 演算法強度要求	
H.2.1.H 手機實作之加密、解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發布之金鑰演算法標準。相關標準臚列如下： ANSI X9.31-1998、 IEEE 802.11-2012、 IEEE 802.11ac-2013、 IEEE 802.1X、 NIST SP 800-38A, 38C~F, 56A~B, 57, 90B	
檢測條件： ■ 申請者須提供書面資料作為審查依據 ■ 必要時請申請者進行功能示範 ■ 資料型別：無 ■ 受測軟體屬性：無	
檢測方法	判定標準
(1)依書面資料審查是否具備此功能。 (2)當無充分資料顯示具備此功能時，則請申請者做功能示範。	於步驟(1)或(2)中，受測硬體之演算法符合技術要求。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

<table>
<tr><td colspan="2">H.2.2.H 手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。相關標準為：
NIST SP 800-38A, 38C~F, 56A~B, 57, 90B</td></tr>
<tr><td colspan="2">檢測條件：
■ 申請者須提供書面資料作為審查依據
■ 必要時請申請者進行功能示範
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)依書面資料審查是否具備此功能。
(2)當無充分資料顯示具備此功能時，則請申請者做功能示範。</td><td>於步驟(1)或(2)中，受測硬體之初始向量符合技術要求。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">H.2.3.H 金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。相關標準臚列如下：
NIST SP 800-90A、
ANSI X9.31-1998</td></tr>
<tr><td colspan="2">檢測條件：
■ 申請者須提供書面資料作為審查依據
■ 必要時請申請者進行功能示範
■ 資料型別：無
■ 受測軟體屬性：無</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)依書面資料審查是否具備此功</td><td>於步驟(1)或(2)中，受測硬體之亂</td></tr>
</table>

能。 (2)當無充分資料顯示具備此功能時，則請申請者做功能示範。	數符合技術要求。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

6.2 選測項目

本章節將說明檢測規範中屬於選測項目之內容，由申請者自行選擇是否檢測。

6.2.1 資料層（Information/Data）選測項目

D.1 資料使用授權	
D.1.2.M(+)手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。	
檢測條件： ■ 申請者須提供書面資料作為審查依據 ■ 必要時請申請者進行功能示範 ■ 受測軟體具備拒絕存取敏感性資料的功能 ■ 資料型別：第 1 型資料及第 2 型資料 ■ 受測軟體屬性：出廠預載、銷售商加載	
檢測方法	判定標準
(1)開啟受測系統。 (2)檢查受測系統之隱私權政策或使用聲明中，是否提供受測軟體存取敏感性資料之相對應說明和使用者同意機制。	步驟(3)中，受測系統無法繼續操作。 或於步驟(5)、(6)中，受測軟體無法繼續操作或無法存取使用者敏感性資料。

(3)如步驟(2)中有提供受測軟體存取敏感性資料之相對應說明和使用者同意機制，則選擇拒絕隱私權政策或使用聲明，並檢查受測系統能否繼續操作。 (4)如步驟(2)中無提供受測軟體存取敏感性資料之相對應說明和使用者同意機制，則執行受測軟體，並拒絕受測軟體存取敏感性資料。 (5)檢查受測軟體是否仍可存取敏感性資料。 (6)當無充分資料顯示具備此功能時，則請申請者做功能示範。	若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

D.2 資料儲存保護	
D.2.2.M(+)手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。	
檢測條件： ■ 申請者須提供智慧型手機管理者權限 ■ 受測軟體具備儲存敏感性資料的功能 ■ 資料型別：第 1 型資料(不包含相片) ■ 受測軟體屬性：出廠預載、銷售商加載	
檢測方法	判定標準
(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)執行受測軟體，並儲存敏感性資	步驟(4)中，受測軟體未以明文方式儲存敏感性資料。

料。 (4)以管理者權限身分使用資料讀取工具，檢查步驟(3)之受測軟體是否以明文方式儲存敏感性資料。	若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。
D.2.3.M(+)手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。	
檢測條件： ■ 申請者須提供智慧型手機管理者權限 ■ 受測軟體具備帳號密碼登入功能 ■ 資料型別：帳號密碼 ■ 受測軟體屬性：出廠預載、銷售商加載	
檢測方法	判定標準
(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)使用資料讀取工具對受測軟體執行檔進行資料讀取。 (4)檢查步驟(3)之受測軟體執行檔中是否以明文方式儲存與遠端伺服器溝通之帳號密碼。	步驟(4)中，執行檔中未以明文方式儲存與遠端伺服器溝通之帳號密碼。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

6.2.2 應用程式層（APPs）選測項目

A.3 程式執行授權
A.3.4.M(+)手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。
檢測條件： ■ 申請者須提供智慧型手機管理者權限

<table>
<tr><td colspan="2">■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)執行受測軟體，並操作其功能。
(4)透過比對通話紀錄、簡訊資料檔案之檔案時間戳記等方式，檢查是否有背景撥打電話、發送簡訊等記錄。</td><td>步驟(4)中，未發現有背景撥打電話、發送簡訊之紀錄。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
<tr><td colspan="2">A.3.5.M(+)手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。</td></tr>
<tr><td colspan="2">檢測條件：
■ 受測軟體為非常駐程式
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1)開啟受測系統。
(2)確認已符合檢測條件。
(3)瀏覽執行中的應用程式清單。
(4)執行並操作受測軟體。
(5)關閉步驟(4)執行之受測軟體，並再次瀏覽執行中的應用程式清單，。
(6)檢查步驟(5)之清單是否與步驟(3)之清單相同。</td><td>步驟(6)中，步驟(5)之清單與步驟(3)之清單相同。

若「符合」判定標準，則本檢測細項通過；
若「不符合」判定標準，則本檢測細項不通過。</td></tr>
</table>

6.2.3 無圖示軟體選測

系統內建軟體包含出廠預設軟體、銷售商加載軟體及無圖示軟體3種屬性，如申請者希望了解無圖示軟體之安全性，可自行選擇增加檢測無圖示軟體之檢測項目如表5，詳細檢測細項內容請參閱6.2.1章節。

表5 無圖示軟體之檢測項目與檢測細項

檢測項目	檢測編號	檢測細項
A.2 程式信任來源	A.2.1.B(+)	手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。
A.3 程式執行授權	A.3.3.M(+)	手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路連接埠(本地服務)」相符。
P.2 協定傳輸保護	P.2.1.B(+)	手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。
	P.2.3.M(+)	手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。

7. 附件

附件 1　智慧型手機系統內建軟體資安檢測申請書

申請日期：　年　月　日

<table>
<tr><td colspan="2">申請者
(公司、商號名稱)</td><td>☐製造商
☐代理商</td><td colspan="2">○○○股份有限公司</td><td rowspan="5">申請者用印
(大、小章)</td></tr>
<tr><td colspan="2">統一編號</td><td colspan="3"></td></tr>
<tr><td colspan="2">營業所地址</td><td colspan="3">☐☐☐-☐☐</td></tr>
<tr><td colspan="2">代表人姓名</td><td colspan="3"></td></tr>
<tr><td rowspan="2">聯絡人</td><td>姓名及職稱</td><td></td><td>電子信箱</td><td></td></tr>
<tr><td>聯絡電話</td><td></td><td>傳真機</td><td></td></tr>
<tr><td colspan="2">製造廠商及地址</td><td colspan="4">○○○股份有限公司
☐☐☐-☐☐</td></tr>
<tr><td colspan="3">智慧型手機之廠牌/型號/名稱</td><td colspan="3">ex. APPLE / a16xx / iPhone 6s</td></tr>
<tr><td colspan="3">智慧型手機申請檢測之作業系統版本</td><td colspan="3">○○○-○○○-○○○</td></tr>
<tr><td colspan="2">申請檢測安全等級</td><td colspan="4">☐初 ☐中 ☐中(含選擇檢測項目) ☐高 ☐高(含選擇檢測項目)</td></tr>
<tr><td colspan="2" rowspan="5">智慧型手機基本資訊</td><td>定位功能</td><td colspan="3">☐ 美國全球定位系統 GPS　☐ 歐盟伽利略 Galileo
☐ 俄羅斯格洛納斯 GLONASS　☐ 其他，_____
☐ 中國北斗衛星導航(☐可雙向傳輸)</td></tr>
<tr><td>無線傳輸技術</td><td colspan="3">☐ 藍牙　☐行動通訊網路 (☐2G ☐3G ☐4G)
☐ WLAN　☐其他，_____
☐ NFC (☐ Peer-to-Peer Mode ☐ Read/Write Mode)</td></tr>
<tr><td>生物辨識</td><td colspan="3">☐無 ☐有，指紋辨識、…</td></tr>
<tr><td>外接記憶體</td><td colspan="3">☐無 ☐有，microSD card、…</td></tr>
<tr><td colspan="2" rowspan="3">檢附智慧型手機樣品數量</td><td>初級</td><td colspan="3">☐受測樣品 2 支</td></tr>
<tr><td>中級</td><td colspan="3">☐受測樣品 2 支，並配合檢測項目需要提供管理者權限</td></tr>
<tr><td>高級</td><td colspan="3">☐受測樣品 2 支，並配合檢測項目需要提供管理者權限</td></tr>
<tr><td colspan="2">檢附文件
(正本或影本)</td><td colspan="4">☐ 1.中文或英文之使用手冊或說明書乙份
☐ 2.中文或英文之規格資料乙份
☐ 3.廠商自我宣告表乙份
☐ 4.安全功能規格表、設計安全性表及安全架構表(申請高級者須檢附)
☐ 5.光碟片乙份(含申請書及第 1 項至第 4 項內容)</td></tr>
<tr><td colspan="6">[註 1]檢測實驗室留存光碟片乙份，其餘文件與樣品於出具檢測報告後一併發還申請者。</td></tr>
<tr><td colspan="2">檢測實驗室</td><td colspan="3">實驗室名稱：
實驗室類型：☐第 1 型 ☐第 2 型</td><td>檢測實驗室用印</td></tr>
</table>

<table>
<tr><td rowspan="3">(由實驗室填寫)</td><td colspan="4">☐ 1.出具檢測報告乙份，報告編號：_____，
資通安全等級為：☐初級 ☐中級 ☐高級。
☐ 2.留存本申請書正本及光碟片乙份。</td><td rowspan="3"></td></tr>
<tr><td>受理日期</td><td></td><td>完成日期</td><td></td></tr>
<tr><td>聯 絡 人</td><td></td><td>聯絡電話</td><td></td></tr>
<tr><td colspan="6">[註2]本申請書正本由檢測實驗室自行留存，另申請者應檢具本申請書影本向本會申請審驗。</td></tr>
</table>

附件 2　廠商自我宣告表-1(範例)

受測軟體基本資訊					資料層		通訊協定
項次	受測軟體名稱	發行商及版本	受測套件名稱	受測軟體屬性	是否存取敏感性資料	是否支援無線傳輸技術	是否具帳號密碼登入
1	電話	company 1.2.2	com. android. phone	☐出廠預載軟體 ☐銷售商加載軟體 ☐無圖示軟體	☐否 ☐第 1 型 ☐第 2 型	☐否 ☐Wifi ☐GPS(定位服務) ☐藍牙 ☐行動網路 ☐NFC(Peer-to-Peer 模式) ☐NFC(Read/Write 模式) ☐紅外線 ☐其他____	☐否 ☐是

附件 2　廠商自我宣告表-2(範例)

受測軟體基本資訊			應用層			
項次	**受測軟體名稱**	**發行商及版本**	**功能說明**	**權限說明**	**資料連結伺服器之 IP/DN/公司名稱及伺服器類型**	**是否具網路連接埠 (本地服務)**
1	電話	company 1.2.2	☐常駐軟體 ☐非常駐軟體 說明： 可從通訊錄中撥打電話。	READ_CONTACTS：用於訊息分享功能	apPchat.example.net：一般主機 111.112.113.114：付費功能主機	☐否 ☐是， 埠號：____
				ACCOUNT_MANAGER：用於新增帳號到社群		
				CAMERA：用於圖片紀錄功能		
				INTERNET：用於連線主機，取得最新公告		

[註] 伺服器類型包含一般主機及付費功能主機。

附件 3　安全功能規格表

安全功能介面名稱 TSFI	目的 Purpose	安全功能介面可實現之安全功能需求 SFR	操作方式 Method of Use	參數 Parameter	執行動作 Actions	錯誤訊息 Error Message
列出所有安全功能介面。	說明各安全功能介面之安全功能目的。	說明各安全功能介面如何實現附檢測項目之 O.7~O.11 以及 H.1~H.5 所列之安全功能需求。	說明如何使用各安全功能介面。	說明各安全功能介面所有參數及其意義。	說明各安全功能介面如何運作及其執行細節。	說明執行各安全功能介面產生之錯誤訊息，包含其意義及產生條件。
範例： *TSFI_CLI*	*範例：* *提供命令列模式操作介面*	*範例：* *SFR_安全管理：提供安全管理功能*	*範例：* *以 ssh 連接待測物，即提供命令列模式操作介面*	*範例：* *ID & password*	*範例：* *可下達管理命令操作待測物*	*範例：* *連接失敗* *認證失敗*

附件 4　設計安全性表

子系統名稱 **Subsystem**	**目的** **Purpose**	**子系統隸屬之安全功能介面** **TSFI**	**子系統行為說明** **Behavior Description**
列出各安全功能介面之子系統。	說明各子系統之安全功能目的。	說明各子系統隸屬於附件 3 所列之安全功能介面。	說明各子系統行為如下： (1) 如何實現安全功能介面的功能。 (2) 與其他子系統間互動之資訊，包含不同子系統間的溝通以及傳遞資料的特性。
範例： *Subsystem_ssh*	*範例：* *提供 ssh 服務*	*範例：* *TSFI_CLI*	*範例：* *(1) 提供 TSFI_CLI 命令列模式操作介面* *(2) 與其他子系統之互動：* *(A) Subsystem_auth: 傳遞認證資訊給 Subsystem_auth，並由回覆訊息確認認證是否成功* *(B) Subsystem_terminal: ...*

附件 5　安全架構表

項目	說明	
1.安全領域 Security Domain	**安全領域名稱**	**安全領域說明**
	列出各安全功能介面對應之安全領域 *範例：* *TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection*	在安全功能操作環境及內部執行限制下，如何區隔所需保護的資料。 *範例：* *透過 TSFI_GUI 來執行管理功能石，該 TSFI 同一時間只能有單一遠端連線，並只能執行單一稽核資料處理請求。*

項目	說明	
2.初始程序 Secure Initialization	**相關元件**	**初始程序說明**
	操作待測物的相關元件/環境 *範例：* *待測物網路連接程序*	提供安全啟動待測物之相關元件啟始步驟及安裝程序。 *範例：* *1. 從端口標記為 0/ 0(ethernet0 / 0 接口)連接一個 RJ- 45 電纜到交換機或路由器 Trust 安全區。* *2. 從端口標記為 0/ 1(ethernet0 / 1 接口)連接一個 RJ- 45 電纜到交換機或路由器中的 DMZ 安全區。*

項目	說明		
3.自我保護 Self-Protection	**自我保護功能**	**與外部設備之關係**	**自我保護機制說明**
	列出各安全功能介面對應之自我保護機制 *範例：* *TSFI_WEB:* *自我保護 1:身分驗證* *自我保護 2:遠端連線加密*	說明安全功能及其介面與外部設備之資料交換動作 *範例：* *遠端以瀏覽器連線待測物進行管理功能時，以 TSFI_WEB GUI 介面進行身分認驗證*	需說明安全功能介面提供實體上或邏輯上的自我保護機制 *範例：* *1. 應輸入通行碼才能進入介面。* *2. 資料傳輸機制：TLS/SSL。* *3. 特殊執行方式：指紋辨識。* *4. 特殊設備需求：指紋辨識器。*

項目	說明	
4.防止繞道 Non-Bypassibility	**防止繞道功能**	**防止繞道機制說明**
	列出各安全功能對應之防止繞道機制 *範例：* *TSF_Authentication 身分驗證功能*	1. 列舉可能繞道之手法 2. 說明防範作法，包含進入安全功能的介面如何被保護、執行階段的資料處理如何保護、是否存有其他對外通道及相關防範非法進入之機制等。 *範例：* *可能直接以維護介面不經身分認證操控待測物。* *防範作法：以實體封鎖方式，防止利用維護介面繞道身分認證程序。*

附件 6　檢測細項安全能力分級

註：(+)表示為選擇檢測細項

檢測編號	檢測項目	檢測細項	安全等級		
			初	中	高
D.1	資料使用授權	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。	✓	✓	✓
		D.1.2.M(+)手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。		✓	✓
D.2	資料儲存保護	D.2.1.B 手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。	✓	✓	✓
		D.2.2.M(+)手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。		✓	✓
		D.2.3.M(+)手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。		✓	✓
D.3	資料遺失保護	D.3.1.B 手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。	✓	✓	✓

檢測編號	檢測項目	檢測細項	安全等級		
			初	中	高
		D.3.2.B 手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。	✓	✓	✓
		D.3.3.B 手機系統應提供資料備份功能。	✓	✓	✓
A.1	程式身分辨識	A.1.1.B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。	✓	✓	✓
A.2	程式信任來源	A.2.1.B 手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。(A.2.1.B(+)適用無圖示軟體)	✓	✓	✓
		A.2.2.B 手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。	✓	✓	✓
A.3	程式執行授權	A.3.1.B 手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。	✓	✓	✓
		A.3.2.B 手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。	✓	✓	✓
A.3	程式執行授權	A.3.3.M 手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告		✓	✓

檢測編號	檢測項目	檢測細項	安全等級		
			初	中	高
		表」所宣告之「網路連接埠(本地服務)」相符。(A.3.3.M(+)適用無圖示軟體)			
		A.3.4.M(+)手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。		✓	✓
		A.3.5.M(+)手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。		✓	✓
A.4	程式執行安全	A.4.1.B 手機系統內建軟體應提供回報安全性問題之管道。	✓	✓	✓
		A.4.2.M 手機系統內建軟體應具備隱碼攻擊字串的處理能力。		✓	✓
		A.4.3.M 手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。		✓	✓
P.1	協定使用授權	P.1.1.B 手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。	✓	✓	✓
		P.1.2.B 當手機之無線傳輸技術功能確認開啟時，應給予使用者相對應的提示狀態。	✓	✓	✓
		P.1.3.B 手機以無線傳輸技術功能與其他設備進行第一次連接時，須經	✓	✓	✓

檢測編號	檢測項目	檢測細項	安全等級		
			初	中	高
		使用者同意後才可建立連線。			
P.2	協定傳輸保護	P.2.1.B 手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。(P.2.1.B(+)適用無圖示軟體)	✓	✓	✓
		P.2.2M 手機系統內建軟體應避免交談識別碼遭重送攻擊。		✓	✓
		P.2.3.M 手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。(P.2.3.M(+)適用無圖示軟體)		✓	✓
P.3	協定執行安全	P.3.1.M 手機系統應具備通訊協定內容的錯誤處理能力。。		✓	✓
O.1	系統操作授權	O.1.1.B 手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。	✓	✓	✓
		O.1.2.B 手機系統於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。	✓	✓	✓
O.2	系統身分辨識	O.2.1.B 手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。	✓	✓	✓

檢測編號	檢測項目	檢測細項	安全等級		
			初	中	高
		O.2.2.B 手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。	✓	✓	✓
		O.2.3.B 手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。	✓	✓	✓
		O.2.4.M 手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。		✓	✓
O.3	系統執行安全	O.3.1.B 手機系統應提供回報安全性問題之管道。	✓	✓	✓
		O.3.2.M 手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。		✓	✓
		O.3.3.H 手機系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。			✓
		O.3.4.H 手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。			✓
		O.3.5.H 手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定			✓

檢測編號	檢測項目	檢測細項	安全等級		
			初	中	高
		門檻值時，應抹除受保護之資訊。			
H.1	金鑰管理保護	H.1.1.H 手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。			✓
		H.1.2.H 手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。			✓
		H.1.3.H 金鑰不得以明文方式存放於非揮發性之記憶體，且不得用任何方式匯出或直接對外傳輸。			✓
H.2	演算法強度要求	H.2.1.H 手機實作之加密、解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發布之金鑰演算法標準。			✓
		H.2.2.H 手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。			✓
		H.2.3.H 金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。			✓

National Communications Commission

Security Criteria for Embedded Software of Smartphone

Technical Specifications (Draft)

(V0.9)

Executive: Information Service Industry

Association of ROC

Date: February 2016

CONTENTS

1. **Summary.....2**
2. **Purpose.....2**
3. **Scope.....3**
4. **Definitions of terms.....4**
5. **Test/Inspection Requirement 14**
6. **Test Items 18**
7. **Attachment 60**

1. Summary

The Internet has become ubiquitous in or lives. It's portable and convenient to raise our productivity and efficiency. However, users are also facing the security threats when using it. Above all, the National Information and Communication Security Taskforce, Executive Yuan, (NICST; "this Taskforce") decided in its 26th meeting of June 24, 2014, to study mobile phone control mechanisms of other countries as well as the division of labor between agencies in Taiwan. The Ministry of Economic Affairs regulates basic security criteria for applications in mobile phones and computers. However, mobile phones come under the purview of Article 42 of the Telecommunications Act, which article regulates terminal devices for telecommunication. The National Communications Commission (NCC) regulates Ex-works embedded software. Therefore, the Mobile Telephone System-Embedded Software Security Testing Project is implemented under the Technical Criteria for Smart Telephone System Embedded Software Security Testing ("the Criteria").

2. Purpose

Serving as standard norms for the industry, this criteria strengthen the security protection of smart phones when they are shipped from the factory and before consumers use them to raise Taiwan's requirements regarding the information security of smartphones and improve consumers' trust and willingness to use smart phones.

However, the nature of information security being risk control, the various security levels after Mobile Telephone System-Embedded Software

Security Testing cannot completely protect tested telephones from malicious access or hacker attacks. Continuous action to raise awareness of information security and the importance of good user's habits will reduce the risk and impact from information security issues.

3. Scope

These criteria apply to smart phone systems and their embedded software to ensure compliance with information security requirements at the current stage. But it does not include the extra services and content which are purchased and downloaded from embedded software.

To meet different security requirements, these criteria provide three levels (basic, medium and high) for embedded software in smartphones. The basic level meets the lowest requirements of basic privacy protection in smartphones. The medium level meets all testing requirements of the basic level and adds testing items for intermediate protection. The high level ensures that the kernel layer of the smartphone cannot be tampered with and information cannot be maliciously captured. This level meets the testing requirements of the basic and medium levels as well as testing items included in the security documents of the mobile phone design. As Table 1, security levels, testing items, and detail testing item correlations are shown in Attachment 6.

Table 1　Security Level Descriptions

Security levels (ID code)	Requirements	Descriptions
Basic (B)	Basic Privacy Protection	Smartphone offers user's privacy-related personal data security, including protection of the mobile phone's security features and personal data. E.g. the user must be clearly notified before personal data is collected.
Medium (M)	Advanced Data Protection	Smartphone provides a complete data protection mechanism during use, storage, and transmission of data, to ensure that all the data can be safely used under any of these conditions.
High security level (H)	Confidentially Data Protect	Smart phones have to ensure that the kernel layer is not tampered with or information is maliciously accessed.

4. Definitions of terms

4.1 Encryption

Mathematical algorithms process electronic data such that they are no longer presented in their original form, in order to achieve confidentiality. The encrypted data can be decrypted to restore their

original form.

4.2 Local Port

The socket port number which is open by system's embedded software for services requirement.

4.3 Session Identification，Session ID

The unique identification number for an activity session when establishes a connection. When the connection terminates, the identification code is released to allow the assigned the code to a new connection established by a user.

4.4 Near Field Communication，NFC

A short-range wireless communication technology which operates at a frequency of 13.56 MHz with a sensing distance of less than 10 cm and the capability of data transfer speeds is up to 424 Kbps. NFC reading methods can be Peer-to-Peer, Read/Write and Card Emulation modes. The Card Emulation Mode could emulate may types of physical cards such as credit card and Easy Card without power supplied.

4.5 Non-Operating System Protection Area

The storage space which is accessed from the external devices like personal computer without root's permission of smartphone. It also includes the smartphone's and external SD card's spaces.

4.6 Injection

The method to get the unauthenticated data or control whole the application and system by using the defect or unexpected external program or iteration of applications. The typical methods are SQL

Injection and OS Command Injection.

4.7 XML Injection）(hidden attacks on Extensible Markup Language)

A kind of Internet attack for attacker to hack the system to change the important files or content by changing the structure or data in XML format when the application executes the input feature by using XML format. The XML format are often used as input and output form for application. whereby the files in XML format are often used as input to and output from an application.

4.8 Personal Data

Personal data includes the name, date of birth, national identification number, passport number, features, fingerprints, marital status, family, education, occupation, medical history, medical, genetic, sex life, health checks, criminal record, contact information, financial situation, social activities and other information that may directly or indirectly to identify a natural person.

4.9 Sensitive Data

Leaking or tampering of content may result in damage to the rights or interests of an individual or owner of data.

4.10 Data Type

Based on the two factors of information sensitivity and input by user. In this criteria, the data types is divided into: Type 1, Type 2, Type 3, and Type 4. The data type classification is described in Table 2.

Table 2 Data type classification

Type	Judgment		Example
	Whether they are sensitive data	Whether they are inputted by the user	
Type 1	Yes	Yes	1. The personal data which is defined in the criteria. 2. Information or content of smartphone including text message, contact record, password of devices, pictures, username and password
Type 2	Yes	No	IMEI, IMSI[Note] and GPS information.
Type 3	No	No	APP list, music playing information, mobile phone operating system, mobile phone serial number, mobile phone firmware version, MCC, MNC, service operator, network transmission method and configuration profile
]Type 4	N/A	N/A	Data encryption, protocol encryption, or w/o encryption and w/ unknown content.
[Note] The IMEI code and the IMSI code are the fixed connections as needed with the mobile service provider or the mobile phone			

Type	Judgment		Example
	Whether they are sensitive data	Whether they are inputted by the user	
manufacturer. Then the IMEI and IMSI codes carry information identifying natural persons. However, as user and registered person may be different, these data are classified as Data type 2.			

4.11 Robustness Testing

A test methodology to validate the robustness of the program by manufacturing errors or unexpected input. This testing assesses the capacity of operating systems, mobile applications or network services when encountering anomalous input or calculations to handle these errors or to continue to operate normally.

4.12 International Mobile Subscriber Identity，IMSI

Refers to a unique identification code consisting of the GSM and UMTS mobile network device user. IMSI consists of a string of 10 to 15 digits. The three digits on the SIM card in a mobile phone represent the mobile country code (MCC). The next digits are the Mobile Network Code (MNC), which consists of three digits in the North American Standard or two digits in the European standard. The remaining digits are the Mobile Subscription Identification Number (MSIN) which is independently determined by each operator. Thus, IMSI consists of a single string of digits formed by the MCC, MNC, and MSIN codes.

4.13 International Mobile Equipment Identity，IMEI

Refers to every independent mobile communication device identified on a network which is the equivalent of a device's identity card. It's a 15-digit serial number, the first six digits of which represent the Type Approval Code (TAC) which represents the type of phone. The next two digits are the Final Assembly Code (FAC) indicating the country of origin. The final six digits are the Serial Number (SNR) which represents the production sequence number. The final digit (SP) is a test code which is usually set to 0. The IMEI code is usually attached to the back of the device but is also stored in the telephone memory.

4.14 Password

Refers to a data string set to protect specific applications and it is typically used for identification and data encryption.

4.15 User Agrees

User agrees means the system provide mechanism for user to choose agree or disagree by notification.

If user choose agree, it means user agree it by actively operation and system notification.

4.16 Wireless Transmission Technology

Wireless Transmission Technology is the methodology for smartphone transmits data from network or peer-to-peer through wireless standards. The wireless transmission technology includes Bluetooth, WLAN NFC, mobile communication network, GPS, IR and wireless charging.

4.17 Wireless Local Network，WLAN

Refers to a network connection established through radio waves or infrared laser light as a media for the transmission of data. Its

functionalities are identical to a wired LAN.

4.18 Internal Mobile Applications

Refers to the mandatory embedded software that mobile telephone manufacturers, mobile communications service providers or application software developers must install the first time that a user uses the smartphone or initialize the network service.

4.19 Internet Protocol Address，IP Address

Refers to a 32-bit number that uniquely identifies a TCP/IP host address on the Internet, commonly referred to as “IP Address”. It typically uses “.” to separate four segments in a ten-digit string.

4.20 Domain Name

Corresponds to an Internet address. Internet users can remember a combination of letters or numbers designating the location of a TCP/IP server (“IP address”).

4.21 Digital Signature

Means the action where the electronic document is translated to certain length of digital data by mathematic computation or other method which will be encrypted with the private key of the signatory to form the Electronic Signature, and it can also be verified with public key in the meantime.

4.22 Buffer Overflow

A type of attack, whereby a malicious attacker exploits a vulnerability in a program to input a string of data or information, which exceeds a predetermined length, causing the program to encounter an unexpected

situation, resulting in buffer overflow. A malicious attacker inserts programming code or information in an original program for a malicious purpose, such as causing the program to shut down in an anomalous manner, execute arbitrary code, or obtain system permissions.

4.23 Certificate

Means the electronic certificate bearing the signature verified data in order to confirm the identity and the qualification of the signatory.

4.24 Certification Authority，CA

A certificate-issuing authority or juristic person trusted by users whose business is issuing, managing, annulling and deleting certificate keys in the public X.509 format.

4.25 Address Space Layout Randomization，ASLR

Means the action utilized to scramble the memory positions of key components during the running process where it would be hard for the attacker to locate key addresses easily such as the executed base, library, memory stack and heap; thus, preventing attacker from run malicious program correctly.

4.26 Common Criteria，CC

The international standard for the evaluation and testing of information security products ISO / IEC 15408 defines Evaluation Assurance Levels (EAL) and determines levels of product security. There are seven EAL levels, with EAL representing the lowest level and EAL 7 the highest level. The standard provides applicants/sponsors, testing laboratories, and verification organizations (institutions) with criteria for the

assessment and testing of the security and functionality of information security products. The related information could be found from the URL: http://www.commoncriteriaportal.org.

4.27 Target of Evaluation，TOE

Means the product and relevant manual required to apply for the evaluation and verification of information communication security.

4.28 Protection Profile，PP

Means the basic security document compiled to satisfy the TOE.

4.29 Security Target，ST

Means the specification-related document produced to proof that the information communication security product can comply with the PP or specific security requirements.

4.30 Security Functional Requirement，SFR

The security-related needs defined in Part 2 of the Common Criteria describe the requirements which the Target Security Features (TSF) of a security product must satisfy. This requirement will be quoted in PP and ST to specifically explain the functional security requirement for such product.

4.31 TOE Security Functions，TSF

Means the function established for the information communication security product to realize the Security Functional Requirement (SFR) that should be achieved for the ST.

4.32 TOE Security Functions Interface，TSFI

Means the external communication interface of TOE for realizing the

SFR.

4.33 Security Domain

Means the resource group that will be accessed by certain proactive individual (user or machine) through authorization, and it is one of the attributes in the security structure.

4.34 Self-Protection

Means the security function that cannot be destroyed by irrelevant program code or facility, and it is one of the attributes in the security structure.

4.35 Non-Bypassibility

Means the technology preventing the tested object from evading the security function inspection. (e.g. The user will not be allowed to access the audit functional interface before passing the identity verification).

5. Test/Inspection Requirement

The testing requirements of this criteria include document review and lab test. The document review involves review of such documents as the test application form, the verdor's self-declaration form and a security features specification table. This review serves to facilitate the implementation of the testing items by the test laboratory. The lab test is the actual test carried out to evaluate the testing items by a testing laboratory.

After the applicant requests a test, the testing laboratory must carry out a documentary review and physical test within the scope of these Norms.

5.1 Embedded Software Properties

The testing scope of smartphone embedded software systems include three types of software: factory preloaded software, vendor uploaded software and iconless software. The iconless software could be optioal test itmes.

(1) Factory preloaded software: smartphones leaving the factory come with installed applications with factory settings, which the user can start using immediately through the icons.

(2) Vendor uploaded software: applications preinstalled on smart phones or which automatically self-install the first time the phone accesses the Internet, which users can start using immediately through the icons.

(3) Iconless software: as opposed to the two previous software types,

the user cannot activate these through icons, but this type of software transfers data back to the backend server.

5.2 Test Layers

In keeping with the internationally accepted concept of testing levels for smartphone security, these criteria is divided the smartphone structure into the following five layers: data layer, application layer, communication protocol layer, operating system layer and hardware layer. As each layer faces different information security risks, the testing items for each layer are differentiated accordingly.

- Information/Data Level: It deals with the security for the information/data transmission, storage and utilization.
- Apps: It deals with the security for the embedded software of the smartphone.
- Communication Protocol: It deals with the security for the wired interface, wireless interface and communication protocol.
- Operating System Level: It deals with the security for the operating system related service and user identification.
- Hardware Level: It deals with the security for key and computation module.

5.3 Data Type

Based on the two factors of information sensitivity and input by user. This criteria divides data types into: Type 1, Type 2, Type 3, and Type 4. The data type classification is described in Table 2.

5.4 Document Review

Applicant should provide Test Application Form (Refer to Attachment 1) and Verdor’s Self-Declaration Conformity (Refer to Attachment 2).

If it applies to High security level, the Security Features Specification Table (Refer to Attachment 3), Design Security Table (Refer to Attachment 4) and Security Architecture Table (Refer to Attachment 5) are required too.

5.4.1 Test Application

The applicant shall submit relevant information including applier, manufactor's information and specifications of smartphone (including vender, model, name, operating system's version, GPS feature, wireless transmittion technology, biology idenfitification and external memory)

5.4.2 Vendor's Self-Declaration Table

The test applicant must submit a description of the embedded software including name of the software, the publisher, version, package name, property, feature description, permission, type of data access and network port (local service).

5.4.3 Security Functions Specification Table

The document must provide descriptions of the Target Security Features Interfaces (TSFI) including the name, purpose, the functional requirements to achieve security, mode of operation, parameters, executive actions, and error messages of the TSFI. Base on the document, the test laboratory reviews whether the security functionality interfaces meet the security requirements.

5.4.4 Design Security Table

The document must provide the description of how the subsystem constiture the security feature interface for the security feature specifications, as well as the names, purpose, security feature interface and behavior description.

5.4.5 Security Architecture Table

The table must provide how the security architecture of the device submitted for testing satisfies the Security Functional Requirements (SFR); propose a security architecture design concept and recommendations for security behavior for the security feature interfaces and their subsystems; describe the security ranges of the security feature divisions, the initial sequence of the security features, and the self-protection mechanisms of the security features of the device submitted for testing, as well as how to avoid loops when the security features are bypassed.

6. Test Items

This criteria regulate the testing items shown in Table 3 based on the test items per level and the detail items derived from the security requirements of these items. The test items and detail items are described in Tale 4. Their numbering principle is as below.

- Test item number：Layer code.test item code
- Detail test item number：Layer code.Test item code.Detail test item code.Security level code (+)
- Description

(1)Layer code：

Layer	**Code**
Data Layer	D
Application Layer	A
Protocol Layer	P
Operation system Layer	O
Hardware Layer	H

(2)Security Level code：

Security Level	**Code**
Basic	B
Medium	M
High	H

(3) If a test item could be selected by applicant as the optional item is marked (+).

- Example：

(1) The test item number of the first test item on the data layer is D and the first detail item is basic level and mandatory. Then the detail item number is D.1.1.B

(2) The test item number of the second item on the data layer is D.2 and its second detail test item is medium with optional. Then the detail item number is D.2.2.M(+)

Table 3 Test Item Description

Layer	Test Item	Security Requirements
Data Layer	D.1 Data Usage Authorization	Before accessing or sharing sensitive data, the embedded software must require for user’s permission.
	D.2 Data Storage Protection	The embedded software must store sensitive data in a protected area of the operating system and offer an encryption functionality, in order to plaintext data from being improperly obtained and decrypted.
	D.3 Data Loss Protection	The operating system must provide a data protection and backup function, in order to prevent data leakage and data loss.
Application Layer	A.1 Program Identity Identification	The embedded software should authenticate the user ID and its permission when accessing the account of the device bound for the first time in order to prevent misuse or abuse of the user account.
	A.2 Trusted Source of Program	The embedded software must confirm all mechanisms and data sources for purchase feature.
	A.3 Program Execution Authorization	The embedded software must obtain the user's agrees for all executions, which are the same as it’s agreement.
	A.4 Program Execution Security	The embedded software must have the capacity to deal with the input of malicious strings.

Layer	Test Item	Security Requirements
Protocol Layer	P.1 Protocol Usage Authorization	When the phone is connected with an external device, the system should be given a corresponding prompt for user choice to enable or disable the wireless transmission technology.
	P.2 Protection Protocol	The encrypted transmission of data between the embedded software and a server must use a security encryption algorithm, in order to avoid attacks during transmission.
	P.3 Protocol Execution Security	The operating system should have the capability of handling errors of protocol contents.
Operating System Layer	O.1 System Operating Authorization	Actions executed by the operating system must obtain the user's consent, and notify a security alert if needed.
	O.2 System Identity Identification	The operating system should provide a secure identity identification mechanism.
	O.3 System Execution Security	The operating system should have program memory protection mechanism, and provide a secure reporting channel.
Hardware Layer	H.1 Key Management Protection	The key management must comply with the standards for key use and management.
	H.2 Algorithm Strength	The phone’s algorithms for encryption / decryption and

Layer	Test Item	Security Requirements
	Requirements	signatures must comply with the key algorithm standards and the requirements for the initialization vector.

Table 4 Descriptions of Test Items and Detail Items

Test Item	Test Number	Detail Item
D.1 Data Usage Authorization	D.1.1.B	Embedded software should ask for user's permission before accessing sensitive data.
	D.1.2.M(+)	Embedded software can't access sensitive data if user configures to deny this permission.
D.2 Data Storage Protection	D.2.1.B	Embedded software should store username and password in a protected area in the operating system or with encrypted algorithm.
	D.2.2.M(+)	Embedded software have to store sensitive data with encrypted algorithm to prevent it will not be obtained by abnormal method and decrypted.
	D.2.3.M(+)	Embedded software should not store the username and password which is used to communicate with remote servers by plain text in the source codes to prevent it will not be obtained by abnormal method.
D.3 Data Loss Protection	D.3.1.B	Operating system should provide user to lock the mobile phone and related configuration to

Test Item	Test Number	Detail Item
		ensure user can lock it remotely when it lost.
	D.3.2.B	Operating system should provide user to delete the data in the mobile phone and related configuration to ensure user can erase the data remotely when it lost.
	D.3.3.B	Operating system should provide backup features to protect user's data.
A.1 Program Identity Identification	A.1.1.B	Embedded software should identify user's identification and permission to bind the devices when the first initialization to prevent user's account to be misused or abused.
A.2 Trusted Source of Program	A.2.1.B	Embedded software should use the certificate within validity period when when it has purchase service to prevent to use the expired certificate.
	A.2.2.B	Embedded software should be able to validate the publisher and version information for user to know its source.
A.3 Program Execution Authorization	A.3.1.B	Embedded software should notify user to confirm before using purchase service.
	A.3.2.B	Embedded software should only use the necessary permissions. The permissions have to conform to the function and permission description in Vendor's Self-Declaration

Test Item	Test Number	Detail Item
		Conformity.
	A.3.3.M	The network socket ports which are turned on by embedded software have to conform to the network service ports (local service) in Vendor’s Self-Declaration Conformity.
	A.3.4.M(+)	Embedded software should not execute the smartphone system function without user’s permission.
	A.3.5.M(+)	Embedded software should terminate all of the related processes which are created by it if user configure it to be disabled.
A.4 Program Execution Security	A.4.1.B	Embedded software should provide the feature to report security issue.
	A.4.2.M	Embedded software should provide the feature to prevent injection attack.
	A.4.3.M	Embedded software should provide the feature to prevent XML injection.
P.1 Protocol Usage Authorization	P.1.1.B	Smartphone should provide the feature to let user enable or disable wireless transmission interface.
	P.1.2.B	When the wireless interface is enabled, system should have the related notification.
	P.1.3.B	Smartphone system should request user’s confirmation to establish the connection to the other devices at the first establishment.

Test Item	Test Number	Detail Item
P.2 Protection Protocol	P.2.1.B	Embedded software should encrypt the sensitive data when using wireless transmission to protect the data is secured.
	P.2.2.M	Embedded software should prevent session identification re-transmission attack.
	P.2.3.M	The connection should be encrypted by secured algorithm between embedded software and purchase service server.
P.3 Protocol Execution Security	P.3.1.M	Embedded software should provide the error tolerance of protocols.
O.1 System Operation Authorization	O.1.1.B	The declared update source of operating system should be the same as the data link server’s IP/DN/Hostname in Vendor’s Self-Declaration Conformity.
	O.1.2.B	Operating system have to notify user the security risk of system when download or install the current update.
O.2 System Identity Identification	O.2.1.B	Operating system should provide screen unlock protection policy to prevent personal information will be accessed without authorization.
	O.2.2.B	Operating system should support the lock protection when unlock error to protect personal information without authentication.

Test Item	Test Number	Detail Item
	O.2.3.B	Operating system should provide at least 72 type of password inputs including upper-case and lower-case letters, one or more numerical digits and special characters. The length of password should support more than 14 characters.
	O.2.4.M	Operating system should not store the password by plain text to prevent to be used without authentication.
O.3 System Execution Security	O.3.1.B	Embedded software should provide the mechanism to report security issue.
	O.3.2.M	Operating system should provide the memory protection mechanism to prevent memory addresses which are owned by the program and related libraries to be used abnormally.
	O.3.3.H	Operating system should establish a trusted channel to the destination to protect the transmitted data.
	O.3.4.H	Operating system should provide password test and software availability test when booting.
	O.3.5.H	Operating system should count the error authentication to the device. It should erase the data which are under protected when the

Test Item	Test Number	Detail Item
		counter is over configured threshold.
H.1 Key Management Protection	H.1.1.H	The key management of the smartphone, including the generation, exchange, merge and erasing of encryption algorithm and privacy key should meet the key usage and management standard of NIST, ANSI and IEEE.
	H.1.2.H	The keys which are stored in the smartphone should be protected to keep the confidentiality and integrity.
	H.1.3.H	The key can’t be stored in the non-volatile memory and can’t be exported or transmitted out of the device.
H.2 Algorithm Strength Requirements	H.2.1.H	The encrypted/decrypted and signature algorithm should match the key algorithm standard which are published by NIST, ANSI and IEEE.
	H.2.2.H	The related algorithms which are depended by the requirement of each mode to generate initialization factor and match the requirement of initialization factor which is published by NIST.
	H.2.3.H	The random number which is used for generating keys should match the

Test Item	Test Number	Detail Item
		requirements of random bit generation which are published by NIST and ANSI.

6.1 Mandatory Items

In the description of the test methodologies and criteria, the operating system will be called System Under Test (SUT), the embedded software will be called Software Under Test (SFUT). The test labs should test the smartphone by the detail items below to ensure all of the tests follow this criteria.

6.1.1 Data Layer

Information security should ensure that user data is protected from unauthorized gathering, sharing, usage, deletion, tampering and storage by bundled system software.

D.1 Data Usage Authorization	
D.1.1 .B Embedded software should ask for user's permission before accessing sensitive data.	
Test Conditions: ■ SFUT has the feature to access sensitive data. ■ Data Type: Type 1 or Type 2 ■ Property of SFUT: Factory Preload or Vendor Uploaded	
Test Methodology	Criteria
(1) Open the SUT. (2) Check if the privacy policy or the	In Step (2), privacy policy or usage declaration should provide the information and user's agreement

declaration of use of the SFUT has complied with the corresponding instructions. (3) If Step (2) is failed. Execute the SFUT and access user's sensitive data. (4) Check if the SFUT provide the corresponding user's agreement mechanism.	mechanism for SFUT to access the sensitive data. Or in Step (4) SFUT provide the corresponding user's agreement mechanism. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

D.2 Data Storage Protection	
D.2.1 .B Embedded software should store username and password in a protected area in the operating system or with encrypted algorithm.	
Test Conditions: ■ SFUT has the feature to login by username and password. ■ Data Type: Username and Password ■ Property of SFUT: Factory Preload or Vendor Uploaded	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the test condition. (3) Execute the SFUT and enter the username and password. Choose to agree to save the username and password and login successfully. (4) Use data access tools to access the data in the areas stored by SFUT	In Step (5), SFUT does not store username and password by plain text in the area which is not protected by operating system. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

which is not protected by operating system. (5) Check if SFUT store the username and password by plain text in the area which is not protected by operating system.	

D.3 Data Loss Protection	
D.3.1 .B Operating system should provide user to lock the mobile phone and related configuration to ensure user can lock it remotely when it lost.	
Test Conditions: ■ Data Type: None ■ Property of SFUT: None	
Test Methodology	Criteria
(1) Open the SUT. (2) Configure and execute the remote lockout feature of SUT. (3) Check if the SUT is locked remotely.	In Step (3), SUT is lockout remotely. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
D.3.2 .B Operating system should provide user to delete the data in the mobile phone and related configuration to ensure user can erase the data remotely when it lost.	
Test Conditions: ■ Data Types: None ■ Property of SFUT: None	

Test Methodologies	Criteria
(1) Open the SUT. (2) Enter the testing data and store it. (3) Execute the remote delete feature and erase the data stored in Step (2). (4) Check if the data stored in Step (2) is erased.	In Step (4), the testing data is erased remotely. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
D.3.3 .B Operating system should provide backup features to protect user's data.	
Test Conditions: ■ Data Type: None ■ Property of SFUT: None	
Test Methodology	Criteria
(1) Open the SUT. (2)Check if the SUT provide backup feature.	In Step (2), the SUT provide the backup feature. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

6.1.2 Application Layer

The security of applications shall ensure the embedded software within the system to avoid any unauthorized access to system resource.

A.1 Program Identity Identification
A.1.1 .B Embedded software should identify user's identification and

permission to bind the devices when the first initialization to prevent user's account to be misused or abused.	
Test Condition: ■ The SFUT has the feature to connect to user's account(s). ■ Data Type: None ■ Property of SFUT: Factory Preload or Vendor Uploaded	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the test condition. (3) Execute the account authentication feature of SFUT. (4) Check if SFUT provide the mechanism for user login authentication and obtain the permission.	In Step (4), SFUT notify the mechanism for user authentication and obtain the permission If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

A.2 Trusted Source of Program	
A.2.1 .B Embedded software should use the certificate within validity period when when it has purchase service to prevent to use the expired certificate.	
Test Condition: ■ Type of Server: Server provides purchase service. ■ Date Type: None ■ Property of SFUT: Factory Preload or Vendor Uploaded	
Test Methodology	Criteria
(1) Open the SUT. (2) Check it match the test condition.	In Step (4), the certificate which is provided by server should not be expired.

(3) SFUT transmits the data to remote server through Internet. (4) Check if server side provide the expired certificate to SFUT.	If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
A.2.2 .B Embedded software should be able to validate the publisher and version information for user to know its source.	
Test Condition: ■ Date Type: None ■ Property of SFUT: Factory Preload or Vendor Uploaded	
Test Methodology	Criteria
(1) Open the SUT. (2) Check it matches the test condition. (3) Check if SFUT or Vendor's Self-Declaration table provide publisher and version information of SFUT.	In Step (3), SFUT or Vender's Self-Declaration Table provide publisher and version information of SFUT. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

A.3 Program Execution Authorization
A.3.1 .B Embedded software should notify user to confirm before using purchase service.
Test Condition: ■ SFUT provides the purchase service. ■ Data Type: None. ■ Property of SFUT: Factory Preload or Vendor Uploaded

Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the test condition. (3) Execute the SFUT and enabled the purchase feature. (4) Check if the SUT or SFUT asks for user's agreement to execute purchase feature.	In Step (4), the SUT or SFUT will execute the purchase feature after user agrees it. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
A.3.2 .B Embedded software should only use the necessary permissions. The permissions have to conform to the function and permission description in Vendor's Self-Declaration Conformity.	
Test Condition: ■ Applicant should fill in Function description and Permission description fields in Vendor's Self-Declaration Conformity. ■ Data Type: None. ■ Property of SFUT: Factory Preload or Vendor Upload.	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the test condition. (3) Execute and operate SFUT and list the feature and permission of the SFUT. (4) Compare to the list in Step (3) and check if it matches to the correspond content in Vendor's Self-Declaration Conformity.	In Step (4), the result showed in Step (3) corresponds with the Vendor's Self-Declaration of Conformity. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

A.3.3 .M The network socket ports which are turned on by embedded software have to conform to the network service ports (local service) in Vendor's Self-Declaration Conformity.	
Test Condition: ■ SFUT open the socket ports to listen for connection. ■ The applicant should fill in Network Service Port (Local Service) field in Vendor's Self-Declaration Conformity. ■ Data Type: None. ■ Property of SFUT: Factory Preload or Vendor Upload.	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the test condition. (3) Execute the SFUT and check open network port number through network test tool. (4) Check the network port number(s) which obtained from Step (3) are matched to the description of Network Service Port(Local Service) in Vendor's Self-Declaration Conformity.	In Step (4), the obtained network port number(s) match description of the Network Service Port(Local Service) in Vendor's Self-Declaration Conformity. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

A.4 Program Execution Security
A.4.1 .B Embedded software should provide the feature to report security issue.
Test Condition: ■ Data Type: None. ■ Property of SFUT: Vendor Upload

Test Methods	Criteria
(1) Open the SUT. (2) Confirm it has complied with the Test Condition. (3) Check if the SFUT, official website or users' manual provide the feature to report issue.	In Step (3), check if the issue found in SFUT could be reported. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
A.4.2 .M Embedded software should provide the feature to prevent injection attack.	
Test Condition: ■ SFUT provides the feature for user to enter data. ■ Date Type: None. ■ Property of SFUT: Factory Preload or Vendor Upload	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the Test Condition. (3) Execute the SFUT and enter data by using the injection attack string. (4) Check if SFUT executes the injection attack string.	In Step (4), SFUT does not execute the injection attack string. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
A.4.3 .M Embedded software should provide the feature to prevent XML injection.	
Test Condition: ■ SFUT accepts data with XML format. ■ Data Type: None.	

■ Property of SFUT: Factory Preload and Vendor Upload.	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the Test Condition. (3) Execute the network transmission feature of SFUT. (4) Use the test tool to capture the packets between SFUT/SUT and remote server. (5) Insert the injection attack string with XML format to the packets which are captured from Step (4) to SFUT. (6) Check if SFUT execute the injection attack string.	In Step (6), SFUT does not execute the injection attack string. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

6.1.3 Protocol Layer

The security of communication protocols shall ensure user's hands on data transmission and the controllability of its surrounding facilities.

P.1 Protocol Usage Authorization
P.1.1 .B Smartphone should provide the feature to let user enable or disable wireless transmission interface.
Test Condition: ■ The Wireless Transmission Technology under test: Bluetooth, WLAN, NFC (Peer-to-Peer mode and Read/Write mode), mobile communication network and GPS. ■ Date Type: None.

<table>
<tr><td colspan="2">■ Property of SFUT: None.</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.
(2) Confirm it has complied with the Test Condition.
(3) Check if the smartphone provides the interface to enable and disable the wireless transmission technologies. Check if the presented status matches to the real status.</td><td>In Step (3), smartphone provide the interface to enable and disable the wireless transmission technologies and the presented status is same as the real status.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
<tr><td colspan="2">P.1.2 .B When the wireless interface is enabled, system should have the related notification.</td></tr>
<tr><td colspan="2">Test Condition:
■ The Wireless Transmission Technology under test: Bluetooth, WLAN, NFC (Peer-to-Peer mode and Read/Write mode), mobile communication network and GPS.
■ Data Type: None.
■ Property of SFUT.</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.
(2) Confirm it has complied with the Test Condition.
(3) Enable the wireless transmission technology for test in smartphone.
(4) Check if the smartphone presents the correspond status</td><td>In Step (4), smartphone provide user’s the correspond status.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
</table>

P.1.3 .B Smartphone system should request user's confirmation to establish the connection to the other devices at the first establishment.	
Test Condition: ■ The Wireless Transmission Technology under test: Bluetooth and WLAN. ■ Date Type: None. ■ Property of SFUT.	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the Test Condition. (3) Enable the wireless transmission technology for test in smartphone. (4) Enable the correspond wireless transmission technology in another devices and establish the connection between them. (5) Choose to deny this connection from SFUT/SUT. (6) Check if SFUT/SUT can establish the connection with the device descripted in Step (4).	In Step (6), the SFUT/SUT can not establish the connection with the device descripted in Step (4). If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

P.2 Protocol Protection
P.2.1 .B Embedded software should encrypt the sensitive data when using wireless transmission to protect the data is secured.
Test Condition:

<table>
<tr><td colspan="2">■ The Wireless Transmission Technology under test: Bluetooth, WLAN and mobile communication network.
■ Date Type: Type 1(does not include picture) and GPS information.
■ Property of SFUT: Factory Preload and Vendor Upload.</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.
(2) Confirm it has complied with the Test Condition.
(3) Execute the SFUT and transmits the sensitive data through the wireless transmission technology under test.
(4) Check if the SFUT transmits the sensitive data by plain text.</td><td>In Step (4), the SFUT does not transmit the sensitive data by plain text.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
<tr><td colspan="2">P.2.2 .M Embedded software should prevent session identification re-transmission attack.</td></tr>
<tr><td colspan="2">Test Condition:
■ SFUT uses session identification when transmitting data via Internet.
■ Data Type: None.
■ Property of SFUT: Factory Preload and Vendor Upload</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.
(2) Confirm it has complied with the Test Condition.
(3) Execute the network transmission feature of SFUT.
(4) Capture the transmitted packets between SFUT and remote server</td><td>In Step (5), the re-transmission attack should not work to the SFUT/SUT.

If the test matches the criteria, then the results is Pass.
If the test does not match the</td></tr>
</table>

and capture the session identification. (5) Execute the re-transmission attack to SFUT/SUT by the session identification captured from Step (4).	criteria, then the results is Fail.
P.2.3 .M The connection should be encrypted by secured algorithm between embedded software and purchase service server.	
Test Condition: ■ Server Type: Server provides purchase service. ■ Applicant should provide the document for validation. ■ If necessary, test laboratory can request the applicant to demonstrate the feature. ■ Data Type: None. ■ Property of SFUT: Factory Preload and Vendor Upload	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the Test Condition. (3) Execute the network transmission feature of SFUT. (4) Use communication encryption algorithm test tool to check if SFUT use the encryption algorithm which is FIPS 140 approved or the applicant can provide the evidence to prove it has the same security level to FIPS 140 to encrypt the the	In Setp(4), the encryption algorithm which is used to encrypt the communication data between SFUT and server is FIPS 140 approved or the applicant have to provide the evidence to prove it has the same security level to FIPS 140. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

communication data when access the server.	

P.3 Protocol Execution Security	
P.3.1 .M Embedded software should provide the error tolerance of protocols.	
Test Condition: ■ The Wireless Transmission Technology under test: Bluetooth and WLAN. ■ Date Type: None. ■ Property of SFUT: None.	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the Test Condition. (3) For smartphone's wireless transmission interface under test, send more than 10000 different test packets during negotiation phase. (4) Check if the wireless transmission interface or SFUT/SUT are still operating as normal.	In Step (4), SFUT/SUT can execute communication connection and data transmission normally. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

6.1.4 Operating System

The security of operating system should ensure operating system can protect and remind system resource and let user be privy to

upgrade the system.

<table>
<tr><td colspan="2">O.1 System Operation Authorization</td></tr>
<tr><td colspan="2">O.1.1 .B The declared update source of operating system should be the same as the data link server’s IP/DN/Hostname in Vendor’s Self-Declaration Conformity.</td></tr>
<tr><td colspan="2">Test Condition:
■ SUT provides the operating system upgrade feature.
■ Applicant should fill in the data link server’s IP/DN/Hostname field in Vendor’s Self-Declaration Conformity.
■ Data Type: None.
■ Property of SFUT: None.</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.
(2) Confirm it has complied with the Test Condition.
(3) Upgrade the operating system through the operating system upgrade feature in SUT.
(4) Capture the destination IP address of the connection to download the upgradation file
(5) Check if the destination IP address matches the content in the Vendor’s Self-Declaration Conformity.</td><td>In Step (5), the destination IP address should the same as the information in Vendor’s Self-Declaration Conformity.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
<tr><td colspan="2">O.1.2 .B Operating system have to notify user the security risk of system when download or install the current update.</td></tr>
<tr><td colspan="2">Test Condition:</td></tr>
</table>

<table>
<tr><td colspan="2">■ SUT provides the operating system upgrade feature.
■ Data Type: None.
■ Property of SFUT: None.</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.
(2) Confirm it has complied with the Test Condition.
(3) Check the SUF or official website provide the system upgrade notification. It also have to provide the detail upgrade content and security risk information without upgrade.</td><td>In Step (3), SUT or official website should provide the system upgrade and security risk information.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
</table>

<table>
<tr><td colspan="2">O.2 System Identity Identification</td></tr>
<tr><td colspan="2">O.2.1 .B Operating system should provide screen unlock protection policy to prevent personal information will be accessed without authorization.</td></tr>
<tr><td colspan="2">Test Condition:
■ Data Type: None.
■ Property of SFUT: None</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.
(2) Enable the screen lockout configuration in the SUT and configure the password.
(3) Lockout the SUT (including shutdown the screen and SUT).</td><td>In Step (5), user can wake up the system by the configuration in Step (2).

If the test matches the criteria, then the results is Pass.</td></tr>
</table>

(4) Wake up the SUT (including wake up the screen and SUT). (5) Check if the configuration of Step (3) works.	If the test does not match the criteria, then the results is Fail.
O.2.2 .B Operating system should support the lock protection when unlock error to protect personal information without authentication.	
Test Condition: ■ Data Type: None. ■ Property of SFUT: None	
Test Methodology	Criteria
(1) Open the SUT. (2) Enable the screen lockout configuration in the SUT and configure the password. (3) Lockout the SUT. (4) Wake up the SUT with error password for times. (5) Check if the SUT prompts the message of the SUT is locked forcibly.	In Step (5), SUT prompts the message of the SUT is locked forcibly. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
O.2.3 .B Operating system should provide at least 72 type of password inputs including upper-case and lower-case letters, one or more numerical digits and special characters. The length of password should support more than 14 characters.	
Test Condition: ■ Data Type: None. ■ Property of SFUT: None	

Test Methodology	Criteria
(1) Open the SUT. (2) Open the interface to configure the password of SUT. (3) Check if SUT provides the interface to set the password with at least 72 possible values including upper-case/lower-case letters, numerical digits and special characters. (4) Check if the password can be configured to more than 14 possible characters.	In Step (3), SUT provides the interface to set the password with at least 72 possible values including upper-case/lower-case letters, numerical digits and special characters. In Step (4), the password can be configured to more than 14 possible characters. If the test match the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
O.2.4 .M Operating system should not store the password by plain text to prevent to be used without authentication.	
Test Condition: ■ Applicant have to provide the root permission of the smartphone. ■ Screen lockout Function: Graphic, Password and Biometric character. ■ Data Type: None. ■ Property of SFUT: None	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the Test Condition. (3) Enable the screen lockout configuration in the SUT and	In Step (4-1) or Step (4-2), the password does not be stored in the smartphone by plain text. If the test matches the criteria, then

configure the password. (4-1) Check if the password is stored in the smartphone by plain text with root permission. (4-2) If the SUT does not provide root permission to check it. Applicant have to provide the detail information and evidence of this test step including the feature description, interface and screenshot. If necessary , test laboratory can ask the applicant to demonstrate this feature.	the results is Pass. If the test does not match the criteria, then the results is Fail.

O.3 System Execution Security	
O.3.1 .B Embedded software should provide the mechanism to report security issue.	
Test Condition: ■ Data Type: None. ■ Property of SFUT: None	
Test Methodology	Criteria
(1) Open the SUT. (2) Check if the SUT, official website or users' manual provide the issue report mechanism.	In Step (2), the issue which is found in SUT could be report through the report mechanism. If the test match the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
O.3.2 .M Operating system should provide the memory protection	

<table>
<tr><td colspan="2">mechanism to prevent memory addresses which are owned by the program and related libraries to be used abnormally.</td></tr>
<tr><td colspan="2">Test Condition:
■ Applicant have to provide the document for review.
■ If necessary, the applicant have to demonstrate the feature.
■ Data Type: None.
■ Property of SFUT: None</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Confirm it has complied with the document review.
(2) If there is no wealthy evidence to prove the SUT provides this feature. The applicant have to demonstrate it.</td><td>In Step (1) or Step (2), the SUT provides the memory protection mechanism.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
<tr><td colspan="2">O.3.3 .H Operating system should establish a secure channel to the destination to protect the transmitted data.</td></tr>
<tr><td colspan="2">Test Condition:
■ Applicant have to provide the document for review.
■ If necessary, the applicant have to demonstrate the feature.
■ Data Type: None.
■ Property of SFUT: None</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Confirm it has complied with the document review.
(2) If there is no wealthy evidence to prove the SUT provides this</td><td>In Step (1) or Step (2), the SUT establish the secure channel to transmit data.</td></tr>
</table>

feature. The applicant have to demonstrate it.	If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
O.3.4 .H Operating system should provide password test and software availability test when booting.	
Test Condition: ■ Applicant have to provide the document for review. ■ If necessary, the applicant have to demonstrate the feature. ■ Data Type: None. ■ Property of SFUT: None	
Test Methodology	Criteria
(1) Confirm it has complied with the document review. (2) If there is no wealthy evidence to prove the SUT provides this feature. The applicant have to demonstrate it.	In Step (1) or Step (2), the SUT provides the self-security test feature when booting. If the test match the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
O.3.5 .H Operating system should count the error authentication to the device. It should erase the data which are under protected when the counter is over configured threshold.	
Test Condition: ■ Applicant have to provide the document for review. ■ If necessary, the applicant have to demonstrate the feature. ■ Data Type: None.	

■ Property of SFUT: None	
Test Methodology	Criteria
(1) Confirm it has complied with the document review. (2) If there is no wealthy evidence to prove the SUT provides this feature. The applicant have to demonstrate it.	In Step (1) or Step (2), the failure authentication process should erase the protected data securely by data coverage. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

6.1.5 Hardware Layer

Hardware security should ensure key management and store protection. The the algorithm strength requirement should meet the international standards and ensure the user is informed to upgrade the key.

H.1 Key Management Protection
H.1.1.H The key management of the smartphone, including the generation, exchange, merge and erasing of encryption algorithm and privacy key should meet the key usage and management standard of NIST, ANSI and IEEE. The related standards are listed as below. ANSI X9.31-1998, IEEE 802.11-2012, IEEE 802.11ac-2013, IEEE 802.1X NIST SP 800-38A, 38C~F, 56A~B, 57, 90B
Test Condition: ■ Applicant have to provide the document for review. ■ If necessary, the applicant have to demonstrate the feature.

<table>
<tr><td colspan="2">■ Data Type: None.
■ Property of SFUT: None</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Confirm it has complied with the document review.
(2) If there is no wealthy evidence to prove the SUT provides this feature. The applicant have to demonstrate it.</td><td>In Step (1) or Step (2), the key management of the device under test have to meet the requirement of Confidentiality and Integrity.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
<tr><td colspan="2">H.1.2.H The keys which are stored in the smartphone should be protected to keep the confidentiality and integrity.</td></tr>
<tr><td colspan="2">Test Condition:
■ Applicant have to provide the document for review.
■ If necessary, the applicant have to demonstrate the feature.
■ Data Type: None.
■ Property of SFUT: None</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Confirm it has complied with the document review.
(2) If there is no wealthy evidence to prove the SUT provides this feature. The applicant have to demonstrate it.</td><td>In Step (1) or Step (2), the key storage mechanism of the device under test have to meet the requirement of Confidentiality and Integrity.

If the test matches the criteria, then the results is Pass.</td></tr>
</table>

	If the test does not match the criteria, then the results is Fail.
H.1.3.H The key can’t be stored in the non-volatile memory by plain text and can’t be exported or transmitted out of the device.	
Test Condition: ■ Applicant have to provide the document for review. ■ If necessary, the applicant have to demonstrate the feature. ■ Data Type: None. ■ Property of SFUT: None	
Test Methodology	Criteria
(1) Confirm it has complied with the document review. (2) If there is no wealthy evidence to prove the SUT provides this feature. The applicant have to demonstrate it.	In Step (1) or Step (2), the key transmission protection should meet the requirement of non-exportable or transport. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

H.2 Algorithm Strength Requirements
H.2.1.H The encrypted/decrypted and signature algorithm should match the key algorithm standard which are published by NIST, ANSI and IEEE. The related standards are as below. ANSI X9.31-1998 IEEE 802.11-2012, IEEE 802.11ac-2013 ,IEEE 802.1X NIST SP 800-38A, 38C~F, 56A~B, 57, 90B

<table>
<tr><td colspan="2">Test Condition:
■ Applicant have to provide the document for review.
■ If necessary, the applicant have to demonstrate the feature.
■ Data Type: None.
■ Property of SFUT: None</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Confirm it has complied with the document review.
(2) If there is no wealthy evidence to prove the SUT provides this feature. The applicant have to demonstrate it.</td><td>In Step (1) or Step (2), the algorithm which is used in the device under test meet the technical requirement.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
<tr><td colspan="2">H.2.2.H The related algorithms which are depended by the requirement of each mode to generate initialization factor and match the requirement of initialization factor which is published by NIST. The related standards are list as below.
NIST SP 800-38A, 38C~F, 56A~B, 57, 90B</td></tr>
<tr><td colspan="2">Test Condition:
■ Applicant have to provide the document for review.
■ If necessary, the applicant have to demonstrate the feature.
■ Data Type: None.
■ Property of SFUT: None</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Confirm it has complied with the document review.
(2) If there is no wealthy evidence to</td><td>In Step (1) or (2), the initialization factor of the device under test meet the technical requirement.</td></tr>
</table>

prove the SUT provides this feature. The applicant have to demonstrate it.	If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
H.2.3.H The random number which is used for generating keys should match the requirements of random bit generation which are published by NIST and ANSI. The related standards are listed as below. NIST SP 800-90A ANSI X9.31-1998	
Test Condition: ■ Applicant have to provide the document for review. ■ If necessary, the applicant have to demonstrate the feature. ■ Data Type: None. ■ Property of SFUT: None	
Test Methodology	Criteria
(1) Confirm it has complied with the document review. (2) If there is no wealthy evidence to prove the SUT provides this feature. The applicant have to demonstrate it.	In Step (1) or Step (2), the random number usage of the device under test meet the technical requirement. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

6.2 Optional Items

This section will describe the test items which are optional. The applicant can choose to test these items or not.

6.2.1 Optional Items of Data Layer

<table>
<tr><td colspan="2">D.1 Data Usage Authorization</td></tr>
<tr><td colspan="2">D.1.2.M(+) Embedded software can’t access sensitive data if user configures to deny this permission.</td></tr>
<tr><td colspan="2">Test Condition:
■ Applicant have to provide the document for review.
■ If necessary, the applicant have to demonstrate the feature.
■ SFUT has the feature to access sensitive data.
■ Date Type: Type 1 and Type 2.
■ Property of SFUT: Factory Preload and Vendor Upload</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.
(2) Check if the privacy policy or usage declaration provide the related description and user’s agreement mechanism in SFUT.
(3) If Step (2) is pass, then choose to deny the privacy policy or usage declaration and then check if the system could be operated.
(4) If Step (2) is failed, then execute the SFUT and deny it to access sensitive data.
(5) Check if SFUT can access the sensitive data.
(6) If there is no wealthy evidence to</td><td>In Step (3), the SUT should not be operated.
Or in Step (5) and Step (6), the SFUT cannot be operated or access the sensitive data.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
</table>

prove the SUT provides this feature. The applicant have to demonstrate it.	

D.2 Data Storage Protection	
D.2.2.M(+) Embedded software have to store sensitive data with encrypted algorithm to prevent it will not be obtained by abnormal method and decrypted.	
Test Condition: ■ Applicant have to provide the root permission of the smartphone. ■ SFUT has the feature to access sensitive data. ■ Date Type: Type 1 (does not include picture) ■ Property of SFUT: Factory Preload and Vendor Upload	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the test condition. (3) Execute the SFUT and save a sensitive data. (4) Use data access tool to access the data by the root's permission and check if the data of Step (3) is stored by plain text	In Step (4), the SFUT does not store the sensitive data by plain text. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
D.2.3.M(+) Embedded software should not store the username and password which is used to communicate with remote servers by plain text in the source codes to prevent it will not be obtained by abnormal method.	

<table>
<tr><td colspan="2">Test Condition:
■ Applicant have to provide the root permission of the smartphone.
■ SFUT has the feature to login by username and password.
■ Date Type: Username and Password
■ Property of SFUT: Factory Preload and Vendor Upload</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.
(2) Confirm it has complied with the test condition.
(3) Use data access tool to access the execution file.
(4) Check if the SFUT stores the username and password by plain text in the execution file of Step (3) for the remote server.</td><td>In Step (4), username and password does not store in the execution file by plain text.

If the test matches the criteria, then the results is Pass.
If the test does not match the criteria, then the results is Fail.</td></tr>
</table>

6.2.2 Optional Items of Application Layer

<table>
<tr><td colspan="2">A.3 Program Execution Authorization</td></tr>
<tr><td colspan="2">A.3.4.M(+) Embedded software should not execute the smartphone system function without user’s permission.</td></tr>
<tr><td colspan="2">Test Condition:
■ Applicant have to provide the root permission of the smartphone.
■ Data Type: None.
■ Property of SFUT: Factory Preload and Vendor Upload</td></tr>
<tr><td>Test Methodology</td><td>Criteria</td></tr>
<tr><td>(1) Open the SUT.</td><td>If Step (4), there is no related record</td></tr>
</table>

(2) Confirm it has complied with the test condition. (3) Execute the SFUT and operate the related feature. (4) Compare to the contact record, file stamp of text message record and check if the SFUT dial the call or send text message on background.	to dial call or send text message on the background. If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.
A.3.5.M(+) Embedded software should terminate all of the related processes which are created by it if user configure it to be disabled.	
Test Condition: ■ SFUT is not a terminate-and-stay-resident program. ■ Data Type: None. ■ Property of SFUT: Factory Preload and Vendor Upload	
Test Methodology	Criteria
(1) Open the SUT. (2) Confirm it has complied with the test condition. (3) Check active application list. (4) Execute and operate the SFUT. (5) Terminate the application in Step (4) and review the active application list again. (6) Check if the list is the same as	In Step (6), the list of Step (5) is same as the list of Step (3). If the test matches the criteria, then the results is Pass. If the test does not match the criteria, then the results is Fail.

Step (3).	

6.2.3 Optional Test Items for Icon-less Software

The embedded software includes factory preload, vendor upload and icon-less software. The applicant can request to test the icon-less software by the test cases listed in Table 5 if applicant want to know the security issue of it. The detail information could be found in section 6.2.1.

Table 5 The test item and detail item for icon-less software

Test Item	Detail Item Number	Detail Item
A.2 Trusted Source of Program	A.2.1.B(+)	Embedded software should use the certificate within validity period when when it has purchase service to prevent to use the expired certificate.
A.3 Program Execution Authorization	A.3.3.M(+)	The network socket ports which are turned on by embedded software have to conform to the network service ports (local service) in Vendor's Self-Declaration Conformity.
P.2 Protocol Protection	P.2.1.B(+)	Embedded software should encrypt the sensitive data when using wireless transmission to protect the data is secured.
	P.2.3.M(+)	The connection should be encrypted by secured algorithm between embedded software and purchase

		service server.

7. Attachment

Attachment 1　Application of Security Test of the Embedded Software for Smartphone System

Date of Application： Year Month Day

<table>
<tr><td colspan="2">Applicant (Company Name)</td><td>☐Manufacturer
☐ Agents</td><td colspan="2">○○○ Co., Ltd</td><td rowspan="4">Company Stamp</td></tr>
<tr><td colspan="2">VAT Number</td><td colspan="3"></td></tr>
<tr><td colspan="2">Company Address</td><td colspan="3">☐☐☐-☐☐</td></tr>
<tr><td colspan="2">Representative</td><td colspan="3"></td></tr>
<tr><td rowspan="2">Contact</td><td>Name and Job Title</td><td></td><td>E-mail</td><td></td></tr>
<tr><td>Phone Number</td><td></td><td>FAX</td><td></td></tr>
<tr><td colspan="2">Company Name and Address</td><td colspan="4">○○○ Co. Ltd
☐☐☐-☐☐</td></tr>
<tr><td colspan="3">Brand Name/Model/Name of the Smartphone</td><td colspan="3">ex. APPLE / a16xx / iPhone 6s</td></tr>
<tr><td colspan="3">System Version for Test</td><td colspan="3">○○○-○○○-○○○</td></tr>
<tr><td colspan="2">Security Level</td><td colspan="4">☐Basic ☐Medium ☐Medium(Include the optional items) ☐High ☐High(Include the optional items)</td></tr>
<tr><td rowspan="4">Basic Information of the Smartphone</td><td>GPS</td><td colspan="4">☐ USA GPS ☐ Europe Galileo
☐ RUSSA GLONASS ☐ Others _____
☐China(☐Bi-Directional Transmission)</td></tr>
<tr><td>Wireless Transmission Technology</td><td colspan="4">☐ Bluetooth
☐ Mobile Communication Network (☐ 2G ☐ 3G ☐ 4G)
☐ WLAN ☐ Others _____
☐ NFC (☐ Peer-to-Peer Mode ☐ Read/Write Mode)</td></tr>
<tr><td>Biometric</td><td colspan="4">☐ No ☐ Yes, fingerprint、…</td></tr>
<tr><td>External Storage</td><td colspan="4">☐ No ☐ Yes, microSD card、…</td></tr>
<tr><td rowspan="3">Sample Quantity</td><td>Basic</td><td colspan="4">☐Two samples for tests</td></tr>
<tr><td>Medium</td><td colspan="4">☐Two samples for test with root permission for the test cases.</td></tr>
<tr><td>High</td><td colspan="4">☐Two samples for test with root permission for the test cases.</td></tr>
<tr><td colspan="2">Documentations (Original or Copy)</td><td colspan="4">☐1. One copy of the Chinese/English user’s guide or manual
☐ 2. One copy of the Chinese/English specification.
☐ 3. One copy of Vendor’s Self-Declaration Conformity
☐ 4. Security Function Specification Table, Design Security Table and Security</td></tr>
</table>

<table>
<tr><td></td><td colspan="4">Architecture Table (For High Security Level usage).
☐ 5. One CD (includes this application and item from 1 to 4)</td></tr>
<tr><td colspan="5">[Note 1] Apply the embedded software security testing documentation of smartphone system, and save one copy of CD in the testing laboratory; on top of that, the remaining documentation and equipment shall be returned to the applied unit after submitting testing report.</td></tr>
<tr><td rowspan="4">Test Laboratory
(Filled out by the laboratory)</td><td colspan="3">Laboratory Name:
Laboratory Type: ☐Type 1 ☐Type 2</td><td rowspan="4"></td></tr>
<tr><td colspan="3">☐ 1. Submit one copy of test report
Report Number：_____ ,
Security Level：☐Basic ☐Medium ☐High
☐ 2. Save one copy of application and CD.</td></tr>
<tr><td>Submit Date</td><td></td><td>Completion Date</td><td></td></tr>
<tr><td>Contact</td><td></td><td>Phone</td><td></td></tr>
<tr><td colspan="5">[Note 2] The original application will be saved in test laboratory, the applicant should submit the test by the copied application.</td></tr>
</table>

Attachment 2　Vendor's Self-Declaration Conformity-1(Template)

BASIC INFORMATION OF SOFTWARE UNDER TEST					DATA LAYER		PROTOCOL
ITEMS	SOFTWARE UNDER TEST	PUBLISHER AND VERSION	PACKAGE UNDER TEST	PROPERTY	SENSITIVE DATA	WIRELESS TRANSMISSION TECHNOLOGY	LOGIN FEATURE BY USERNAME AND PASSWORD

1	Phone	company 1.2.2	com. android. phone	☐Factory Preload ☐Vendor Upload ☐Icon-less software	☐No ☐Type 1 ☐Type 2	☐No ☐Wi-Fi ☐GPS ☐Bluetooth ☐Mobile Communication Network ☐NFC(Peer-to-Peer Mode) ☐NFC(Read/Write Mode) ☐IR ☐Others____	☐No ☐Yes

Attachment 2　Vendor's Self-Declaration Conformity-2(Template)

BASIC INFORMATION OF SOFTWARE UNDER TEST			**APPLICATION LAYER**			
ITEM	**SOFTWARE UNDER**	**PUBLISHER AND**	**FUNCTION DESCRIPTIO**	**PERMISSION DESCRIPTION**	**DATA LINK SERVER'S**	**NETWORK**

	TEST	VERSION	N		IP/DN/HOSTNAME AND SERVER TYPE	SERVICE PORTS (LOCAL SERVICE)
1	Phone	company 1.2.2	☐Terminate-and-Stay-Resident (TSR) ☐Non-TSR Description: Dial number from the contacts in the phone.	READ_CONTACTS：For feature of sharing information.	apPchat. example.net：server 111.112. 113.114：purchase server	☐No ☐Yes Port Number：____
				ACCOUNT_MANAGER：For adding account to the social network		
				CAMERA：For picture record		
				INTERNET：For connecting to server to get the newest announcement		

[Note] There are server and purchase server in server type field.

Attachment 3 Security Function Specification Table

TOE Security Function Interface (TSFI)	Purpose	Security Function Requirement (SFR)	Method of Use	Parameter	Actions	Error Message
List all the security function interfaces.	Explain the purpose of security function on each security function interface.	Explain how each security function interface achieves the security function requirements listed in the attached test items O.7~O.11 and H.1~H.5.	Explain how to use each security function interface.	Explain how to use all the parameters and its meaning on each security function interface.	Explain how to operate and execute details on each security function interface.	Explain the error message appeared on each security function interface including its meaning and derivative conditions.
Ex:	*Ex:*	*Ex:*	*Ex:*	*Ex:*	*Ex:*	*Ex:*

TOE Security Function Interface (TSFI)	Purpose	Security Function Requirement (SFR)	Method of Use	Parameter	Actions	Error Message
TSFI_CLI	*Provide the operation interface in command line mode.*	*SFR_Security Management: Provide security management function.*	*Use ssh to connect the device under tested to provide the operation interface in the command line mode.*	*ID & password*	*Operate the device under test by command iteration*	*Connection fail Authentication fail*

Attachment 4 Design Security Table

Subsystem	Purpose	TSFI	Behavior Description
List all security function interface of each subsystem.	Describe the purpose of the security function of each subsystem.	Describe each subsystem that belongs to the security function interface in Attachment 3.	Describe the behavior of each subsystem: (1) How to implement the functions of the security function interface. (2) Information about the interaction with other subsystems, including the communication between different subsystems and the characteristics of the delivered data.
Ex: *Subsystem_ssh*	*Ex:* *Provide ssh service*	*Ex:* *TSFI_CLI*	*Ex:* *(1) Provide command line mode for TSFI_CLI* *(2) The interaction with the other subsystem* *(A) Subsystem_auth: Send the authentication information to Subsystem_auth and confirm whether authentication was successfully by replying a message*

Subsystem	Purpose	TSFI	Behavior Description
			(B) Subsystem_terminal: ...

Attachment 5　Security Architecture Table

Item	Description	
1.Security Domain	**Security Domain Name**	**Security Domain Description**
	List the security domain to which each security function interface corresponds. *Ex:* *TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection*	How to separate the data to be protected in the security function operation environment and subject to internal execution limitations. *Ex:* *When the management function is executed via TSFI_GUI, TSFI is allowed to have only one remote connection at a time, and may execute only one audit data processing request.*

Item	Description	
2.Secure Initialization	**Related Components**	**Security Initialization Description**
	Operate the components/environments related to the device under test. *Ex:* *Networking procedure for the device under test*	Provide the initial steps and installation procedures for secure activation of the components related to the object to be tested. *Ex:* *1. Connect a RJ-45 cable to the switch or trusted secure area of the router from the terminal marked as 0/0 (ethernet0 / 0 port).* *2. Give a 0/1(ethernet0/1 port) at the port and connect a RJ-45 cable to the DMZ security area in the switchboard or router.*

Item	Description		
3.Self-Protection	**Self-protection Function**	**Relation with External Equipment**	**自我保護機制說明**

Item	Description		
	List the self-protection mechanism to which each security function interface corresponds. *Ex:* *TSFI_WEB:* *Self-protection 1: Identity identification* *Self-protection 2: Remote connection encryption*	Describe the data exchange between the security function and its interface and the external equipment. *Ex:* *When the device under test is connected remotely via a browser for execution of the management function, the identity is verified using the TSFI_WEB GUI interface.*	Describe that the security function interface provides the physical or logical self-protection mechanism. *範例：* *1. The passcode must be input to enter the interface.* *2. Data transmission mechanism: TLS/SSL* *3. Special execution method: Fingerprint recognition.* *4. Special equipment requirement: Fingerprint reader.*

Item	Description	
4. Non-Bypassibility	**Non-Bypassibility Function**	**Non-bypassibility Mechanism Description**
	List the non-bypassibility mechanism to which each security function corresponds. *Ex:* *TSF_Authentication identity identification function*	1. Enumerate possible bypassing approaches. 2. Describe possible precautions, including protection for access to the security function interface, protection for the data processed during the runtime, existence of other external accesses, and protective mechanisms against illegal accesses. *Ex:* *The device under test may be operated via the maintenance interface without identity verification.* *Precaution: Use a physical blocking approach to prevent taking bypasses to avoid identity verification.*

Attachment 6 Security Capability Level of Detail Items

Note: (+) indicates an optional item

NUMBER	TEST ITEM	DETAIL ITEM	SECURITY LEVEL		
			B	M	H
D.1	Data Usage Authorization	D.1.1.B Embedded software should ask for user's permission before accessing sensitive data.	✓	✓	✓
		D.1.2.M(+) Embedded software can't access sensitive data if user configures to deny this permission.		✓	✓
D.2	Data Storage Protection	D.2.1.B Embedded software should store username and password in a protected area in the operating system or with encrypted algorithm.	✓	✓	✓
		D.2.2.M(+) Embedded software have to store sensitive data with encrypted algorithm to prevent it will not be obtained by abnormal method and decrypted.		✓	✓
		D.2.3.M(+) Embedded software should not store the username and password which is used to communicate with remote servers by plain text in the source codes to prevent it will not be obtained by abnormal method.		✓	✓

NUMBER	TEST ITEM	DETAIL ITEM	SECURITY LEVEL		
			B	M	H
D.3	Data Loss Protection	D.3.1.B Operating system should provide user to lock the mobile phone and related configuration to ensure user can lock it remotely when it lost.	✓	✓	✓
		D.3.2.B Operating system should provide user to delete the data in the mobile phone and related configuration to ensure user can erase the data remotely when it lost.	✓	✓	✓
		D.3.3.B Operating system should provide backup features to protect user's data.	✓	✓	✓
A.1	Program Identity Identification	A.1.1.B Embedded software should identify user's identification and permission to bind the devices when the first initialization to prevent user's account to be misused or abused.	✓	✓	✓
A.2	Trust Source of Program	A.2.1.B Embedded software should use the certificate within validity period when when it has purchase service to prevent to use the expired certificate.	✓	✓	✓
		A.2.2.B Embedded software should be able to validate the publisher and version information for user to know its source.	✓	✓	✓

NUMBER	TEST ITEM	DETAIL ITEM	SECURITY LEVEL		
			B	M	H
A.3	Program Execution Authorization	A.3.1.B Embedded software should notify user to confirm before using purchase service.	✓	✓	✓
		A.3.2.B Embedded software should only use the necessary permissions. The permissions have to conform to the function and permission description in Vendor's Self-Declaration Conformity.	✓	✓	✓
A.3	程式執行授權	A.3.3.M The network socket ports which are turned on by embedded software have to conform to the network service ports (local service) in Vendor's Self-Declaration Conformity.		✓	✓
		A.3.4.M(+) Embedded software should not execute the smartphone system function without user's permission.		✓	✓
		A.3.5.M(+) Embedded software should terminate all of the related processes which are created by it if user configure it to be disabled.		✓	✓
A.4	Program Execution Security	A.4.1.B Embedded software should provide the feature to report security issue.	✓	✓	✓

NUMBER	TEST ITEM	DETAIL ITEM	SECURITY LEVEL		
			B	M	H
		A.4.2.M Embedded software should provide the feature to prevent injection attack.		✓	✓
		A.4.3.M Embedded software should provide the feature to prevent XML injection.		✓	✓
P.1	Protocol Usage Authorization	P.1.1.B Smartphone should provide the feature to let user enable or disable wireless transmission interface.	✓	✓	✓
		P.1.2.B When the wireless interface is enabled, system should have the related notification.	✓	✓	✓
		P.1.3.B Smartphone system should request user's confirmation to establish the connection to the other devices at the first establishment.	✓	✓	✓
P.2	Protocol Transmission Protection	P.2.1.B Embedded software should encrypt the sensitive data when using wireless transmission to protect the data is secured. (P.2.1.B(+) could be applied for icon-less software)	✓	✓	✓

NUMBER	TEST ITEM	DETAIL ITEM	SECURITY LEVEL		
			B	M	H
		P.2.2M Embedded software should prevent session identification re-transmission attack.		✓	✓
		P.2.3.M The connection should be encrypted by secured algorithm between embedded software and purchase service server. (P.2.3.M(+) could be applied for icon-less software)		✓	✓
P.3	Protocol Execution Security	P.3.1.M Embedded software should provide the error tolerance of protocols.		✓	✓
O.1	System Operation Authorization	O.1.1.B The declared update source of operating system should be the same as the data link server's IP/DN/Hostname in Vendor's Self-Declaration Conformity.	✓	✓	✓
		O.1.2.B Operating system have to notify user the security risk of system when download or install the current update.	✓	✓	✓
O.2	System Identity Identification	O.2.1.B Operating system should provide screen unlock protection policy to prevent personal information will be accessed without authorization.	✓	✓	✓

NUMBER	TEST ITEM	DETAIL ITEM	SECURITY LEVEL		
			B	M	H
		O.2.2.B Operating system should support the lock protection when unlock error to protect personal information without authentication.	✓	✓	✓
		O.2.3.B Operating system should provide at least 72 type of password inputs including upper-case and lower-case letters, one or more numerical digits and special characters. The length of password should support more than 14 characters.	✓	✓	✓
		O.2.4.M Operating system should not store the password by plain text to prevent to be used without authentication.		✓	✓
O.3	System Execution Security	O.3.1.B Embedded software should provide the mechanism to report security issue.	✓	✓	✓
		O.3.2.M Operating system should provide the memory protection mechanism to prevent memory addresses which are owned by the program and related libraries to be used abnormally.		✓	✓
		O.3.3.H Operating system should establish a trusted channel to the			✓

NUMBER	TEST ITEM	DETAIL ITEM	SECURITY LEVEL		
			B	M	H
		destination to protect the transmitted data.			
		O.3.4.H Operating system should provide password test and software availability test when booting.			✓
		O.3.5.H Operating system should count the error authentication to the device. It should erase the data which are under protected when the counter is over configured threshold.			✓
H.1	Key Management	H.1.1.H The key management of the smartphone, including the generation, exchange, merge and erasing of encryption algorithm and privacy key should meet the key usage and management standard of NIST, ANSI and IEEE.			✓
		H.1.2.H The keys which are stored in the smartphone should be protected to keep the confidentiality and integrity.			✓
		H.1.3.H The key can’t be stored in the non-volatile memory and can’t be exported or transmitted out of the device.			✓
H.2	Algorithm	H.2.1.H The encrypted/decrypted and signature algorithm should match the			✓

NUMBER	TEST ITEM	DETAIL ITEM	SECURITY LEVEL		
			B	M	H
	Strength Requirement	key algorithm standard which are published by NIST, ANSI and IEEE.			
		H.2.2.H The related algorithms which are depended by the requirement of each mode to generate initialization factor and match the requirement of initialization factor which is published by NIST.			✓
		H.2.3.H The random number which is used for generating keys should match the requirements of random bit generation which are published by NIST and ANSI.			✓

附件 4 資通設備資通安全檢測實驗室管理作業要點修正草案

資通設備資通安全檢測實驗室管理作業要點修正草案

中華民國 100 年 12 月 23 日通傳技字第 10043035000 號函下達

壹. 資通設備資通安全檢測實驗室管理作業要點

一、 國家通訊傳播委員會（以下簡稱本會）為確保資通設備資通安全品質，執行資通設備資通安全檢測實驗室（以下簡稱檢測實驗室）認可與管理作業，特訂定本要點。

二、 本會認可檢測實驗室，應依其檢測能力認可其檢測範圍(如附件一)，檢測範圍包括類別與項目，由檢測實驗室申請之。

三、 本會受理檢測實驗室認可申請，應審查下列各款事項：

（一）檢測實驗室申請書（如附件一）。

（二）依法設立之本國法人、機構之證明文件影本。

（三）取得本國實驗室認證組織依下列規定核發之認證證明影本：

1. 一般規定

符合中華民國國家標準（以下簡稱 CNS）17025 或國際標準化組織所定標準（以下簡稱 ISO/IEC）17025，有關測試與校正實驗室能力一般要求之規定。

2. 專業規定

(1) 書面審查能力

具備 ISO/IEC 15408 資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation, CC）及 ISO/IEC 18045 資訊技術安全評估共同方法論(Common Methodology for Information Technology Security Evaluation, CEM)之測試評估能力。

(2) 實機測試能力

具備連結網際網路(Internet)真實情境之測試平台，該平台應符合下列之測試環境：

A.具備至少 100 人同時上線使用，且能記錄使用者透過該平台進行之網路活動。

B.具備至少 10,000 條之最大同時連線數量，至少 3,000 條之平均同時連線數量。

C.具備至少 100Mbps 之最大流量速度，至少 30Mbps 之平均流量速度。

D.於該平台上使用之應用類型至少包括下列 10 種，每一應用類型至少須含一個應用項目，全部可供使用之應用項目須達 50 個以上。

a. Chat：msn, yahoo messenger, icq, qq
b. Email：gmail, hotmail, smtp protocol, pop3 protocol, imap protocol
c. File Transfer：ftp protocol, flashget, smb protocol
d. Game：garena, ms-directplay, facebook app
e. P2P：bittorrent protocol, edonkey, xunlei, fs2you, ed2k, ares, emule
f. Remote Access：windows remote desktop, telnet protocol, ssh protocol, vnc, Hamachi
g. Streaming：rtsp protocol, qqtv, pplive, qvod, flashcom, itunes, funshion
h. VoIP：skpye, skypeout, sip protocol
i. Web：http, http download, http video, http range get, https, http proxy
j. Others：sslvpn, nntp protocol, dns protocol, snmp protocol, dhcp protocol, mysql, ntp protocol

E.於該平台上使用之 IP 協定應包括 IPv4 及 IPv6。

F.待測設備安裝於平台上，可連續進行場測(Field Trial)至少達 336 小時。

G.可錄製平台流量之容量至少達 20,000G 位元組，並可用重播工具將該流量導入待測設備。

(3) 符合一般規定之檢測實驗室若僅具專業規定所列能力之一者，得藉由其他實驗室延伸另一專業規定所列能力，但須經本國實驗室認證組織合併認證之。

（四）檢測實驗室技術主管、品質主管及資通安全檢測報告簽署人之資格條件之證明文件影本：

1. 書面審查

(1) 技術主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、電信工程、電子工程、電機工程或其他相關科系畢業，並接受 CCRA 認可實驗室之 ISO/IEC 15408 測試評估相關專業訓練，訓練時數至少 360 小時，從事相關設備測試評估實務工作達三年以上。

(2) 品質主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校畢業，並接受品質管理相關專業訓練，且從事相關設備品質管理實務工作達三年以上。

(3) 報告簽署人：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、電信工程、電子工程、電機工程或其他相關科系畢業，並接受 CCRA 認可實驗室之 ISO/IEC 15408 測試評估相關專業訓練，訓練時數至少 360 小時，從事相關設備測試評估實務工作達二年以上。

2. 實機測試

(1) 技術主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、電信工程、電子工程、電機工程或其他相關科系畢業，從事相關設備測試評估實務工作達三年以上。

(2) 品質主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校畢業，並接受品質管理相關專業訓練，且從事相關設備品質管理實務工作

達三年以上。

(3) 報告簽署人：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、電信工程、電子工程、電機工程或其他相關科系畢業，從事相關設備測試評估實務工作達二年以上。

（五）檢測實驗室成員至少 4 人，應分別為

1. 具備技術主管資格者 1 人
2. 具備品質主管資格者 1 人
3. 具備安全檢測報告簽署人資格者 2 人

（六）資通安全檢測報告簽署人於同一案件不得同時擔任技術主管或品質主管。

四、 前項各款文件有不全或記載不完備者，本會應通知限期補正，屆期未補正或補正不完備者，不予受理其申請。補正期間以一個月為限。

五、 檢測實驗室經本會審查符合前點規定者，由本會核發檢測實驗室認可證書（以下簡稱認可證書，格式如附件二），其有效期間為三年。

認可證書應記載事項如下：

（一）法人/機構名稱。

（二）代表人。

（三）檢測實驗室名稱。

（四）檢測實驗室地址。

（五）認可檢測範圍。

（六）有效期間。

六、 檢測實驗室有下列情形之一者，認可證書失其效力：

（一）不符合第三點條件。

（二）資通安全檢測報告有虛偽不實。

（三）受理檢測申請案件，有無正當理由之拒絕或差別待遇。

七、 檢測實驗室或其服務人員對於申請者及檢測相關資料，應嚴守秘密，退職人員亦同。

八、 本會應備查檢測實驗室所報之檢測費用，該費用須以下列方式訂定，並符合透明、公平之原則：

（一）設備檢測費用應依該設備之安全測試等級分為基礎型檢測費用與進階型檢測費用。

（二）通過基礎型檢測合格之設備，自檢測合格日起三個月內，申請同一設備之進階型檢測者，其檢測費用只須補足基礎型與進階型費用之差額。

（三）通過檢測合格之設備，當版本更新時，得針對有變更之檢測項目進行重新檢測，其檢測費用為全項檢測費用乘以重新檢測項目數占全部檢測項目數之比例計算；需重新檢測之項目，由申請者提出並由檢測實驗室認定之。

（四）申請系列產品檢測之設備，其檢測費用為全項檢測費用乘以重新檢測項目數占全部檢測項目數之比例計算；需重新檢測之項目，由申請者提出並由檢測實驗室認定之。

（五）檢測實驗室通知申請者設備檢測未符合規定時，應列舉不符合事項並通知申請者改善，通知改善次數以二次為限，每次改善時間不得超過一個月，無須另外收費。

資通設備資通安全檢測實驗室申請書

申請日期：____年____月____日　　受理編號：_____

法人/機構名稱					
代表人					
檢測實驗室名稱					
檢測實驗室地址					
本國實驗室認證組織之認證證書	證書證號		有效期間		
檢測範圍	1. 應用服務類 □公文管理系統□監控管理系統□金鑰管理系統 □數位簽章系統□智慧卡系統□其它項目_____ 2. 伺服器系統類 □網站伺服系統□資料庫伺服系統□儲存伺服系統 □其它項目_____ 3. 資安防護類 □入侵偵測防禦設備□網路型防火牆設備□防毒閘道設備 □垃圾郵件過濾設備□網頁應用防火牆設備 □應用軟體控管設備□網路封包鑑識分析設備 □網路流量分析設備□網路日誌事件監控設備 □其它項目_____ 4. 終端存取類 □乙太網路交換器□路由交換器□網路電話設備 □網路電話類比閘道器□無線網路攝影機□無線區域網路設備 □其它項目_____ 5. 其它類 □其它項目_____				
聯絡人		地址			
電話		傳真		電子信箱	

檢附文件：

□ 1.法人/機構之身分證明文件影本。

□ 2.本國實驗室認證組織之認證證明文件影本。

□ 3.向本國實驗室認證組織申請檢測實驗室認證時，所檢附相關資料之光碟片。

□ 4.其他經本會指定者。

本檢測實驗室願遵守國家通訊傳播委員會資通設備安全檢測實驗室管理作業要點及相關規定，如有違反致造成損害，願依相關法律負起責任。

謹　此

負責人：_____（簽章）

資通設備資通安全檢測實驗室認可證書

證書號碼：NCC-ICSEL-0X

一、 法人/機 構 名 稱：

二、 代表人：

三、 檢測實驗室名稱：

四、 檢測實驗室地址：

五、 認可檢測範圍：

六、 有效期間：自　　年　　月　　日至　　年　　月　　日止

（以下空白）

中 華 民 國　　年　　月　　日

主任委員

貳. 智慧型手持式行動臺資通安全檢測實驗室管理作業要點

中華民國 OOO 年 OO 月 OO 日通傳技字第 OOOOO 號函下達

一、國家通訊傳播委員會（以下簡稱本會）為確保智慧型手機系統內建軟體資通安全品質，執行智慧型手機系統內建軟體資通安全檢測實驗室（以下簡稱檢測實驗室）認可與管理作業，特訂定本要點。

二、本會認可之檢測實驗室分為第 1 型及第 2 型檢測實驗室，由申請擔任檢測實驗室者（以下簡稱申請人）依智慧型手機系統內建軟體資通安全檢測技術規範之檢測範圍（如附件一）申請之。

三、本會受理申請人申請檢測實驗室認可，應審查下列各款事項：

(一)智慧型手機系統內建軟體資通安全檢測實驗室申請書（如附件二）。

(二)依法設立之本國法人、機構之證明文件影本。

(三)取得本國實驗室認證組織核發符合中華民國國家標準（以下簡稱 CNS）17025 或國際標準化組織所定標準（以下簡稱 ISO/IEC）17025 有關測試與校正實驗室能力一般要求規定之認證證明影本。

(四)申請第 1 型檢測實驗室認可者，其成員及檢測能力應符合下列資格條件，並檢附相關證書之影本及檢測能力佐證資料：

1.檢測實驗室成員：

(1)技術主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且具資訊安全相關管理職經驗 2 年以上或從事資安測試評估實務工作達 2 年以上，並具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。

(2)品質主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且從事品質管理、專案管理或稽核相關工作經驗 2 年以上，並具備品質管理、專案管理或稽核相關訓練合格證書。

(3)報告簽署人：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且具資訊安全相關工作經驗 3 年以上，並符合以下規定：

A.具備道德駭客認證（Certified Ethical Hacker，CEH）或國際網路資安認證（CompTIA Security+）有效之資訊安全相關專業證照。

B.具備下列任一有效之資訊安全相關專業證照：

(A) 資訊系統安全專家證照（Certified Information Systems Security Professional，CISSP）

(B) 資安軟體開發專家證照（Certified Secure Software Lifecycle Professional，CSSLP）

(C) 資安分析專家證照（EC-Council Certified Security Analyst，ECSA）

(D) 資安鑑識調查專家證照（EC-Council Computer Hacking Forensic Investigator，CHFI）

(E) 滲透測試專家證照（GIAC Penetration Tester，GPEN）

(F) 行動裝置資安分析專家證照（GIAC Mobile Device Security Analyst，GMOB）

(G) 安全程式設計師證照（EC-Council Certified Secure Programmer，ECSP）

(H) 資安專業人員證照（Systems Security Certified Practitioner，SSCP）

C.非屬本目所列有效之資訊安全相關專業證照者，需經本會認可。

2.檢測能力：

(1)須具備 3 年內智慧型手機系統內建軟體資通安全檢測實際執行經驗，並提供執行之證明文件。

(2)須具備下列檢測工具，並建置可與智慧型手機連線及檢測之操作環境：

A.於藍牙、WLAN 及行動通訊網路之無線傳輸環境下，可攔截、分析及修改網路傳輸封包之工具。

B.可連線及操作智慧型手機作業系統（至少包含 Android 和 iOS 平臺）之指令作業工具。

C.具掃描網路連接埠功能之工具。

D.具檢測加密演算法強度之工具。

E.具模擬藍牙與 WLAN 無線傳輸發射端和接收端功能之模糊測試（Fuzz Testing）工具。

F.軟體開發工具（Software Design Kit）及軟體反組譯工具（至少包含 Android 和 iOS 平臺）。

(五)申請第 2 型檢測實驗室認可者，其成員及檢測能力應符合下列資格條件，並檢附相關證書之影本及檢測能力佐證資料：

1.檢測實驗室成員：

(1)技術主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且具資訊安全相關管理職經驗 2 年以上或從事資安測試評估實務工作達 2 年以上，並具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。

(2)品質主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且從事品質管理、專案管理或稽核相關工作經驗 2 年以上，並具備品質管理、專案管理或稽核相關訓練合格證書。

(3)報告簽署人：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、電信工程、電子工程、電機工程或其他相關科系畢業，並具備接受 CCRA 或本會認可實驗室之 ISO/IEC 15408 測試評估相關專業訓練時數至少 360 小時以上之證明文件影本，且從事資通設備資安檢測評估實務工作達 2 年以上。

2.檢測能力：

須為本會認可之資通安全設備及保護剖繪測試實驗室，或具備密碼演算驗證程序（Cryptographic Algorithm Validation Program，CAVP）之檢測能力，並提供證明文件影本。

(六)檢測實驗室成員至少 3 人，應分別為：

1.具備技術主管資格者 1 人。

2.具備品質主 管資格者 1 人。

3.具備報告簽署人資格者１人。

(七)檢測實驗室技術主管與報告簽署人不得同時擔任品質主管。

四、前點各款文件有不全或記載不完備者，本會應通知限期補正，屆期未補正或補正不完備者，不予受理其申請。補正期間以一個月為限。

五、申請人經本會審查符合第三點規定者，由本會核發智慧型手機系統內建軟體資通安全檢測實驗室認可證書（如附件三，以下簡稱認可證書），其有效期間為三年。認可證書應記載事項如下：

(一)法人/機構名稱。

(二)代表人。

(三)檢測實驗室名稱。

(四)檢測實驗室地址。

(五)認可檢測範圍。

(六)有效期間。

六、檢測實驗室有下列情形之一者，認可證書失其效力：

(一)不符合第三點條件。

(二)檢測報告有虛偽不實。

(三)受理檢測申請案件，有無正當理由之拒絕或差別待遇。

七、檢測實驗室於認可證書有效期間出具之智慧型手機系統內建軟體資通安全檢測報告（以下簡稱檢測報告），可由受測者提交向本會申請核發智慧型手機系統內建軟體資通安全審驗證明。

八、檢測實驗室與其服務人員對於受測者及檢測相關資料，應嚴守秘密，退職人員亦同。

九、檢測實驗室應報請本會備查訂定之檢測費用，該費用須以下列方式訂定，並符合透明、公平之原則：

(一)檢測費用依安全等級區分為初級、中級及高級之檢測費用，各安全等級之檢測範圍如附件一。

(二)經檢測合格之智慧型手機，當作業系統版本或系統內建軟體版本更新時，應針對有變更之部分重新申請檢測。其檢測費用以全項檢測費用乘以重新檢測項目數占全部檢測項目數之比例計算；需重新檢

測之項目，由受測者提供並由檢測實驗室認定之。

(三)檢測實驗室通知受測者檢測未符合規定時，應列舉不符合事項並通知受測者改善，通知改善方式及收費機制由檢測實驗室自訂。

附件一、智慧型手機系統內建軟體資通安全檢測技術規範之檢測範圍

檢測實驗室類型	檢測範圍（檢測細項）	安全等級		
		初	中	高
第一型檢測實驗室	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。	✓	✓	✓
	D.1.2.M(+)手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。		✓	✓
	D.2.1.B 手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。	✓	✓	✓
	D.2.2.M(+)手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。		✓	✓
	D.2.3.M(+)手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。		✓	✓
	D.3.1.B 手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。	✓	✓	✓
	D.3.2.B 手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。	✓	✓	✓
	D.3.3.B 手機系統應提供資料備份功能。	✓	✓	✓
	A.1.1.B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。	✓	✓	✓
	A.2.1.B 手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。	✓	✓	✓
	A.2.2.B 手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。	✓	✓	✓
	A.3.1.B 手機系統內建軟體在未調整付費功能使用設定情況	✓	✓	✓

檢測實驗室類型	檢測範圍 （檢測細項）	安全等級		
		初	中	高
	下，應於每次付費前，提示並取得使用者同意後才可執行。			
	A.3.2.B 手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。	✓	✓	✓
	A.3.3.M 手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路連接埠(本地服務)」相符。		✓	✓
	A.3.4.M(+)手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。		✓	✓
	A.3.5.M(+)手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。		✓	✓
	A.4.1.B 手機系統內建軟體應提供回報安全性問題之管道。	✓	✓	✓
	A.4.2.M 手機系統內建軟體應具備隱碼攻擊字串的處理能力。		✓	✓
	A.4.3.M 手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。		✓	✓
	P.1.1.B 手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。	✓	✓	✓
	P.1.2.B 當手機之無線傳輸技術功能確認開啟時,應給予使用者相對應的提示狀態。	✓	✓	✓
	P.1.3.B 手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。	✓	✓	✓
	P.2.1.B 手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。	✓	✓	✓
	P.2.2M 手機系統內建軟體應避免交談識別碼遭重送攻擊。		✓	✓
	P.2.3.M 手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。		✓	✓
	P.3.1.M 手機系統應具備通訊協定內容的錯誤處理能力。		✓	✓
	O.1.1.B 手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。	✓	✓	✓

檢測實驗室類型	檢測範圍（檢測細項）	安全等級		
		初	中	高
	O.1.2.B 手機系統於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。	✓	✓	✓
	O.2.1.B 手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。	✓	✓	✓
	O.2.2.B 手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。	✓	✓	✓
	O.2.3.B 手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。	✓	✓	✓
	O.2.4.M 手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。		✓	✓
	O.3.1.B 手機系統應提供回報安全性問題之管道。	✓	✓	✓
	O.3.2.M 手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。		✓	✓
第二型檢測實驗室	O.3.3.H 手機系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。			✓
	O.3.4.H 手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。			✓
	O.3.5.H 手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。			✓
	H.1.1.H 手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。			✓
	H.1.2.H 手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。			✓
	H.1.3.H 金鑰不得以明文方式存放於非揮發性之記憶體，且不得用任何方式匯出或直接對外傳輸。			✓
	H.2.1.H 手機實作之加密、解密及簽章演算法，應符合			✓

檢測實驗室類型	檢測範圍 （檢測細項）	安全等級		
		初	中	高
	NIST、ANSI 及 IEEE 發布之金鑰演算法標準。			
	H.2.2.H 手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。			✓
	H.2.3.H 金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。			✓

附件二、智慧型手機系統內建軟體資通安全檢測實驗室申請書

申請日期：____年____月____日

申請人名稱(法人/機構)				統一編號	
代表人	姓名			性別	
	身分證統一編號			出生年月日	
	住居所				
檢測實驗室名稱					
檢測實驗室地址	□□□-□□				
本國實驗室認證組織之認證證書	證書證號		有效期間		
檢測實驗室類別	□ 第1型檢測實驗室 □ 第2型檢測實驗室				
聯絡人			電子信箱		
電話			傳真機		

檢附文件：

□ 1.依法設立之本國法人、機構之證明文件影本。
□ 2.本國實驗室認證組織之認證證明文件影本。
□ 3.向本國實驗室認證組織申請檢測實驗室認證時,所檢附相關資料之光碟片。
□ 4.申請檢測實驗室之成員資格證明文件。
□ 5.申請檢測實驗室之檢測能力證明文件。
□ 6.其他經本會指定者。
□ 7.光碟片1片（內含本申請書及上述1至6項文件電子檔)。

※ 本檢測實驗室願遵守國家通訊傳播委員會智慧型手機系統內建軟體資通安全檢測實驗室管理作業要點及相關規定,如有違反致造成損害,願依相關法律負起責任。

謹　此

申請人（蓋章)：　　代表人（蓋章)：

附件三、智慧型手機系統內建軟體資通安全檢測實驗室認可證書

國家通訊傳播委員會

智慧型手機系統內建軟體資通安全
檢測實驗室認可證書

證書號碼：NCC-ICSEL-0X

一、申請人名稱：

二、代表人：

三、檢測實驗室名稱：

四、檢測實驗室地址：

五、認可檢測實驗室類別：

六、有效期間：自　　年　　月　　日至　　年　　月　　日止

（以下空白）

中 華 民 國　　年　　月　　日

主任委員

智慧型手機系統內建軟體資通安全檢測實驗室管理作業要點
（草案）

中華民國 OOO 年 OO 月 OO 日通傳技字第 OOOOO 號函下達

一、國家通訊傳播委員會（以下簡稱本會）為確保智慧型手機系統內建軟體資通安全品質，執行智慧型手機系統內建軟體資通安全檢測實驗室（以下簡稱檢測實驗室）認可與管理作業，特訂定本要點。

二、本會認可之檢測實驗室分為第 1 型及第 2 型檢測實驗室，由申請擔任檢測實驗室者（以下簡稱申請人）依智慧型手機系統內建軟體資通安全檢測技術規範之檢測範圍（如附件一）申請之。

三、本會受理申請人申請檢測實驗室認可，應審查下列各款事項：

（一） 智慧型手機系統內建軟體資通安全檢測實驗室申請書（如附件二）。

（二） 依法設立之本國法人、機構之證明文件影本。

（三） 取得本國實驗室認證組織核發符合中華民國國家標準（以下簡稱 CNS）17025 或國際標準化組織所定標準（以下簡稱 ISO/IEC）17025 有關測試與校正實驗室能力一般要求規定之認證證明影本。

（四） 申請第 1 型檢測實驗室認可者，其成員及檢測能力應符合下列資格條件，並檢附相關證書之影本及檢測能力佐證資料：

1. 檢測實驗室成員：

（1）技術主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且具資訊安全相關管理職經驗 2 年以上或從事資安測試評估實務工作達 2 年以上，並具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。

（2）品質主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且從事品質管理、專案管理或稽核相關工作經驗 2 年以上，並具備品質管理、專案管理或稽核相關訓練合格證書。

（3）報告簽署人：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且具資訊安全相關工作經驗 3 年以

上，並符合以下規定：

A. 具備道德駭客認證（Certified Ethical Hacker，CEH）或國際網路資安認證(CompTIA Security+)有效之資訊安全相關專業證照。

B. 具備下列任一有效之資訊安全相關專業證照：

（A）資訊系統安全專家證照（Certified Information Systems Security Professional，CISSP）

（B）資安軟體開發專家證照(Certified Secure Software Lifecycle Professional，CSSLP）

（C）資安分析專家證照(EC-Council Certified Security Analyst，ECSA）

（D）資安鑑識調查專家證照（EC-Council Computer Hacking Forensic Investigator，CHFI）

（E）滲透測試專家證照（GIAC Penetration Tester，GPEN）

（F）行動裝置資安分析專家證照（GIAC Mobile Device Security Analyst，GMOB）

（G）安全程式設計師證照（EC-Council Certified Secure Programmer，ECSP）

（H）資安專業人員證照(Systems Security Certified Practitioner，SSCP）

C. 非屬本目所列有效之資訊安全相關專業證照者，需經本會認可。

2. 檢測能力：

（1）須具備 3 年內智慧型手機系統內建軟體資通安全檢測實際執行經驗，並提供執行之證明文件。

（2）須具備下列檢測工具，並建置可與智慧型手機連線及檢測之操作環境：

A. 於藍牙、WLAN 及行動通訊網路之無線傳輸環境下，可攔截、分析及修改網路傳輸封包之工具。

B. 可連線及操作智慧型手機作業系統（至少包含 Android 和 iOS

平臺）之指令作業工具。

C. 具掃描網路連接埠功能之工具。

D. 具檢測加密演算法強度之工具。

E. 具模擬藍牙與 WLAN 無線傳輸發射端和接收端功能之模糊測試（Fuzz Testing）工具。

F. 軟體開發工具（Software Design Kit）及軟體反組譯工具（至少包含 Android 和 iOS 平臺）。

（五） 申請第 2 型檢測實驗室認可者，其成員及檢測能力應符合下列資格條件，並檢附相關證書之影本及檢測能力佐證資料：

1. 檢測實驗室成員：

（1）技術主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且具資訊安全相關管理職經驗 2 年以上或從事資安測試評估實務工作達 2 年以上，並具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。

（2）品質主管：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校學歷，且從事品質管理、專案管理或稽核相關工作經驗 2 年以上，並具備品質管理、專案管理或稽核相關訓練合格證書。

（3）報告簽署人：國內公立或立案之私立大專以上學校或經教育部承認之國外大專以上學校之資訊工程、電信工程、電子工程、電機工程或其他相關科系畢業，並具備接受 CCRA 或本會認可實驗室之 ISO/IEC 15408 測試評估相關專業訓練時數至少 360 小時以上之證明文件影本，且從事資通設備資安檢測評估實務工作達 2 年以上。

2. 檢測能力：

須為本會認可之資通安全設備及保護剖繪測試實驗室，或具備密碼演算驗證程序（Cryptographic Algorithm Validation Program，CAVP）之檢測能力，並提供證明文件影本。

（六） 檢測實驗室成員至少 3 人，應分別為：

1. 具備技術主管資格者 1 人。

2. 具備品質主管資格者 1 人。

3. 具備報告簽署人資格者 1 人。

（七） 檢測實驗室技術主管與報告簽署人不得同時擔任品質主管。

四、前點各款文件有不全或記載不完備者，本會應通知限期補正，屆期未補正或補正不完備者，不予受理其申請。補正期間以一個月為限。

五、申請人經本會審查符合第三點規定者，由本會核發智慧型手機系統內建軟體資通安全檢測實驗室認可證書（如附件三，以下簡稱認可證書），其有效期間為三年。認可證書應記載事項如下：

（一） 法人/機構名稱。

（二） 代表人。

（三） 檢測實驗室名稱。

（四） 檢測實驗室地址。

（五） 認可檢測範圍。

（六） 有效期間。

六、檢測實驗室有下列情形之一者，認可證書失其效力：

（一） 不符合第三點條件。

（二） 檢測報告有虛偽不實。

（三） 受理檢測申請案件，有無正當理由之拒絕或差別待遇。

七、檢測實驗室於認可證書有效期間出具之智慧型手機系統內建軟體資通安全檢測報告（以下簡稱檢測報告），可由受測者提交向本會申請核發智慧型手機系統內建軟體資通安全審驗證明。

八、檢測實驗室與其服務人員對於受測者及檢測相關資料，應嚴守秘密，退職人員亦同。

九、檢測實驗室應報請本會備查訂定之檢測費用，該費用須以下列方式訂定，並符合透明、公平之原則：

（一） 檢測費用依安全等級區分為初級、中級及高級之檢測費用，各安全等級之檢測範圍如附件一。

（二） 經檢測合格之智慧型手機，當作業系統版本或系統內建軟體版本更

新時，應針對有變更之部分重新申請檢測。其檢測費用以全項檢測費用乘以重新檢測項目數占全部檢測項目數之比例計算；需重新檢測之項目，由受測者提供並由檢測實驗室認定之。

（三）檢測實驗室通知受測者檢測未符合規定時，應列舉不符合事項並通知受測者改善，通知改善方式及收費機制由檢測實驗室自訂。

附件一、智慧型手機系統內建軟體資通安全檢測技術規範之檢測範圍

檢測實驗室類型	檢測範圍（檢測細項）	安全等級		
		初	中	高
第一型檢測實驗室	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。	✓	✓	✓
	D.1.2.M(+)手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。		✓	✓
	D.2.1.B 手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。	✓	✓	✓
	D.2.2.M(+)手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。		✓	✓
	D.2.3.M(+)手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。		✓	✓
	D.3.1.B 手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。	✓	✓	✓
	D.3.2.B 手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。	✓	✓	✓
	D.3.3.B 手機系統應提供資料備份功能。	✓	✓	✓
	A.1.1.B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。	✓	✓	✓
	A.2.1.B 手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。	✓	✓	✓
	A.2.2.B 手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。	✓	✓	✓
	A.3.1.B 手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。	✓	✓	✓

檢測實驗室類型	檢測範圍（檢測細項）	安全等級		
		初	中	高
	A.3.2.B 手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。	✓	✓	✓
	A.3.3.M 手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路連接埠(本地服務)」相符。		✓	✓
	A.3.4.M(+)手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。		✓	✓
	A.3.5.M(+)手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。		✓	✓
	A.4.1.B 手機系統內建軟體應提供回報安全性問題之管道。	✓	✓	✓
	A.4.2.M 手機系統內建軟體應具備隱碼攻擊字串的處理能力。		✓	✓
	A.4.3.M 手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。		✓	✓
	P.1.1.B 手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。	✓	✓	✓
	P.1.2.B 當手機之無線傳輸技術功能確認開啟時,應給予使用者相對應的提示狀態。	✓	✓	✓
	P.1.3.B 手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。	✓	✓	✓
	P.2.1.B 手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。	✓	✓	✓
	P.2.2M 手機系統內建軟體應避免交談識別碼遭重送攻擊。		✓	✓
	P.2.3.M 手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。		✓	✓
	P.3.1.M 手機系統應具備通訊協定內容的錯誤處理能力。		✓	✓
	O.1.1.B 手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。	✓	✓	✓

檢測實驗室類型	檢測範圍（檢測細項）	安全等級		
		初	中	高
	O.1.2.B 手機系統於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。	✓	✓	✓
	O.2.1.B 手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。	✓	✓	✓
	O.2.2.B 手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。	✓	✓	✓
	O.2.3.B 手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。	✓	✓	✓
	O.2.4.M 手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。		✓	✓
	O.3.1.B 手機系統應提供回報安全性問題之管道。	✓	✓	✓
	O.3.2.M 手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。		✓	✓
第二型檢測實驗室	O.3.3.H 手機系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。			✓
	O.3.4.H 手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。			✓
	O.3.5.H 手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。			✓
	H.1.1.H 手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合 NIST、ANSI 及 IEEE 發布之金鑰使用及管理標準。			✓
	H.1.2.H 手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。			✓
	H.1.3.H 金鑰不得以明文方式存放於非揮發性之記憶體，且不得用任何方式匯出或直接對外傳輸。			✓
	H.2.1.H 手機實作之加密、解密及簽章演算法，應符合			✓

檢測實驗室類型	檢測範圍 （檢測細項）	安全等級		
		初	中	高
	NIST、ANSI 及 IEEE 發布之金鑰演算法標準。			
	H.2.2.H 手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。			✓
	H.2.3.H 金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。			✓

附件二、智慧型手機系統內建軟體資通安全檢測實驗室申請書

申請日期：____年____月____日

<table>
<tr><td colspan="2">申請人名稱
(法人/機構)</td><td colspan="2"></td><td>統一編號</td><td></td></tr>
<tr><td rowspan="3">代表人</td><td>姓名</td><td colspan="2"></td><td>性別</td><td></td></tr>
<tr><td>身分證統一編號</td><td colspan="2"></td><td>出生年月日</td><td></td></tr>
<tr><td>住居所</td><td colspan="4"></td></tr>
<tr><td colspan="2">檢測實驗室名稱</td><td colspan="4"></td></tr>
<tr><td colspan="2">檢測實驗室地址</td><td colspan="4">□□□-□□</td></tr>
<tr><td colspan="2">本國實驗室認證組織之認證證書</td><td>證書證號</td><td></td><td>有效期間</td><td></td></tr>
<tr><td colspan="2">檢測實驗室類別</td><td colspan="4">□ 第1型檢測實驗室
□ 第2型檢測實驗室</td></tr>
<tr><td colspan="2">聯絡人</td><td colspan="2"></td><td>電子信箱</td><td></td></tr>
<tr><td colspan="2">電話</td><td colspan="2"></td><td>傳真機</td><td></td></tr>
</table>

檢附文件：

□ 1.依法設立之本國法人、機構之證明文件影本。
□ 2.本國實驗室認證組織之認證證明文件影本。
□ 3.向本國實驗室認證組織申請檢測實驗室認證時，所檢附相關資料之光碟片。
□ 4.申請檢測實驗室之成員資格證明文件。
□ 5.申請檢測實驗室之檢測能力證明文件。
□ 6.其他經本會指定者。
□ 7.光碟片1片（內含本申請書及上述1至6項文件電子檔）。

※ 本檢測實驗室願遵守國家通訊傳播委員會智慧型手機系統內建軟體資通安全檢測實驗室管理作業要點及相關規定，如有違反致造成損害，願依相關法律負起責任。

謹　此

申請人（蓋章）：　　代表人（蓋章）：

附件三、智慧型手機系統內建軟體資通安全檢測實驗室認可證書

國家通訊傳播委員會

智慧型手機系統內建軟體資通安全
檢測實驗室認可證書

證書號碼：NCC-ICSEL-0X

一、申請人名稱：

二、代表人：

三、檢測實驗室名稱：

四、檢測實驗室地址：

五、認可檢測實驗室類別：

六、有效期間：自　　年　　月　　日至　　年　　月　　日止

（以下空白）

中 華 民 國　　年　　月　　日

主任委員

智慧型手機系統內建軟體資通安全檢測實驗室認可試辦說明（草案）

一、國家通訊傳播委員會（以下簡稱本會）為確保智慧型手機系統內建軟體資通安全品質，規劃於正式辦理智慧型手機系統內建軟體資通安全檢測實驗室（以下簡稱檢測實驗室）認可前，先行試辦檢測實驗室認可程序，特訂定本說明。

二、試辦期間自 105 年◯月◯日至 105 年◯月◯日止，本會保留變更之權利。

三、本會認可試辦之檢測實驗室（以下簡稱試辦實驗室）分為第 1 型及第 2 型試辦實驗室，由申請擔任試辦實驗室者（以下簡稱申請人）依智慧型手機系統內建軟體資通安全檢測技術規範之檢測範圍（如附件一）申請之。

四、本會受理申請人申請試辦實驗室認可，應審查下列各款事項：

（一）智慧型手機系統內建軟體資通安全檢測實驗室申請書（試辦期）（如附件二）。

（二）依法設立之本國法人、機構之證明文件影本。

（三）取得本國實驗室認證組織核發符合中華民國國家標準（以下簡稱 CNS）17025 或國際標準化組織所定標準（以下簡稱 ISO/IEC）17025 有關測試與校正實驗室能力一般要求規定之認證證明影本。

（四）申請人得以「智慧型手機系統內建軟體資通安全檢測服務計畫書」替代前項規定。前揭計畫書內容應載明申請人具備之實驗室管理程序，包括：檢測方法及流程、檢測設備及軟體工具、檢測結果品質管理程序等。

（五）三年內曾經實際執行智慧型手機系統內建軟體資通安全檢測經驗之證明文件。

（六）試辦實驗室之基本成員至少應有 3 人，分別為技術主管、品質主管及報告簽署人，並符合下列資格條件：

1. 申請第 1 型試辦實驗室認可者：

（1）至少有 1 人具備資訊安全相關管理職經驗 2 年以上或從事資

安測試評估實務工作達 2 年以上，並具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。

（2）至少有 1 人具備道德駭客認證(Certified Ethical Hacker，CEH）或國際網路資安認證（CompTIA Security+）有效之資訊安全相關專業證照。

（3）至少有 1 人具備下列任一有效之資訊安全相關專業證照：

A. 資訊系統安全專家證照（Certified Information Systems Security Professional，CISSP）

B. 資安軟體開發專家證照（Certified Secure Software Lifecycle Professional，CSSLP）

C. 資安分析專家證照（EC-Council Certified Security Analyst，ECSA）

D. 資安鑑識調查專家證照（EC-Council Computer Hacking Forensic Investigator，CHFI）

E. 滲透測試專家證照（GIAC Penetration Tester，GPEN）

F. 行動裝置資安分析專家證照（GIAC Mobile Device Security Analyst，GMOB）

G. 安全程式設計師證照（EC-Council Certified Secure Programmer，ECSP）

H. 資安專業人員證照（Systems Security Certified Practitioner，SSCP）

（4）非屬本款所列有效之資訊安全相關專業證照者，需經本會認可。

2. 申請第 2 型試辦實驗室認可者：

（1）應符合本說明申請第 1 型試辦實驗室認可者之成員資格條件。

（2）至少有 1 人取得 CCRA 或本會認可檢測實驗室之 ISO/IEC 15408 測試評估專業訓練時數達 360 小時以上之證明文件影本。

（七）試辦實驗室技術主管與報告簽署人不得同時擔任品質主管。

五、前點各款文件有不全或記載不完備者，本會應通知限期補正，屆期未補正或補正不完備者，不予受理其申請。補正期間以一個月為限。

六、申請人經本會審查符合第四點規定者，由本會核發智慧型手機系統內建軟體資通安全檢測實驗室認可證書（試辦期）(如附件三，以下簡稱認可證書)。

七、認可證書自核發之日起算六個月內有效，試辦實驗室得於本會正式辦理智慧型手機系統內建軟體資通安全檢測實驗室認可時，向本會申請認可。

八、試辦實驗室有下列情形之一者，認可證書失其效力：

（一）不符合第四點條件。

（二）檢測報告有虛偽不實。

（三）受理檢測申請案件，有無正當理由之拒絕或差別待遇。

九、試辦實驗室於認可證書有效期間出具之智慧型手機系統內建軟體資通安全檢測報告（以下簡稱檢測報告)，可由受測者提交向本會申請核發智慧型手機系統內建軟體資通安全審驗證明。

十、試辦實驗室與其服務人員對於受測者及檢測相關資料，應嚴守秘密，退職人員亦同。

附件一、智慧型手機系統內建軟體資通安全檢測技術規範之檢測範圍

檢測實驗室類型	檢測範圍（檢測細項）	安全等級		
		初	中	高
第一型檢測實驗室	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。	✓	✓	✓
	D.1.2.M(+)手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。		✓	✓
	D.2.1.B 手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。	✓	✓	✓
	D.2.2.M(+)手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。		✓	✓
	D.2.3.M(+)手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。		✓	✓
	D.3.1.B 手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。	✓	✓	✓
	D.3.2.B 手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。	✓	✓	✓
	D.3.3.B 手機系統應提供資料備份功能。	✓	✓	✓
	A.1.1.B 手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保使用者具備該帳戶使用權限。	✓	✓	✓
	A.2.1.B 手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。	✓	✓	✓
	A.2.2.B 手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。	✓	✓	✓

檢測實驗室類型	檢測範圍（檢測細項）	安全等級		
		初	中	高
	A.3.1.B 手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。	✓	✓	✓
	A.3.2.B 手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。	✓	✓	✓
	A.3.3.M 手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路連接埠(本地服務)」相符。		✓	✓
	A.3.4.M(+)手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。		✓	✓
	A.3.5.M(+)手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。		✓	✓
	A.4.1.B 手機系統內建軟體應提供回報安全性問題之管道。	✓	✓	✓
	A.4.2.M 手機系統內建軟體應具備隱碼攻擊字串的處理能力。		✓	✓
	A.4.3.M 手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。		✓	✓
	P.1.1.B 手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。	✓	✓	✓
	P.1.2.B 當手機之無線傳輸技術功能確認開啟時，應給予使用者相對應的提示狀態。	✓	✓	✓
	P.1.3.B 手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。	✓	✓	✓
	P.2.1.B 手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。	✓	✓	✓
	P.2.2M 手機系統內建軟體應避免交談識別碼遭重送攻擊。		✓	✓
	P.2.3.M 手機系統內建軟體與付費功能伺服器間之資料加		✓	✓

檢測實驗室類型	檢測範圍（檢測細項）	安全等級		
		初	中	高
	密傳輸，應使用安全之加密演算法。			
	P.3.1.M 手機系統應具備通訊協定內容的錯誤處理能力。		✓	✓
	O.1.1.B 手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。	✓	✓	✓
	O.1.2.B 手機系統於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。	✓	✓	✓
	O.2.1.B 手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。	✓	✓	✓
	O.2.2.B 手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。	✓	✓	✓
	O.2.3.B 手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。	✓	✓	✓
	O.2.4.M 手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。		✓	✓
	O.3.1.B 手機系統應提供回報安全性問題之管道。	✓	✓	✓
	O.3.2.M 手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。		✓	✓
第二型檢測實驗室	O.3.3.H 手機系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。			✓
	O.3.4.H 手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。			✓
	O.3.5.H 手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。			✓
	H.1.1.H 手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合 NIST、ANSI 及 IEEE 發布之			✓

檢測實驗室類型	檢測範圍（檢測細項）	安全等級		
		初	中	高
	金鑰使用及管理標準。			
	H.1.2.H 手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。			✓
	H.1.3.H 金鑰不得以明文方式存放於非揮發性之記憶體，且不得用任何方式匯出或直接對外傳輸。			✓
	H.2.1.H 手機實作之加密、解密及簽章演算法，應符合 NIST、ANSI 及 IEEE 發布之金鑰演算法標準。			✓
	H.2.2.H 手機實作之演算法，應依據各模式要求，產生初始化向量，並符合 NIST 發布之初始化向量要求。			✓
	H.2.3.H 金鑰使用之亂數，應符合 NIST、ANSI 發布之隨機位元產生規範要求。			✓

附件二、智慧型手機系統內建軟體資通安全檢測實驗室申請書（試辦期）

申請日期：____年____月____日

<table>
<tr><td colspan="2">申請人名稱
(法人/機構)</td><td colspan="2"></td><td>統一編號</td><td></td></tr>
<tr><td rowspan="3">代表人</td><td>姓名</td><td colspan="2"></td><td>性別</td><td></td></tr>
<tr><td>身分證統一編號</td><td colspan="2"></td><td>出生年月日</td><td></td></tr>
<tr><td>住居所</td><td colspan="4"></td></tr>
<tr><td colspan="2">試辦實驗室名稱</td><td colspan="4"></td></tr>
<tr><td colspan="2">試辦實驗室地址</td><td colspan="4">□□□-□□</td></tr>
<tr><td colspan="2">本國實驗室認證組織之認證證書</td><td>證書證號</td><td></td><td>有效期間</td><td></td></tr>
<tr><td colspan="2">試辦實驗室類別</td><td colspan="4">□ 第1型試辦實驗室
□ 第2型試辦實驗室</td></tr>
<tr><td colspan="2">聯絡人</td><td colspan="2"></td><td>電子信箱</td><td></td></tr>
<tr><td colspan="2">電話</td><td colspan="2"></td><td>傳真機</td><td></td></tr>
</table>

檢附文件：

□ 1.依法設立之法人、機構之證明文件影本。

□ 2.本國實驗室認證組織之認證證明文件影本。

□ 3.向本國實驗室認證組織申請檢測實驗室認證時，所檢附相關資料之光碟片。

□ 4.智慧型手機系統內建軟體資通安全檢測服務計畫書。

□ 5.申請試辦實驗室之成員資格證明文件。

□ 6.三年內曾經實際執行智慧型手機系統內建軟體資通安全檢測經驗之證明文件。

□ 7.其他經本會指定者。

□ 8.光碟片1片（內含本申請書及上述1至7項文件電子檔）。

※本試辦實驗室願遵守國家通訊傳播委員會智慧型手機系統內建軟體資通安全檢測實驗室認可試辦說明及相關規定，如有違反致造成損害，願依相關法律負起責任。

謹　此

申請人（蓋章）：　　代表人（蓋章）：

附件三、智慧型手機系統內建軟體資通安全檢測實驗室認可證書（試辦期）

國家通訊傳播委員會

智慧型手機系統內建軟體資通安全檢測實驗室認可證書（試辦期）

證書號碼：NCC-ICSEL-0X

一、申請人名稱：

二、代表人：

三、試辦實驗室名稱：

四、試辦實驗室地址：

五、認可試辦實驗室類別：

六、有效期間：自　　年　　月　　日至　　年　　月　　日止

（以下空白）

中 華 民 國　　年　　月　　日

主任委員

智慧型手機系統內建軟體資通安全審驗作業要點(草稿)

中華民國○年○月○日通傳○字第○號函下達

一、 國家通訊傳播委員會(以下簡稱本會)為執行組織法第三條第八款規定以及確保智慧型手機系統內建軟體資通安全品質,執行智慧型手機系統內建軟體資通安全審驗作業,特訂定本要點。

二、 本要點用詞定義如下:

(一)智慧型手機系統內建軟體:係指手機製造商、行動通信服務業者或應用軟體開發商,於使用者初次使用智慧型手機或於智慧型手機上初次啟用網路服務時,強制安裝之內建軟體。

(二)申請者:指申請智慧型手機系統內建軟體資通安全審驗之手機製造商或代理商。

(三)檢測實驗室:指經本會依「智慧型手機系統內建軟體資通安全檢測實驗室管理作業要點」認可或是依「智慧型手機系統內建軟體資通安全檢測實驗室認可試辦說明」認可之實驗室。

(四)審驗作業:指本會對檢測實驗室所出具之智慧型手機系統內建軟體資通安全檢測報告,審驗其是否符合相關規定,並出具書面審驗證明之程序。

三、 本會應訂定智慧型手機系統內建軟體資通安全檢測技術規範(以下簡稱手機資安技術規範),據以辦理智慧型手機系統內建軟體之資通安全檢測及審驗。

四、 智慧型手機系統內建軟體之資通安全審驗作業程序(如附件一)如下:

(一)申請智慧型手機系統內建軟體資通安全檢測報告(以下簡稱檢測報告):

1. 申請者應填具智慧型手機系統內建軟體資通安全檢測申請書(如附表一),並檢附下列文件正本或影本一份以及待測之智慧型手機樣品向檢測實驗室申請檢測;經檢測合格者,由檢測實驗室出具檢測報告。

(1) 中文或英文之使用手冊或說明書。

(2) 中文或英文之規格資料。

(3) 手機資安檢測技術規範要求之相關資料。

(4) 光碟片一份(包含檢測申請書及第一款至第三款電子檔)。

2. 檢測實驗室除留存申請書正本及光碟片外，其餘文件及樣品於出具檢測報告時一併發還申請者。
3. 檢測報告內容應包括下列各款：
   (1) 智慧型手機樣品 4x6 吋以上之清晰可辨之彩色照片或圖片。
   (2) 智慧型手機之廠牌、型號及名稱。
   (3) 申請者之名稱及地址。
   (4) 製造商之名稱及地址。
   (5) 智慧型手機經檢測合格之作業系統版本及系統內建軟體版本。
   (6) 智慧型手機經檢測合格之安全等級（分為初級、中級或高級）。
   (7) 檢測實驗室之名稱及地址。
   (8) 檢測報告之唯一識別碼及每頁之頁碼。
   (9) 測試儀器之名稱、廠牌及型號，及其校正日期、有效期限。
   (10) 適用之技術規範所定之檢測項目與標準。
   (11) 書面審查紀錄、實機測試數據及判定結果。
   (12) 檢測受理及完成日期。
4. 檢測報告應經檢測實驗室相關人員簽署。
5. 申請者提供之文件或樣品有誤漏或不全時，檢測實驗室應通知申請者於一個月內補正；逾期未補正或補正仍不完備者，駁回其申請。
6. 檢測不符合手機資安技術規範相關規定時，檢測實驗室應列舉不符合事項，並通知申請者改善及申請複檢，通知改善次數以二次為限，每次改善時間不得超過一個月。申請複檢逾期或第二次複檢仍不符合者，檢測實驗室應駁回其申請。

(二) 申請智慧型手機系統內建軟體資通安全審驗證明（以下簡稱審驗證明）：

1. 申請者取得符合手機資安技術規範之檢測報告後，應填具智慧型手機系統內建軟體資通安全審驗申請書(如附表三)，並檢附下列文件正本或影本一份向本會申請審驗，必要時，本會得要求申請者檢送智慧型手機樣品；經審驗合格者，由本會核發印有智慧型手機系統內建軟體安全等級標章（以下簡稱安全標章）式樣之審驗證明（如附表四）。

(1) 中文或英文之使用手冊或說明書。

(2) 中文或英文之規格資料。

(3) 公司登記證明文件或商業登記證明文件；申請者為代理商時，應檢附該智慧型手機製造商之設立相關證明文件。

(4) 申請者及檢測實驗室填具及用印之智慧型手機系統內建軟體資通安全檢測申請書（如附表一）。

(5) 檢測報告。

(6) 與檢測報告內容相符之公開資訊一覽表（如附表二）。

(7) 其他經本會指定之資料。

(8) 光碟片一份（包含審驗申請書及第一款至第七款電子檔）。

2. 本會除留存申請書正本及光碟片外，其餘文件於核發審驗證明時一併發還申請者。

3. 本會應依檢測報告評定智慧型手機之安全等級（分為初級、中級或高級）核發審驗證明。

4. 不同廠牌、型號之智慧型手機應分別申請審驗；經審驗合格之智慧型手機，當作業系統版本或系統內建軟體版本更新時，應針對有變更之部分重新申請檢測及審驗。須重新申請檢測之部分，由申請者提供並由檢測實驗室認定之。

5. 申請審驗智慧型手機之廠牌名稱如非屬申請者所有，申請者應提出使用該廠牌名稱之授權書。

6. 經審驗合格者，得依本會核發印有安全標章式樣之審驗證明，於通過審驗之智慧型手機之販賣宣傳管道或產品本身、包裝上使用安全標章。

7. 安全標章式樣如附件二。

8. 申請者提供之文件或樣品有誤漏或不全時，本會應通知申請者於一個月內補正；逾期未補正或補正仍不完備者，駁回其申請。

9. 審驗不合格時，本會應列舉不合格事項，通知申請者於二個月內改善並向本會申請複審；申請複審逾期或複審仍不合格者，駁回其申請。

五、 審驗證明遺失、毀損或證明內登載事項變更時，申請者得檢附下列文件向本會申請補發或換發：

（一）換（補）發申請函。

（二）智慧型手機符合技術規範之聲明書。

（三）公司或商業登記證明文件。

六、 申請審驗證明內登載事項變更，應符合下列情形之一：

（一）製造商變更或新增。

（二）申請者變更公司名稱。

（三）申請者因公司合併或分割，經報請主管機關同意由合併或分割後存續或新設之公司使用原審驗證明。

七、 本會得隨時抽驗公開陳列或販賣使用安全標章之智慧型手機。

八、 取得審驗證明後，經發現申請時所檢附之資料為偽造或虛偽不實者，本會得撤銷其審驗證明。

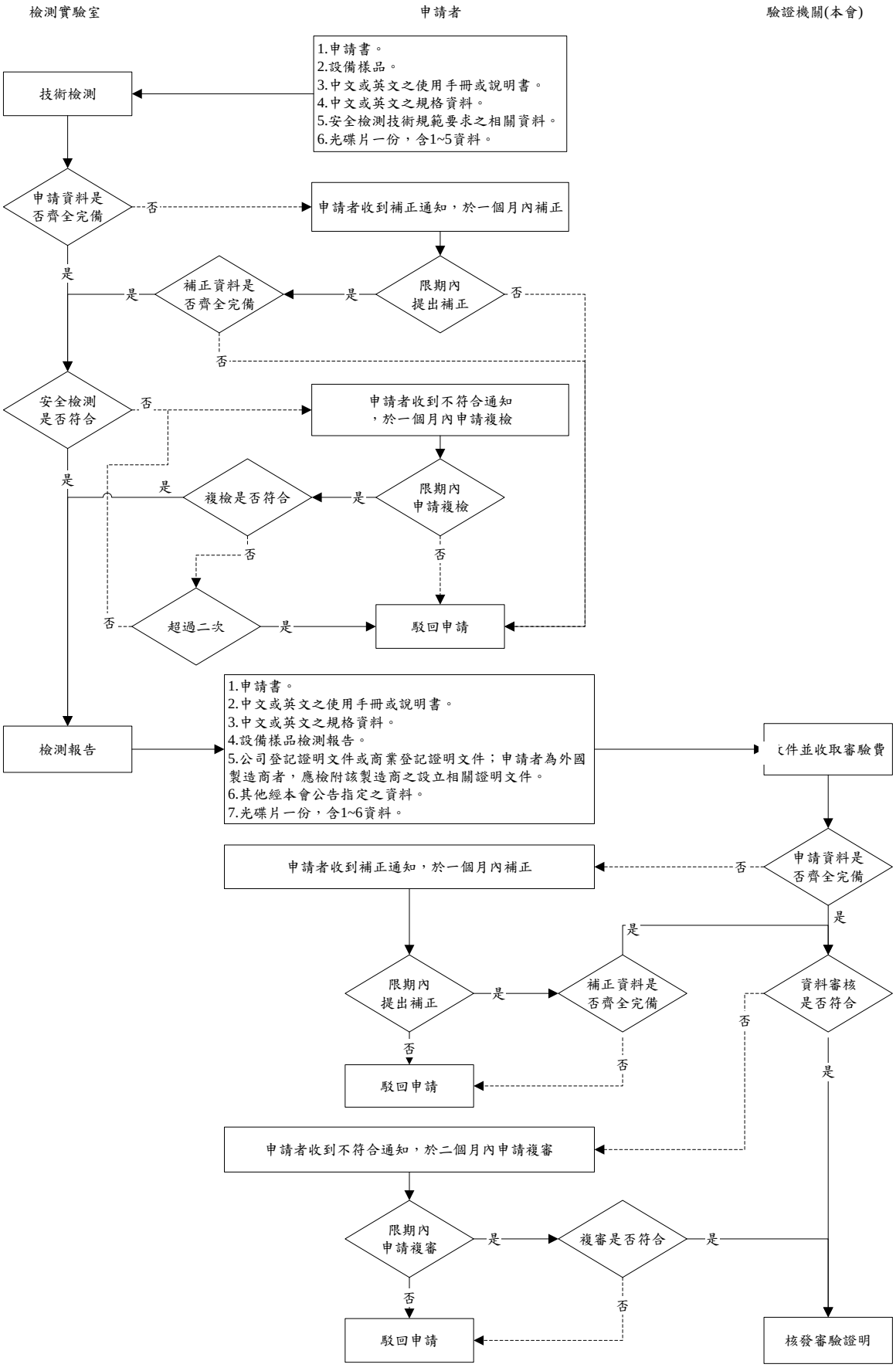
九、 取得審驗證明後，有下列情形之一者，本會得廢止其審驗證明：

（一）經抽驗未能符合手機資安技術規範者。

（二）因代理權、專利權爭議，經法院判決敗訴確定或違反其他規定致不得販賣經審驗合格之智慧型手機。

十、 審驗證明經撤銷或廢止者，本會得將原持有者及撤銷或廢止事由公告之。

附件一、智慧型手機系統內建軟體之資通安全審驗申請作業程序 (尚未調整)



附件二、智慧型手機系統內建軟體安全等級標章

一、星星數：

(一) 1 顆星：代表安全等級為初級。

(二) 2 顆星：代表安全等級為中級。

(三) 3 顆星：代表安全等級為高級。

二、序號編碼（YY mm sss tt L）：(軟協建議)

(一) YY：表年份（0-9，0-9）：西元 2007 年以 07 表示，2008 年以 08 表示…依此類推。

(二) mm：表設備商（A~Z，A-Z）:設備商 AA，設備商 AB…依此類推。

(三) sss：表設備型號（0-9，0-9）:型號 00，型號 01…依此類推。

(四) tt：表版本號碼（0-9，0-9）: 版本 00，系列 01…依此類推。

(五) L：表安全等級（1-3）：1:普級；2:中級；3:高級。

二、序號編碼（SP mmm sss）：(3 科建議)

(一) SP：固定碼，為 Smart Phone 之縮寫。

(二) mmm：表年份（105-999）。

(三) sss：表流水號（001-999）。

附表一、智慧型手機系統內建軟體資通安全檢測申請書

申請日期：　年　月　日

<table>
<tr><td colspan="2">申請者
(公司、商號名稱)</td><td>□製造商
□代理商</td><td colspan="3">○○○股份有限公司</td><td rowspan="5">申請者用印
(大、小章)</td></tr>
<tr><td colspan="2">統一編號</td><td colspan="4"></td></tr>
<tr><td colspan="2">營業所地址</td><td colspan="4">□□□-□□</td></tr>
<tr><td colspan="2">代表人姓名</td><td colspan="4"></td></tr>
<tr><td rowspan="2">聯絡人</td><td>姓名及職稱</td><td></td><td>電子信箱</td><td colspan="2"></td></tr>
<tr><td>聯絡電話</td><td></td><td>傳真機</td><td colspan="2"></td></tr>
<tr><td colspan="3">製造廠商及地址</td><td colspan="4">○○○股份有限公司
□□□-□□</td></tr>
<tr><td colspan="3">智慧型手機之廠牌/型號/名稱</td><td colspan="4">ex. APPLE / a16xx / iPhone 6s</td></tr>
<tr><td colspan="3">智慧型手機申請檢測之作業系統版本</td><td colspan="4">○○○-○○○-○○○</td></tr>
<tr><td colspan="3">申請檢測安全等級</td><td colspan="4">□初 □中 □中(含選擇檢測項目) □高 □高(含選擇檢測項目)</td></tr>
<tr><td colspan="2" rowspan="5">智慧型手機基本資訊</td><td>定位功能</td><td colspan="4">□ 美國全球定位系統 GPS　□ 歐盟伽利略 Galileo
□ 俄羅斯格洛納斯 GLONASS　□ 其他，_____
□ 中國北斗衛星導航(□可雙向傳輸)</td></tr>
<tr><td>無線傳輸技術</td><td colspan="4">□ 藍牙　□行動通訊網路 (□2G □3G □4G)
□ WLAN　□其他，_____
□ NFC (□ Peer-to-Peer Mode □ Read/Write Mode)</td></tr>
<tr><td>生物辨識</td><td colspan="4">□無 □有， 指紋辨識、…</td></tr>
<tr><td>外接記憶體</td><td colspan="4">□無 □有， microSD card、…</td></tr>
<tr><td colspan="2" rowspan="3">檢附智慧型手機樣品數量</td><td>初級</td><td colspan="4">□受測樣品 2 支</td></tr>
<tr><td>中級</td><td colspan="4">□受測樣品 2 支，並配合檢測項目需要提供管理者權限</td></tr>
<tr><td>高級</td><td colspan="4">□受測樣品 2 支，並配合檢測項目需要提供管理者權限</td></tr>
<tr><td colspan="2">檢附文件
(正本或影本)</td><td colspan="5">□ 1.中文或英文之使用手冊或說明書乙份
□ 2.中文或英文之規格資料乙份
□ 3.廠商自我宣告表乙份
□ 4.安全功能規格表、設計安全性表及安全架構表(申請高級者須檢附)
□ 5.光碟片乙份(含申請書及第 1 項至第 4 項內容)</td></tr>
<tr><td colspan="7">[註 1]檢測實驗室留存光碟片乙份，其餘文件與樣品於出具檢測報告後一併發還申請者。</td></tr>
<tr><td colspan="2" rowspan="4">檢測實驗室
(由實驗室填寫)</td><td colspan="4">實驗室名稱：
實驗室類型：□第 1 型 □第 2 型</td><td rowspan="4">檢測實驗室用印</td></tr>
<tr><td colspan="4">□ 1.出具檢測報告乙份，報告編號：_____，
安全等級為：□初級 □中級 □高級。
□ 2.留存本申請書正本及光碟片乙份。</td></tr>
<tr><td>受理日期</td><td></td><td>完成日期</td><td></td></tr>
<tr><td>聯絡人</td><td></td><td>聯絡電話</td><td></td></tr>
<tr><td colspan="7">[註 2]本申請書正本由檢測實驗室自行留存，另申請者應檢具本申請書影本向本會申請審驗。</td></tr>
</table>

附表二、與檢測報告內容相符之公開資訊一覽表

公開資訊一覽表

1.智慧型手機之廠牌/型號/名稱：APPLE / a16xx / iPhone 6s

2.審驗日期：○年○月○日

3.智慧型手機經審驗合格之作業系統版本：○○○-○○○-○○○

4.智慧型手機經審驗合格之內建軟體資訊如下：

編號	名稱	發行商	版本	屬性[註1]	功能說明	權限說明
APP01	電話	Company	1.2.2	■出廠預載 □銷售商加載 □無圖示	從通訊錄中撥打電話	READ_CONTACTS：用於訊息分享功能 ACCOUNT_MANAGER：用於新增帳號到社群 CAMERA：用於圖片紀錄功能 INTERNET：用於連線主機，取得最新公告
APP02	…					
…	…					

[註1] 內建軟體分為出廠預設、銷售商加載及無圖示3種。

[註2] 資料型別定義詳如「智慧型手機系統內建軟體資通安全檢測技術規範」4.用語釋義第4.11項。

附表三、智慧型手機系統內建軟體資通安全審驗申請書

申請日期：　年　月　日

<table>
<tr><td colspan="2">申請者
(公司、商號名稱)</td><td>□製造商
□代理商</td><td colspan="3">○○○股份有限公司</td></tr>
<tr><td colspan="2">統一編號</td><td colspan="4"></td></tr>
<tr><td colspan="2">營業所地址</td><td colspan="4">□□□-□□</td></tr>
<tr><td rowspan="3">代表人</td><td>姓名</td><td></td><td>性別</td><td colspan="2"></td></tr>
<tr><td>身分證統一編號</td><td></td><td>出生年月日</td><td colspan="2"></td></tr>
<tr><td>住居所</td><td colspan="4"></td></tr>
<tr><td rowspan="2">聯絡人</td><td>姓名</td><td></td><td>電子信箱</td><td colspan="2"></td></tr>
<tr><td>聯絡電話</td><td></td><td>傳真機</td><td colspan="2"></td></tr>
<tr><td colspan="2">製造廠商及地址</td><td colspan="4">○○○股份有限公司
□□□-□□</td></tr>
<tr><td colspan="3">智慧型手機之廠牌/型號/名稱</td><td colspan="3">ex. APPLE / a16xx / iPhone 6s</td></tr>
<tr><td colspan="3">出具檢測報告之檢測實驗室名稱</td><td colspan="3"></td></tr>
<tr><td colspan="3">智慧型手機經檢測合格之安全等級</td><td colspan="3">□初級 □中級 □高級</td></tr>
<tr><td colspan="3">智慧型手機經檢測合格之作業系統版本</td><td colspan="3">○○○-○○○-○○○</td></tr>
<tr><td>檢附文件</td><td colspan="5">(正本或影本)
□1.中文或英文之使用手冊或說明書乙份。
□2.中文或英文規格資料乙份。
□3.公司登記證明文件或商業登記證明文件乙份：申請者為代理商時，應檢附該智慧型手機製造商之設立相關證明文件。
□4.申請者及檢測實驗室填具及用印之智慧型手機系統內建軟體資通安全檢測申請書乙份。
□5.檢測報告乙份。
□6.與檢測報告內容相符之公開資訊一覽表乙份。
□7.其他經本會指定之資料(如：廠牌授權書)。
□8.光碟片乙份。(含本申請書及第1項至第7項內容)</td></tr>
</table>

申請日期：　年　月　日

申請者公司章：　　代表人簽章：

附表四、智慧型手機系統內建軟體資通安全審驗證明

國家通訊傳播委員會

智慧型手機系統內建軟體資通安全審驗證明

一、申 請 者：

（地址：□□□-□□　　）

二、製 造 商：

（地址：□□□-□□　　）

三、廠牌/型號：

四、審驗日期：　年　月　日

五、經審驗合格之作業系統版本及系統內建軟體版本：詳備註。

六、安全等級：□初級　□中級　□高級

七、安全等級標章：

驗證機關用印處

說明：

1. 經審驗合格者，得依本會核發印有安全標章式樣之審驗證明，於通過審驗之智慧型手機之販賣宣傳管道或產品本身、包裝上使用安全標章。
2. 取得審驗證明之資通設備，有下列情形之一者，得撤銷或廢止審驗證明：
   （1）經發現申請審驗時所檢附之資料為偽造或虛偽不實者。
   （2）經抽驗未能符合智慧型手機系統內建軟體資通安全檢測技術規範者。
   （3）因代理權、專利權爭議，經法院判決敗訴確定或違反其他規定致不得販賣經審驗合格之資通設備。

備註：經審驗合格之作業系統版本及系統內建軟體版本詳如下：

項次	作業系統版本	系統內建軟體版本	審驗日期	備註
1.	○○○-○○○-○○○	詳「公開資訊一覽表-01」	○年○月○日	初次審驗
2.	○○○-○○○-○○○	詳「公開資訊一覽表-02」	○年○月○日	OS升版
3.				

附件 5 所測暢銷市售手機資安檢測結果

智慧型手機系統內建軟體資通安全檢測技術規範

所測暢銷市售手機資安檢測結果
綜合分析報告

目　次

壹、 前言 ..... 附件 5-1

貳、 檢測結果綜合分析 ..... 附件 5-2

一、 測試手機之選定 ..... 附件 5-2

二、 檢測要求及檢測範圍 ..... 附件 5-3

三、 技術規範草案可行性與合理性評估 ..... 附件 5-6

四、 修正規範檢測結果 ..... 附件 5-19

參、 綜合檢討與建議 ..... 附件 5-33

一、 送測之手機未具備管理者權限 ..... 附件 5-33

二、 廠商自我宣告表資訊不足 ..... 附件 5-33

圖 目 次

圖 1　臺灣智慧行動手機廠牌排名 ..... 附件 5-3
圖 2　測項可行性與合理性評估流程 ..... 附件 5-6
圖 3　檢測層別與測試項目 ..... 附件 5-20
圖 4　各手機測試結果統計比較 ..... 附件 5-22
圖 5　E-mail 帳號以明文方式儲存於非作業系統保護區圖示 ..... 附件 5-24
圖 6　敏感性資料以明文方式儲存於手機內 ..... 附件 5-25
圖 7　延伸標記語言攻擊成功圖示 ..... 附件 5-27
圖 8　定位資訊明文傳輸 ..... 附件 5-28
圖 9　加密協定與加密演算法 ..... 附件 5-30
圖 10　手機系統無回應 ..... 附件 5-31

表 目 次

表 1　2011~2014 年智慧型手機作業系統市占率變化(來源：IDC) ....附件 5-2
表 2　受測樣機清單 .....附件 5-3
表 3　資料型別分類表 .....附件 5-5
表 4　第一版規範之檢測結果系統比較 .....附件 5-8
表 5　初級與中級測試項目之測試結果一覽 .....附件 5-20
表 6　測項 D.2.1.B 之測試結果.....附件 5-23
表 7　測項 D.2.2.M(+)之測試結果.....附件 5-25
表 8　測項 A.4.3.M 之測試結果.....附件 5-26
表 9　測項 P.2.1.B 之測試結果.....附件 5-28
表 10　測項 P.2.4.M 之測試結果.....附件 5-29
表 11　測項 P.3.1.M 之測試結果.....附件 5-31
表 12　測項 O.2.3.B 之測試結果.....附件 5-32

壹、前言

本計畫主要乃針對智慧型手機系統內建軟體之資通安全，訂定智慧型手機系統內建軟體資安檢測技術規範，希望協助廠商在智慧型手機系統內建軟體資通安全上能達一定的要求，且進一步幫助消費者做把關動作，讓消費者在拿到智慧型手機使用時能安心無虞。

技術規範制定上有分為幾個階段，分別是國內外相關法規的蒐集與分析、再參考這些法規之內容制訂出相關資安要求與檢測項目、最後依據制訂出的要求與檢測項目去實際進行測試，判斷測項之可行性與合理性，若不合理則會再進行測項的修改調整。

本報告將針對智慧型手機系統內建軟體資安檢測技術規範(以下簡稱本規範)之可行性評估及手機實際試測結果等進行分析與討論。

貳、檢測結果綜合分析

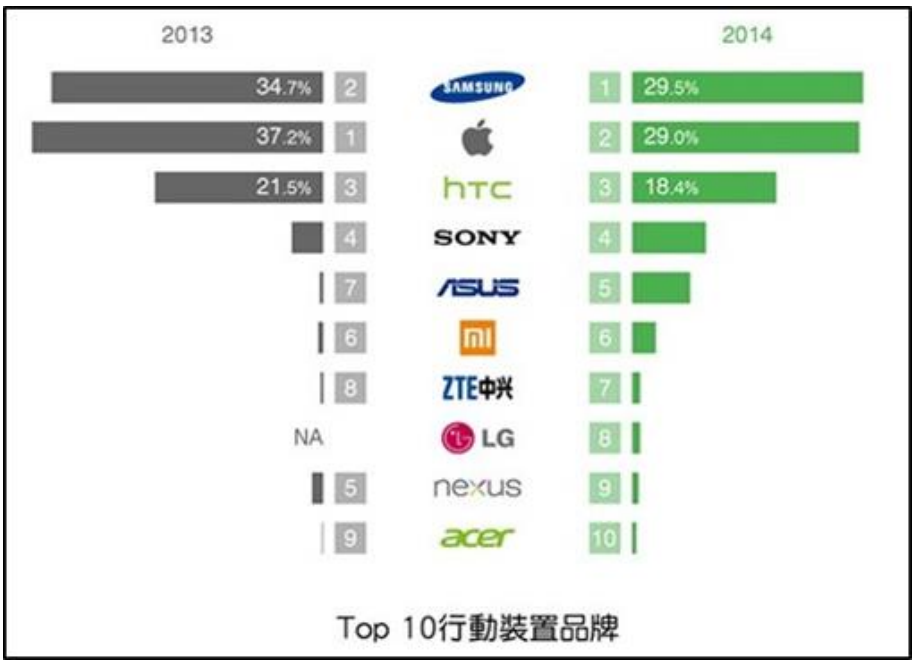
一、測試手機之選定

因市場手機廠牌眾多，為能適切瞭解我國人普遍使用之手機可能潛在之資安問題，乃針對作業系統及代表性廠牌市占率高者為優先考量。在手機作業系統方面，以 IDC 國際數據資訊提供之調查報告顯示 2011 年至 2014 年有關智慧型手機作業系統排名，因 Android、iOS 及 Windows 這三款作業系統即佔了整個市場的 98.8%，故測試上即考慮這三類作業系統之手機，IDC 調查報告結果如下表 1 所示。

表1　2011~2014 年智慧型手機作業系統市占率變化(來源：IDC)

作業系統 / 時間	**Android**	**iOS**	**Windows**	**其他**
2014 年第 2 季	84.7%	11.7%	2.5%	1.2%
2013 年第 2 季	79.6%	13.0%	3.4%	4.0%
2012 年第 2 季	69.3%	16.6%	3.1%	11%
2011 年第 2 季	36.1%	18.3%	1.2%	44.4%

而手機廠牌部分的考慮，以 Vpon 之市調顯示 2013 年至 2014 年之手機廠牌在台熱銷前 5 名有三星、蘋果、HTC、SONY 及華碩，Vpon 調查結果如下圖 1 所示；iOS 系統之手機就以蘋果的近期新款手機，Windows 系統手機雖無擠進前 5 名但屬重要代表性作業系統，故其中 1 款待測樣機為微軟之智慧型手機；Andorid 系統手機則依據熱銷及代表性程度，故選擇 SAMSUNG、HTC、SONY 及小米之近期新款手機作為測試標的，其選定之受測樣機詳見詳見表 2。



資料來源：Vpon

圖1　臺灣智慧行動手機廠牌排名

表2　受測樣機清單

對應代號	廠牌	型號
MOBILE01	SAMSUNG(Galayx S6)	SM-G9250
MOBILE02	Microsoft	RM-1065
MOBILE03	APPLE(iPhone 6)	3A019TA/A
MOBILE04	HTC	Desire 728 dual sim
MOBILE05	SONY	Xperia Z3+
MOBILE06	MI	Redmi Note 2

資料來源：本計畫彙整

後續相關檢測之受測樣機均以代號表之。

二、檢測要求及檢測範圍

自 12/1 起針對初版技術規範內容進行 6 支手機安全等級中級(M)之

完整可行性測試，高級規範內容則因手機業者無法配合填寫相關書審內容，故未納入本次可行性評估範圍。本報告則針對各檢測細項進行測試結果之分析與比較。

(一)內建軟體屬性

智慧型手機系統內建軟體(以下簡稱系統內建軟體)包含出廠預載軟體、銷售商加載軟體及無圖示軟體 3 種屬性，其中無圖示軟體得由申請者自行選擇是否檢測：

1.出廠預載軟體：智慧型手機出廠時預設搭載安裝之應用程式，且使用者可透過圖示啟動。

2.銷售商加載軟體：智慧型手機銷售時預設搭載或首次連結網路後自動安裝之應用程式，且使用者可透過圖示啟動。

3.無圖示軟體：於上述兩種情況所安裝之應用程式，使用者無法透過圖示啟動，且該軟體會將資料回傳至遠端伺服器。

(二)檢測層別

依據國際間對智慧型手機安全之分層概念，將智慧型手機區分為資料層、應用程式層、通訊協定層、作業系統層及硬體層五個層別，考量不同層別可能面臨的資訊安全風險有所不同，故對各層別分別訂定檢測項目。各檢測層別之主要包含內容如下：

- 資料層(Information/Data)：主要包含資料的傳送、儲存或使用等相關安全。
- 應用程式層(APPs)：主要包含手機系統內建軟體等相關安全。
- 通訊協定層(Protocol)：主要包含無線傳輸技術及通訊協定等相關安全。

- 作業系統層（Operating System）：主要包含作業系統相關服務與身分辨識等相關安全。
- 硬體層（Hardware）：主要包含金鑰與演算模組等安全。

(三)資料型別

本規範依資料之敏感性與是否為使用者輸入等兩個因素，將其分成第 1 型、第 2 型、第 3 型、第 4 型。資料型別分類說明如表 3。

表3　資料型別分類表

型別	判斷標準		範例
	是否屬於敏感性資料	是否為使用者輸入	
第 1 型	是	是	1.本規範用語釋義之個人資料。 2.手機相關資訊：簡訊內容、通話錄音、裝置密碼、帳號密碼、相片。
第 2 型	是	否	IMEI、IMSI[註]、定位資訊。
第 3 型	否	否	APP 列表、音樂播放資訊、手機作業系統、手機型號、手機韌體版本、MCC、MNC、行動通信業者、網路傳送方式、設定檔。
第 4 型	N/A	N/A	資料加密、協定加密、無加密但內容未知。
[註]IMEI 碼及 IMSI 碼須與行動通信業者或手機廠商之銷售保固連結，該 IMEI 碼及 IMSI 碼才具備個資識別性，但使用人與登錄人可能不同，故歸類為第 2 型。			

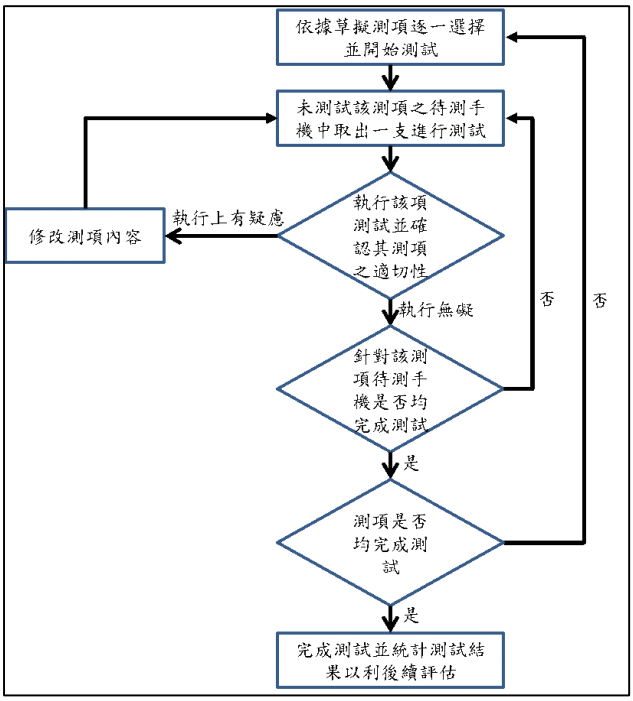
資料來源：智慧型手機系統內建軟體資安檢測技術規範草案

三、技術規範草案可行性與合理性評估

(一)可行性評估做法

本次檢測主要針對於 104 年 11 月底所訂定之規範草案進行可行性評估，確保制訂出之檢測項目能適用於國人普遍使用之智慧型手機，故試測範圍包含三大主流作業系統及銷售排行榜前幾名之手機品牌。其可行性與合理性評估之作法如　所示，

- 依據草擬之規範之測項逐一測試。
- 依據先前決定之待測機種，從中挑選一款進行測試。
- 判斷該測項之測試可行性，若執行上有疑慮則回報規範制定組進行修改，反之，若測試執行無礙則換下款未測之手機進行該測項之測試，反覆執行至所有手機於該測項皆確實完成測試。
- 進行下一個測項，或測試均完成則統計測試結果以利後續評估。



資料來源：本計畫彙整

圖2　測項可行性與合理性評估流程

(二)可行性評估範圍

本規範訂定出之檢測項目考慮範圍包含資料層、應用程式層、通訊協定層、作業系統層及硬體層，並劃分初級(B)、中級(M)、高級(H)三個安全等級，自 12/1 起針對初版技術規範內容進行 6 支手機安全等級中級(M)之完整可行性測試，高級規範內容則因手機業者無法配合填寫相關書審內容，故未納入本次可行性評估範圍。

(三)跨平台可行性評估

本規範相關檢測項目因涉及到不同的作業系統，包含 Android、iOS 及 Windows 這三大作業系統，不同作業系統之設計架構各異，實際測試作業上發現部分檢測項目因其系統原本之特性而無法確實執行測試，以及檢測條件、方法、判定標準等有疑慮之測項將其測項內容與屬性進行修改，測項於各作業系統適用性測試結果彙整詳見表 4。

初版規範內容共規劃基本與進階 2 個安全等級，計有 41 個檢測項目，其中 Android 作業系統之手機，除部分測項需獲得手機管理者權限方可檢視判斷該測項是否通過檢測外，均可執行測試；iOS 系統與 Windows 系統因較為封閉，其中又以 Windows 之手機更甚，故共初次檢測時共有 11 個測項因這兩個作業系統之特性而不適用無法進行檢測，而相關不適用之測項將於後續說明。

表4　第一版規範之檢測結果系統比較

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
D.1 首次執行手機系統內建軟體時，於存取敏感性資料前須經過使用者同意。	D.1.1 手機系統內建軟體存取敏感性資料之提示機制	基礎	可	可	可	
D.2 手機系統應提供使用者拒絕內建軟體存取敏感性資料之權利。	D.2.1 手機系統內建軟體提供使用者拒絕存取敏感性資料之機制	基礎	可	不適用	不適用	納入選測項目
D.3 手機系統之內建軟體間，應提供敏感性資料分享之提示機制，避免未經許可的資料共享行為。	D.3.1 手機系統內建軟體間分享敏感性資料之提示機制	基礎	可	可	可	
D.4 手機系統內建軟體須將敏感性資料儲存於作業系統保護區域，並提供資料加密功能，避免遭不	D.4.1 手機系統內建軟體不應將敏感性資料儲存於暫存檔或記錄檔中	進階	可 (需 root)	可 (需 JB)	不適用	調整檢測項目，將暫存檔與記錄檔改為非作業

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
正當方式取得資料並得以解密回明文資料。						系統保護區內
	D.4.2 手機系統內建軟體儲存敏感性資料時應以密文方式儲存	進階	可 (需 root)	可 (需 JB)	不適用	納入選測項目
	D.4.3 手機系統內建軟體與遠端伺服器溝通之帳號密碼不應儲存於非作業系統保護區內	基礎	可	可	可	
	D.4.4 手機系統內建軟體與遠端伺服器溝通之帳號密碼不應以明文方式存在於程式碼中	進階	可 (需 root)	不適用	不適用	納入選測項目
D.5 手機系統內建軟體透過無線網路傳輸敏	D.5.1 手機系統內建軟體使用	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
感性資料時，應使用加密傳輸，以確保敏感性資料安全。	WLAN 傳輸敏感性資料					
	D.5.2 手機系統內建軟體使用行動通訊網路傳輸敏感性資料	基礎	可	可	可	
D.6 手機系統應提供使用者資料之遠端保護能力及相關安全設定，讓使用者可在遠端啟動保護功能，以保護手機系統內之資料。	D.6.1 使用者資料的遠端鎖定	基礎	可	可	可	
	D.6.2 使用者資料的遠端刪除	基礎	可	可	可	
D.7 手機系統應支援備份功能。 使用者資料的備份包括本機備份與遠端備份兩種：本機備份是通過手機的周邊介面進行資料備	D.7.1 使用者資料的本機備份	基礎	可	可	不適用	調整檢測項目，不區分遠端或本機備份型態
	D.7.2 使用者資料的遠端備份	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
份；遠端備份是通過 WLAN 或行動網路將使用者資料備份至遠端伺服器。						
A.1 手機系統內建軟體執行手機系統功能前，須經使用者同意。	A.1.1 手機系統內建軟體執行手機系統功能	進階	可 (需 root)	可 (需 JB)	不適用	調整檢測項目強調未經同意於背景執行系統功能，並納入選測項目
A.2 手機系統內建軟體在使用付費服務前，應提示並取得使用者同意後才能進行資源之使用。	A.2.1 付費服務的提示	基礎	可	可	可	
A.3 手機系統內建軟體在初次存取使用者帳戶時 ，應先行認證使用者	A.3.1 手機系統內建軟體使用者身分認證與授權機制	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
身分與其權限，以避免使用者帳戶遭到誤用或濫用。						
A.4 手機系統內建軟體須避免交談識別碼被重送攻擊。	A.4.1 手機系統內建軟體交談識別碼安全	進階	可	可	可	
A.5 手機系統內建軟體應確認伺服器憑證之有效性，以避免使用過期的憑證。	A.5.1 手機系統內建軟體伺服器憑證有效性	基礎	可	可	可	
A.6 手機系統內建軟體與伺服器間之資料加密傳輸，應使用安全之加密演算法。	A.6.1 手機系統內建軟體與伺服器加密演算法檢測	進階	可	可	可	
A.7 手機系統內建軟體應可識別其發行商與版本資訊，以確保使用者瞭解其來源。	A.7.1 來源識別	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
A.8 手機系統應提供使用者可查詢與關閉執行中之內建軟體。	A.8.1 手機系統內建軟體之關閉	基礎	可	可	可	
	A.8.2 手機系統內建軟體之背景執行關閉	基礎	可	不適用	不適用	納入選測項目
A.9 關閉手機系統內建軟體時，應停止該內建軟體所有相關程序。	A.9.1 手機系統內建軟體關閉之功能檢測	進階	可 (需 root)	可 (需 JB)	不適用	修改檢測方法並合併 A.9.2 納入選測項目
	A.9.2 手機系統內建軟體背景執行關閉之功能檢測	進階	可 (需 root)	可 (需 JB)	不適用	修改檢測方法並合併 A.9.1 並納入選測項目
A.10 手機系統內建軟體應具惡意字串的處理能力。	A.10.1 隱碼攻擊字串檢測	進階	可	可	可	
	A.10.2 延伸標記語言安全檢測	進階	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
A.11 手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路服務連接埠」相符。(搭配我宣告)	A.11.1 網路連接埠控管	進階	可	可 (調整測試方式)	可 (調整測試方式)	調整檢測方式
A.12 手機系統內建軟體應僅使用其所需之權限，且權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。	A.12.1 功能權限聲明之驗證	基礎	可	可	可	
P.1 手機與不同設備以有線周邊介面進行第一次連接時，應給予使用者相對應的提示機制。	P.1.1 有線周邊介面連接建立之提示機制	基礎	可	可	可	
P.2 對於具備無線介面的手	P.2.1 無線介面之開關	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
機，應提供使用者可進行開啟及關閉之功能介面。						
P.3 當手機的無線介面確認開啟時，應給予使用者相對應的提示狀態。	P.3.1 無線介面連線之提示狀態	基礎	可	可	可	
P.4 手機與不同設備以無線周邊介面進行第一次連接時，應給予使用者相對應的提示機制，且須經使用者同意後才可建立連線。	P.4.1 無線介面配對連線建立之提示機制	基礎	可	可	可	
P.5 手機系統內建軟體應具通訊協定內容的錯誤處理能力。	P.5.1 強健性測試	進階	可	可	可	
O.1 手機系統應支援待機時設定保護機制，以保護個	O.1.1 手機開機及螢幕解鎖保護機制	基礎	可	可	可	

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
人資訊，避免遭未經授權的使用。	O.1.2 手機之強制鎖定	基礎	可	可	可	
	O.1.3 手機密碼儲存之檢測	進階	可 (需 root)	可 (需 JB)	不適用	修改檢測條件
O.2 手機的作業系統更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。	O.2.1 作業系統更新來源	基礎	可	可	可	
O.3 手機的作業系統下載更新或安裝更新時應提供更新公告，並告知使用者安全風險之資訊。	O.3.1 作業系統更新公告	基礎	可	可	可	
O.4 當手機韌體更新方式為手動上傳方式，作業系統應檢查韌體簽章、完整性及可用性，以避免遭惡意	O.4.1 韌體保護機制	進階	可	不適用	不適用	建議刪除，現大多以網路更新系統而不以韌體更

原技術要求及編號	原檢測項目及編號	安全等級	測項於不同作業系統之適用性			建議調整方式
			Android	iOS	Windows	
修改之韌體更新至手機系統。						新，且iOS &WP皆不適用，故刪除
O.5 手機系統內建軟體應提供回報安全性問題之管道。	O.5.1 手機系統內建軟體問題回報	基礎	可	可	可	
O.6 手機的作業系統應具備位址空間配置隨機化功能，以避免程式與參考函式在記憶體中的位址為固定值。	O.6.1 位址空間配置隨機化	進階	可	可(廠商提供佐證資料)	可(廠商提供佐證資料)	調整檢測方法

資料來源：本計畫彙整

(四)檢測細項合理性評估

於上述系統測試分析結果有 11 項被評斷為不適用，其詳細說明如下：

1.原技術要求 D.2 與原檢測項目 D.2.1 之測項

在 iOS 系統手機上僅 GPS 可設定關閉，而 Windows 系統之手機也僅部分內建軟體有提供可拒絕存取的功能，而在 Android

系統之手機雖然也有類似狀況，但因為 Android 系統之手機獲得管理者權限後就能下指令方式去查看其軟體存取之動態行為，故該測項會因作業系統不同而無法落實測試之執行。

2.原技術要求 D.4 與原檢測項目 D.4.1、D.4.2 之測項

該測項因需檢視暫存檔或紀錄檔中是否有儲存敏感性資料，故需取得最高管理者權限才可檢視作業系統保護區之資料，而本次執行試測之樣機其中僅 Android 系統之手機有獲得管理者權限，且目前沒有任何關於 Windows 系統手機於管理者權限的操作方法，所以無法執行該檢測項目。

3.原技術要求 D.4 與原檢測項目 D.4.4 之測項

該測項需考慮逆向工程之技術來檢視程式碼內是否有發現帳密是明文方式儲存，目前僅 Android 系統較為可行，而 iOS 與 Windows 系統之內建軟體均因技術尚無法克服而目前判斷為不適用。

4.原技術要求 D.7 與原檢測項目 D.7.1 之測項

因該測項考慮本機之備份機制，但 Windows 系統之手機僅提供雲端備份機制，故該測項判斷為不適用。

5.原技術要求 A.1 與原檢測項目 A.1.1 之測項

該測項需檢視通話紀錄與簡訊資料檔，但是同樣沒獲得管理者權限之手機則無法查詢，有技術上問題。

6.原技術要求 A.8 與原檢測項目 A.8.2 之測項

該測項需有介面工瀏覽正在執行中的應用軟體之功能，但在 iOS 與 Windows 系統之手機卻無提供此功能服務。

7.原技術要求 A.9 與原檢測項目 A.9.1 之測項

該測項需透過系統指令的方式去查看所有執行之應用軟體，故需獲得最高管理者權限外，且 Windows 系統之手機尚無相關可查詢之指令資訊，亦無法判斷。

8.原技術要求 A.9 與原檢測項目 A.9.2 之測項

iOS 與 Windows 系統均無提供瀏覽執行中程式的功能，故判斷為不適用。

9.原技術要求 O.1 與原檢測項目 O.1.3 之測項

該測項需針對生物辨識螢幕所定功能之手機去判斷，但目前 Windows 系統之手機並不支援此功能。

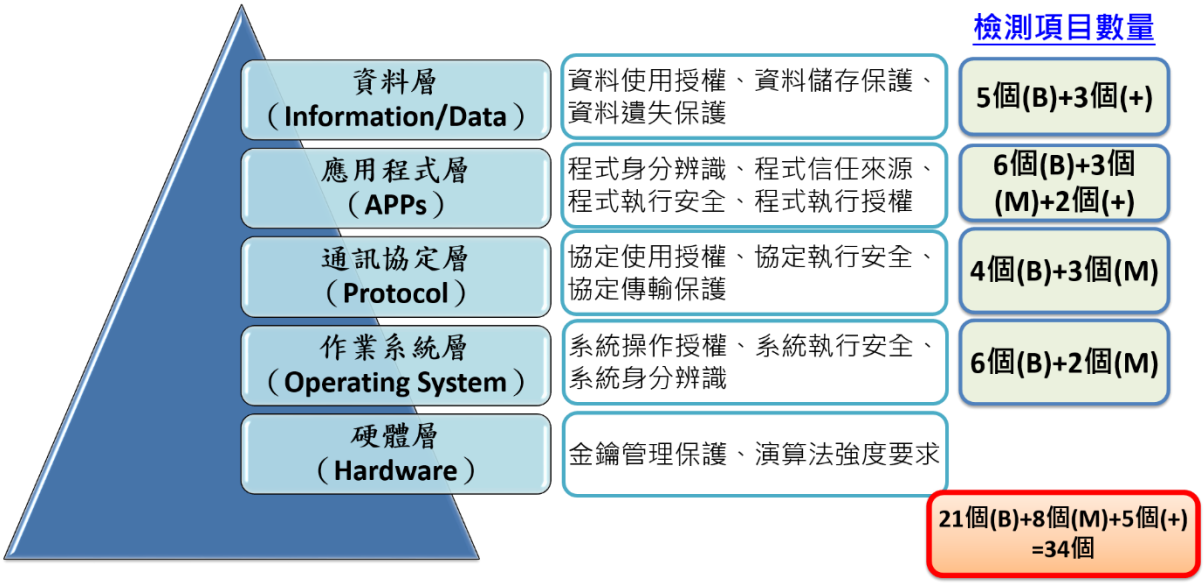
10.原技術要求 O.4 與原檢測項目 O.4.1 之測項

目前 iOS 與 Windows 系統之手機並不支援手動更新韌體之功能，故判斷該項為不適用。

上述這 11 項測項，經判斷非均適用於 Android、iOS 及 Windows 之系統手機，故經建議可修改檢測條件、檢測方法或判定標準，以達可跨平台檢測之目標，但若因作業系統設計關係或條件與技術無法進行，則建議可將刪除測項或將其設計為選測項目，由送測單位自由選擇是否檢測，以確保本規範必檢測項目可滿足跨平台的要求。

四、修正規範檢測結果

經過規範調整後，安全等級調整為初級(B)、中級(M)及高級(H)，中級相關必測項目與選測項目共 29+5=34 個測項，其檢測層別與測項分佈詳見資料來源：所示。



資料來源：本計畫彙整

圖3　檢測層別與測試項目

依本次 6 款測試樣機，包含 4 款 Android 系統手機及 iOS 與 Windows 系統手機各 1 款，針對修正更新後之 34 個測項，其測試結果一覽如表 5，其中該測項之測試結果若符合檢測判定標準則標示為符合，若不符合判定標準則標示為不符合，若因特殊原故導致測試結果無法判斷或不適用則標示為 NA。

表5　初級與中級測試項目之測試結果一覽

檢測細項	MOBILE 01	MOBILE 02	MOBILE 03	MOBILE 04	MOBILE 05	MOBILE 06
D.1.1.B	符合	符合	符合	符合	符合	符合
D.1.2.M(+)	符合	符合	符合	符合	符合	符合
D.2.1.B	符合	符合	符合	符合	不符合	符合
D.2.2.M(+)	不符合	NA	NA	不符合	不符合	不符合
D.2.3.M(+)	符合	NA	NA	符合	符合	符合

檢測細項	MOBILE 01	MOBILE 02	MOBILE 03	MOBILE 04	MOBILE 05	MOBILE 06
D.3.1.B	NA	符合	符合	符合	符合	符合
D.3.2.B	NA	符合	符合	符合	符合	符合
D.3.3.B	符合	符合	符合	符合	符合	符合
A.1.1.B	符合	符合	符合	符合	符合	符合
A.2.1.B	符合	符合	符合	符合	符合	符合
A.2.2.B	符合	符合	符合	符合	符合	符合
A.3.1.B	符合	符合	符合	符合	符合	符合
A.3.2.B	NA	NA	NA	NA	NA	NA
A.3.3.M	NA	NA	NA	NA	NA	NA
A.3.4.M(+)	符合	NA	NA	符合	符合	符合
A.3.5.M(+)	NA	NA	NA	NA	NA	NA
A.4.1.B	NA	NA	NA	符合	NA	NA
A.4.2.M	符合	符合	符合	符合	符合	符合
A.4.3.M	不符合	NA	NA	不符合	不符合	符合
P.1.1.B	符合	符合	符合	符合	符合	符合
P.1.2.B	符合	符合	符合	符合	符合	符合
P.1.3.B	符合	符合	符合	符合	符合	符合
P.2.1.B	符合	不符合	符合	符合	符合	符合
P.2.2.M	符合	符合	符合	符合	符合	符合
P.2.3.M	符合	符合	NA	符合	符合	符合
P.3.1.M	符合	不符合	符合	不符合	符合	符合
O.1.1.B	NA	NA	NA	NA	NA	NA
O.1.2.B	符合	NA	符合	NA	符合	符合

檢測細項	MOBILE 01	MOBILE 02	MOBILE 03	MOBILE 04	MOBILE 05	MOBILE 06
O.2.1.B	符合	符合	符合	符合	符合	符合
O.2.2.B	符合	符合	符合	符合	符合	符合
O.2.3.B	符合	不符合	符合	符合	符合	不符合
O.2.4.M	符合	NA	符合	符合	符合	符合
O.3.1.B	符合	符合	符合	符合	符合	符合
O.3.2.M	符合	符合	NA	NA	符合	NA

資料來源： 本計畫彙整

各測試樣機於初、中級測項之試測結果之統計比較詳見圖 4

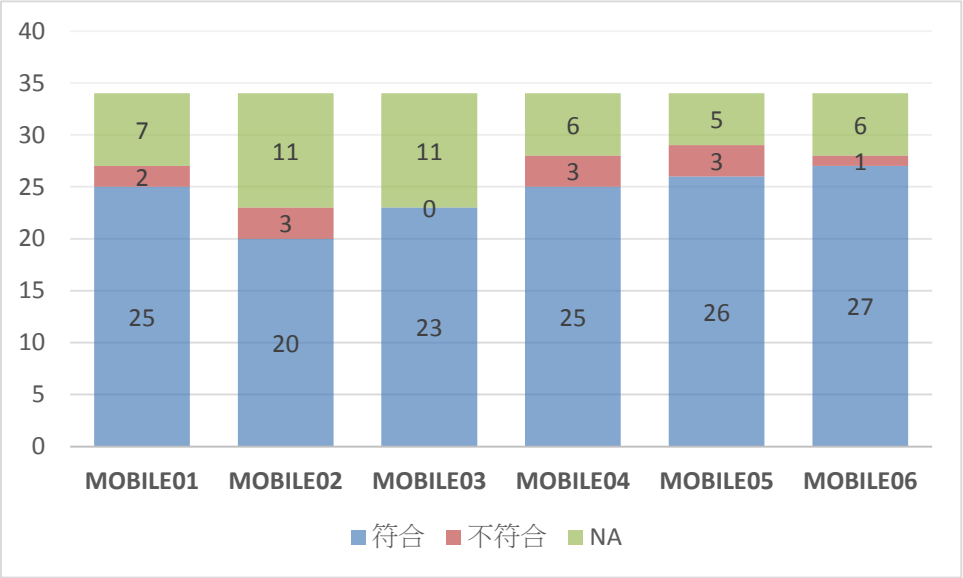


圖4　各手機測試結果統計比較

資料來源： 本計畫彙整

(一)檢測結果比較分析

針對各測試樣機之測試結果有不符合或 NA 之測項進行比較與分析如下。

1.資料儲存保護之比較(檢測細項：D.2.1.B)

(1)檢測說明與分析

於資料儲存保護部分，在檢測細項 D.2.1.B，要求手機系統內建軟體應將帳號密碼儲存於作業系統保護區內或以加密方式儲存。

該測項之重點在於首先其內建軟體之檢測條件須滿足：

- 受測軟體具備帳號密碼登入功能
- 資料型別：帳號密碼
- 受測軟體屬性：出廠預載、銷售商加載

且考慮是否發現帳號密碼明文儲存於非作業系統保護區內，若有發現則不符合該測項之檢測要求,反之則符合檢測要求。

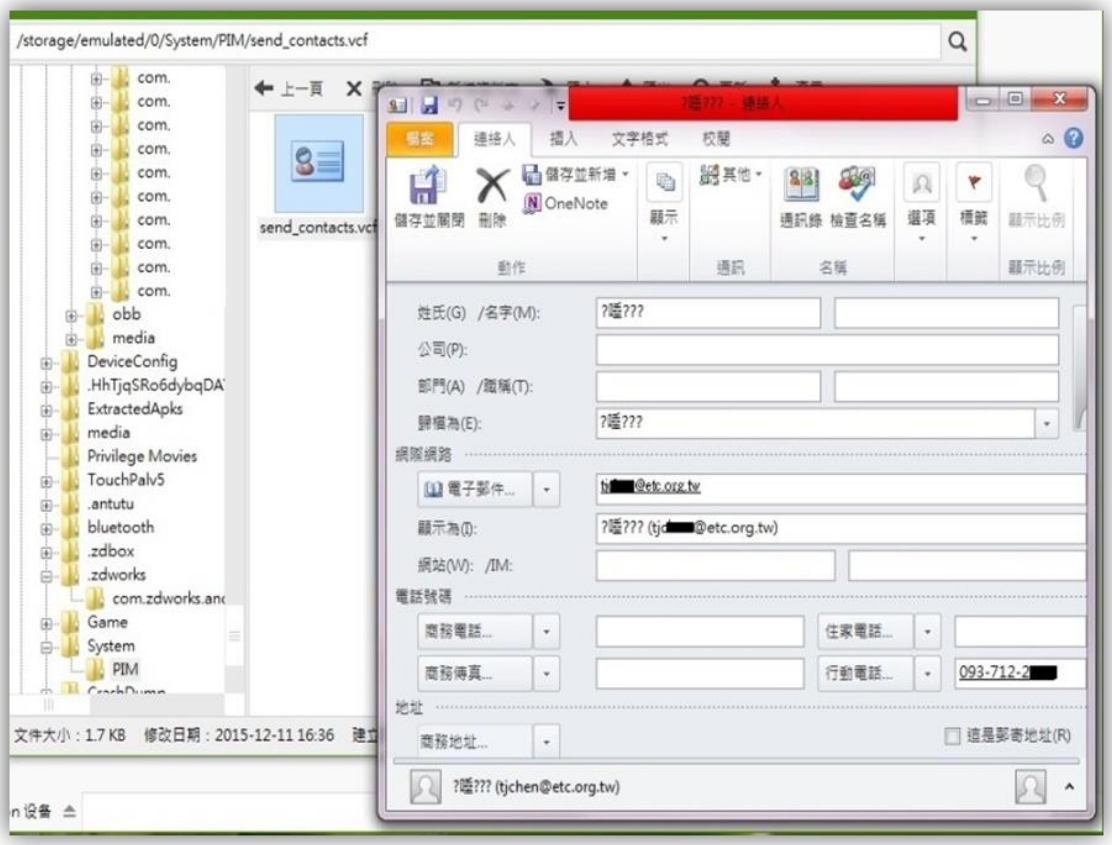
(2)各手機檢測結果與討論

該測項之測試結果統計如表 6,在 6 款測試樣機中有 5 款手機符合測試要求，1 款不符合測試要求。

表6　測項 D.2.1.B 之測試結果

各手機之測試結果	
符合	5
不符合	1

該款手機乃因發現有 E-mail 帳號以明文方式儲存於非作業系統保護區，故不符合檢測要求，詳見資料來源：。



資料來源：本計畫彙整

圖5　E-mail 帳號以明文方式儲存於非作業系統保護區圖示

2.資料儲存保護之比較(檢測細項：D.2.2.M(+))

(1)檢測說明與分析

於資料儲存部分，在檢測細項 D.2.2.M(+)，要求手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。

該測項之重點在於檢測申請者需提供管理者權限之手機才能測試。且其內建軟體之檢測條件須滿足

- 受測軟體具備儲存敏感性資料的功能
- 資料型別：第 1 型資料(不包含相片)

- 受測軟體屬性：出廠預載、銷售商加載

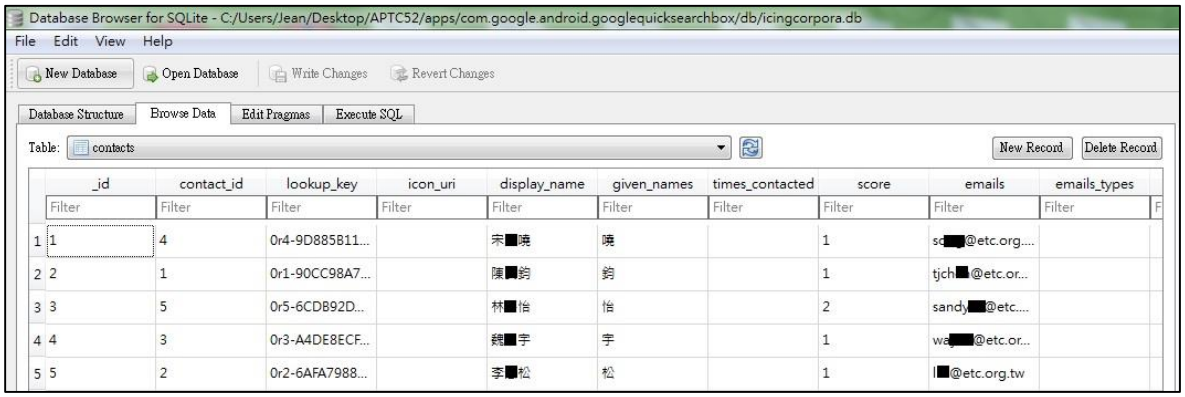
以管理者權限身分，並搭配資料讀取工具，檢查受測軟體是否以明文方式儲存敏感性資料，若檢測之受測軟體均無發現有敏感性資料以明文方式儲存與手機內則符合測試，反之則不符合測試。

(2)各手機檢測結果與討論

該測項之測試結果統計如表 7，在 6 款測試樣機中，因其中有 2 款手機無法獲得管理者權限，故無法確實執行該測項，另外 4 款手機則均有發現敏感性資料以明文方式儲存於手機內，如資料來源：，故不符合測試要求。

表7　測項 D.2.2.M(+)之測試結果

各手機之測試結果	
NA	2
不符合	4



資料來源：本計畫彙整

圖6　敏感性資料以明文方式儲存於手機內

3.程式執行安全之比較(檢測細項 A.4.3.M)

(1)檢測說明與分析

於程式執行安全部分，在檢測細項 A.4.3.M，要求手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。

該測項之重點在於首先其內建軟體之檢測條件須滿足：

- 受測軟體可接收延伸標記語言
- 資料型別：無
- 受測軟體屬性：出廠預載、銷售商加載

透過網路工具監聽並攔截網路封包，當有發現具延伸標記語言(XML)之封包則，注入攻擊字串並傳送至受測軟體，去看軟體會如何反應，若受測軟體執行注入之攻擊字串則不符合檢測要求，反之則符合檢測要求。

(2)各手機檢測結果與討論

在該測項，非全部手機均有發現具延伸標記語言(XML)封包，且注入之攻擊字串也未必都能成功，故測試結果統計如表 8，6 款測試樣機中，有 3 款符合檢測要求，3 款不符合檢測要求。

表8　測項 A.4.3.M 之測試結果

各手機之測試結果	
符合	3
不符合	3

3 款不符合檢測要求之手機乃因發現可成功竄改封包內之圖

檔連結，若置入之圖檔有植入木馬，則手機使用者將可能因點擊了具木馬圖檔而有資安之疑慮，故不符合該測項要求，詳細攻擊成功之畫面詳如圖 7。

資料來源：本計畫彙整

圖7　延伸標記語言攻擊成功圖示

4.協定傳輸保護之敏感性資料加密傳輸保護比較(檢測細項 P.2.1.B)

(1)檢測說明與分析

於敏感性資料加密傳輸保護部分，在檢測細項 P.2.1.B，要求手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。

該測項之重點在於首先其內建軟體之檢測條件須滿足：

- 無線傳輸技術：藍牙、WLAN 及行動通訊網路
- 資料型別：第 1 型資料(不包含相片)及定位資訊
- 受測軟體屬性：出廠預載、銷售商加載

透過網路封包監聽之工具，查看傳輸之封包內容是否出現敏感性資料以明文方式傳輸，若有則不符合該項檢測要求，反之則符合檢測要求。

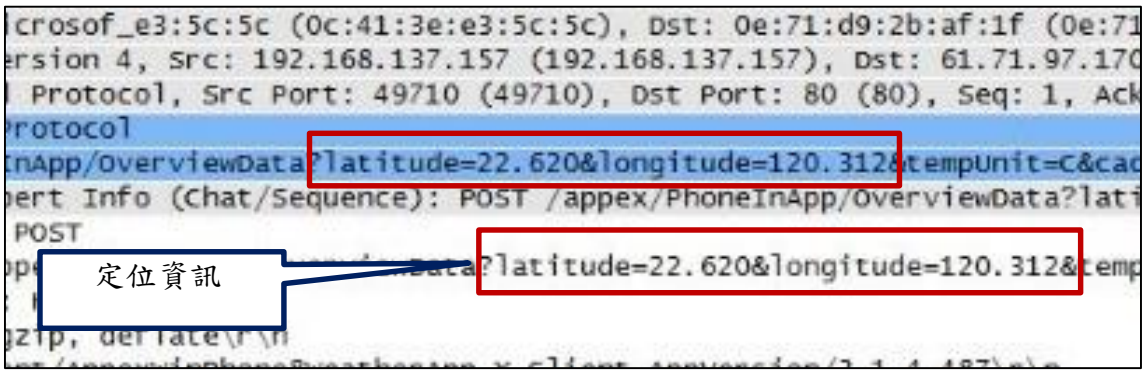
(2)各手機檢測結果與討論

在該測項之測試結果統計如表 9，6 款測試樣機中，有 5 款符合檢測要求，1 款不符合檢測要求。

表9　測項 P.2.1.B 之測試結果

各手機之測試結果	
符合	5
不符合	1

未通過測試之手機乃因發現定位資訊以明文方式傳輸，故不符合該測項之檢測要求，詳細結果請見圖 8。



資料來源：本計畫彙整

圖8　定位資訊明文傳輸

5.協定傳輸保護之安全加密演算法比較(檢測細項 P.2.3.M)

(1)檢測說明與分析

於安全加密演算法部分，在檢測細項 P.2.3.M，要求手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。

該測項之重點在於首先其內建軟體之檢測條件須滿足：

- 伺服器類型：付費功能的主機
- 申請者須提供書面資料作為審查依據
- 必要時，檢測實驗室得請申請者進行功能示範
- 資料型別：無
- 受測軟體屬性：出廠預載、銷售商加載

透過網路監控封包之工具，查看內建軟體與伺服器間加密傳輸之加密演算法是否為 FIPS 140 核准之加密演算法，若是則符合該檢測要求，反之則不符合該檢測要求。

(2)各手機檢測結果與討論

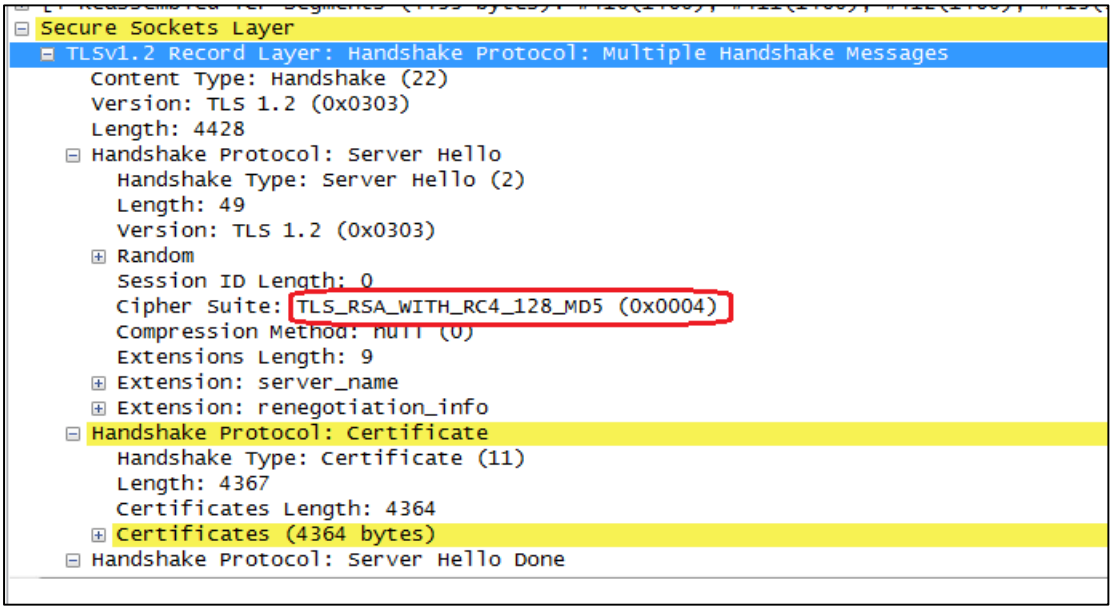
在該測項之測試結果統計如表 10，5 款測試樣機均符合測試。

表10　測項 P.2.4.M 之測試結果

各手機之測試結果	
符合	5
NA	1

該測項中，其中 1 款手機發現到採用的加密演算法為

“TLS_RSA_WITH_RC4_128_MD5”，其中採用 MD5 為其雜湊演算法，MD5 在 FIPS140 中為非核准之雜湊演算法，在 OWASP 中 MD5 亦被認定為弱的雜湊演算法，但因該伺服器需廠商協助確認是否為具付費功能的主機，因此判為 NA。



資料來源： 本計畫彙整

圖9　加密協定與加密演算法

6.協定執行安全之錯誤處理能力比較(檢測細項 P.3.1.M)

(1)檢測說明與分析

於通訊協定錯誤處理能力部分，在檢測細項 P.3.1.M，要求手機系統內建軟體應具通訊協定內容的錯誤處理能力。

該測項之重點在於首先其內建軟體之檢測條件須滿足：

- 受測軟體具開啟 WLAN/藍牙介面

並使用 WLAN 與藍芽之模糊測試工具(Fuzz Testing tool)進行測試，若測試過程中手機系統發生無法正常運作，則該測項不符合檢測要求，反之則符合檢測要求。

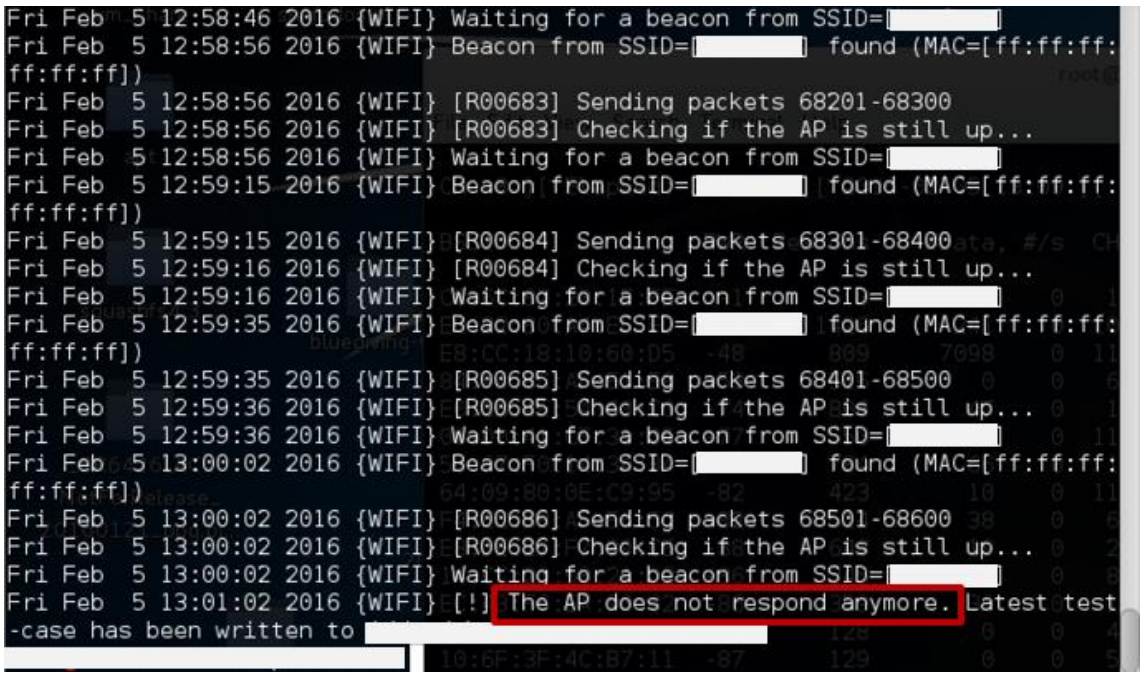
(2)各手機檢測結果與討論

在該測項之測試結果統計如表 11，6 款測試樣機中，4 款符合檢測要求，2 款不符合檢測要求。

表11　測項 P.3.1.M 之測試結果

各手機之測試結果	
符合	4
不符合	2

測項中發現有其中 2 款手機於 WLAN 的檢測部分，因測試過程中，手機系統發生無法正常運作現象，如 0，測試樣機出現系統無回應現象，故判定為不符合檢測要求。



資料來源：本計畫彙整

圖10　手機系統無回應

7.系統身分辨識之密碼設定複雜度比較(檢測細項 O.2.3.B)

(1)檢測說明與分析

於密碼設定複雜度部分，在檢測細項 O.2.3.B，要求手機系統應提供至少 72 種密碼輸入值，包含英文大寫、英文小寫、數字及特殊符號等，且密碼長度應可達 14 碼以上。

該測項之重點在於首先其手機系統之檢測條件須滿足具密碼設定功能，接著在可輸入密碼設定之介面上嘗試各種可能的輸入值，可輸入的值需達 72 種以上，另外還須支援密碼長度 14 碼以上才算符合該測項之檢測要求。

(2)各手機檢測結果與討論

在該測項之測試結果統計如表 12，6 款測試樣機中，4 款符合檢測要求，2 款不符合檢測要求。

表12　測項 O.2.3.B 之測試結果

各手機之測試結果	
符合	4
不符合	2

不符合測試之手機，其中，1 款因密碼設定僅具數字輸入而無其他英文或符號等可能之輸入組合，也就是僅能輸入 10 種輸入值，未達 72 種以上可能之輸入值，故不符合該測項之檢測要求；另 1 款則因僅提供數字與英文字母做為密碼的值，也僅達 62 種輸入值，亦未達 72 種以上可能之輸入值。

參、綜合檢討與建議

本次技術規範草案相關檢測項目之測試執行，在測試過程中發現不少狀況而導致部分測項無法順利判斷其結果是否符合或不符合該測項之檢測要求，其主要原因有二：

一、送測之手機未具備管理者權限

送測手機數量多為 1~2 支，且未開啟管理者權限，因此部分中級檢測細項，因無管理者權限而無法確認該測項之要求是否符合。

二、廠商自我宣告表資訊不足

本計畫執行期間，由於本次檢測屬試測狀態，故各家手機原廠僅提供樣機，僅有 1 家手機業者配合繳交自我宣告表，且繳交之自我宣告表內容亦有部分資訊填寫不完全，導致部分測項無法確認是否符合檢測要求。

因此，建議未來實際執行本規範之測試時，送測單位須得配合繳交完整廠商自我宣告表；並提供 2 支以上同款樣機，若送測安全等級中級以上者，應於其中 1 支樣機中開立管理者權限，如此才能完整執行所有測項，以利檢測規範與安全等級判定。

附件 6 座談會會議紀錄、簽到表及研析意見

國家通訊傳播委員會

104 年度「手機系統內建軟體資安檢測」計畫

第一場學者專家座談會會議紀錄

一、會議名稱：國際智慧型手機行動裝置資通安全檢測發展現況及各國規範探討座談會

二、時間：104 年 8 月 18 日(星期二) 下午 3 時 30 分

三、地點：台大醫院國際會議中心 401 會議室（台北市徐州路 2 號）

四、議程：

時間	議題	主講人
15:10~15:30	報到	
15:30~15:40	開場致詞	
15:40~16:00	手機安全檢測國際發展現況分析	財團法人電信技術中心 蔡志明組長
16:00~16:15	NCC 手機系統內建規範研擬方向	安華聯網科技(股)公司 洪光鈞總經理
16:15~16:50	綜合討論&意見交流互動	

五、主席：中華民國資訊軟體協會 喻維貞 副秘書長

記錄：姚人鳳

六、座談議題：

(一)就政府機關而言，對使用手機處理公務的政策為何？對手機資料傳輸、使用權限、網路存取上，機關目前最在意的問題是什麼？於資安部分考量面向有哪些？

(二)目前手機檢測部分皆屬上市前型式認證，對檢測實驗室而言執行上較困難的地方為何？

(三)智慧型手機已是現代人生活常備物品，然而手機內儲存許多個人資料

與檔案，新聞媒體也常報導 Apps 涉及洩漏個人隱私資料，是否可提供手機端與 App 端一些資安技術面與使用面的建議？

七、座談會討論內容(依發言先後排序)：

(一)行政院資訊處 洪高級分析師

1.iphone 每個版本的安全該怎麼分？如果很久的 Android 版本該怎麼去檢測？檢測部分應須考量作業系統版本問題。

2.大陸的 APP(QQ 和百度)這樣的 APP 國際上是安全，但國內算安全嗎？這該怎麼去評估？

3.手機的安全預設值應該做個規範，例如定位功能，預設時是否就應該是關掉之類的規範？

(二)工業局 曾技正

1.請 NCC 考量 APP 檢測應訂為強制性規範或自主管理。

2.經濟部工業局目前也正在進行「行動 APP 安全認證」，將訂立 APP Store 上架前之 APP 檢測標準，並且由經濟部標準檢驗局(TAF)訂立 APP 檢測實驗室資格標準，該標準將以 ISO17025 為基準，未來一般檢測實驗室可依循該資格標準申請行動 APP 安全認證檢測實驗室，將檢測作業向下延伸至一般檢測實驗室，創造民間自主管理環境。但在此之前，示範期間之檢測則委託資策會進行。

3.檢測實驗室具備之能力依民眾使用的方式區分初級、中級及高級，初級為民眾下載僅在單機使用之 APP 的檢測；中級為下載的 APP 之資料儲存有涉及到雲端傳輸層面之檢測；高級為民眾下載之 APP 涉及到行動支付與金流傳輸之檢測，目前資策會檢測環境已將完成初級部分，年底前則將進行中級與高級部分。

4.NCC 之手機系統內建軟體資安檢測規範推動，可與工業局相互討論，將手機安全建立更加完善，為消費者、檢測業者、軟體開發商創造最大獲利。

(三)經濟部技術處新世代通訊技術推進辦公室 許資深技術經理

1.台灣資通標準協會於 7 月成立，著手參與網路資訊安全、檢測認證機構相關業務，建議 NCC 草擬之規範可與該協會相互交流，未來將規範推動至國際，與國際標準接軌。

(四)香港商立德國際商品試驗有限公司 蕭協理

1.針對大陸白牌手機的檢測及白牌手機所提供之報告完整性是否能符合 NCC 要求，皆需考量至規範訂立中。
2.白牌手機的代理商該如何確認產品規格(因白牌手機商在台灣沒有研發或資通安全軟體人員)，檢測實驗室又該如何確定白牌手機規格符合需求，這是未來與 NCC 規範制訂須討論的問題點。

(五)交大網路測試中心 許執行主任

1.政府對此規範的強制性將為重要議題，建議 NCC 如果能將此項規範強制性應有助行動裝置安全環境。
2.測試的時程與測試內容深度一定會需要權衡，建議可先確認容忍的測試時程為何？進而決定測試深度該到多深。
3.關於個人資訊外洩的問題是否會進行檢測？如果有那又會在哪裡又該如何檢測？
4.檢測內容有分等級，對於送測高等級的廠商有何益處？ ex: 政府或公務機關採購可以規定一定要採購等級多高以上的？
5.關於 App 或手機權限等自我宣告的內容建議應該也要檢測。
6.使用者同意相關宣告之後才可以使用，但是如何檢測確認真的要使用者同意之後才取得相關權限？
7.預設的設定等內容應該可以強制化，ex: GPS 預設應該為關閉，所以建議可以定一個範圍輪廓提供政府機關或民眾參考，甚至是強制預設設定規範標準。

(六)財團法人資訊工業策進會 陳組長

1.建議可透過檢測說明書將檢測要求列為強制性，例如檢測實驗室訂立一套類似安全需求/要求，該需求說明 APP 安全保護方式(如定位功能保護方式說明)，另手機商則提供安全性說明，而實驗室則可針對安全性說明來判斷手機商是否有符合安全性說明，此可達到強制性需求，又符合國際作法，因國外在推動安全規範是以「讓評估者(如通訊商)可依據檢測報告作為是否採購之關鍵因素」為主。

(七)趨勢科技全球核心技術部門 蔡資深協理

1.目前手機功能已趨近於電腦，因此估計過去與現在於電腦上存在的病毒未來勢必會發生在手機上，而手機上有更多個人隱私資料，因此對於安全問題更加嚴重。
2.對於手機安全最重要的防禦方法不外乎為：「不要下載及安裝不明 APP」及「不要使用太簡單的密碼，盡量使用雙重認證方式保護帳號」。

(八)台灣威瑞特系統科技股份有限公司 鄭技術經理

1.手機五個層次的安全評分標準需要嚴謹訂立，對於 OS 層的問題提出一個假設，如果今天發現某支手機的 OS 層出現資安問題，是否判別該手機為不合格手機，那以 Android 而言，是否所有的 Android 手機皆不安全？還是等到 OS 廠商修復完成再進行手機檢測？
2.對於手機安全問題，目前各大資安廠商皆已做的相當完善，然而資安風險最重要還是「消費者使用習慣」。

(九)台灣檢驗科技股份有限公司 陳技術經理

1.對檢測實驗時而言，取得原始碼、足夠的裝置存取權限及沙盒的建置是在檢測執行上比較常遇到的困難點。
2.以下是給檢測規範的一些檢測要點建議：

(1) 檢視軟體是否未進行內容編碼，就直接將資料傳輸到網路瀏覽器，避免 XSS 問題。

(2) 帳密不得採明文儲存，以避免傳輸層保護不足問題。

(3) 避免直接使用 SQL Injection，避免攻擊者透過欺騙 interpreter 執行指令或竄改資料。

(4) 檢視程式碼是否包含不安全的遠端資料存取。

(5) Trace 資料內容是否傳輸資訊至第三方。

(6) Debug Log 出廠時必須關閉及伺服器端必須進行弱點掃描以避免洩露使用者帳密。

(7) 軟體應避免使用直覺的命名方式來定義 file、folder、或 database record 及 key 作為 URL 或是 Form 的參數。攻擊者可藉由操作這些 references 進入其他 objects。

(8) 檢視軟體是否強迫 browser 傳輸 pre-authenticated request，以 browser 執行對攻擊者有好處的行為。

(9) 軟體撰寫不得採用 Get 方式傳輸，或直接將帳密透過 URL 網址傳遞。

(10) Cache 是否有適當的保護措施 multi-task 下 Background Screenshot 可能造成資料洩露。

八、與會者討論

(一)與會者提問：

1.手機內建的軟體資安認證以後會是強制性的嗎？

2.對於目前「行動 APP 安全認證」之計畫中，對於檢測實驗室目前進行狀況，是否有具體時程和規劃，可讓 TAF 有準備進行檢測實驗室認證受理作業？

3.TAF 認證的角色是否與工業局目前自主檢測推動制度角色是一樣的？

(二)與談者回覆：

1.中華民國資訊軟體協會 喻副祕書長

(1) 目前是自主性與鼓勵性為主，未來可建議 NCC 強制規定。

2.工業局 曾技正

(1) 由於工業局所訂之規範不僅是針對國內 APP 開發業商，而國內的 APP 開發商相較於國外則屬較不利的地位，因此目前行動 APP 安全認證之推動是以輔導來替代強制立法規範。

(2) 目前已將認證能力之需求已擬訂完成，目前有 8 家檢測業者配合工業局進行示範性檢測，希望 TAF 能一年內訂立完成檢測實驗室規定，讓檢測實驗室能進行認證申請。

九、會議決議

(一)安全等級規劃應以使用者角度為出發點，以使用者隱私相關的資料安全為主，確保所有資料在各狀態下可被安全使用。

(二)規範撰擬須與國際規範標準一致，將參考 OWASP Mobile Security Project、NIST 800-164.163 及 ITU-T YD 2407-2013.2408-2013。

(三)資料型別以是否屬於敏感性資料，以及是否為使用者輸入作為判定標準，將資料區分 4 種型態。

(四)自我宣告屬於本規範之書審重點，未來期望透過公開廠商自我宣告表及實驗室檢測結果，讓民眾可上網審視手機權限要求是否與廠商自行聲明相符與妥適性。

國家通訊傳播委員會

104 年度「手機系統內建軟體資安檢測」計畫

第二場學者專家座談會會議紀錄

時間：中華民國 104 年 09 月 18 日(星期五) 14:00~17:00
地點：中華民國資訊軟體協會 (台北市承德路二段 239 號 6 樓)
主席：計畫主持人 中華民國資訊軟體協會喻維貞副秘書長
出席代表：

國家通訊傳播委員會蘇勇吉科長
國家通訊傳播委員會李福懿技正
經濟部工業局曾技正
經濟部標準檢驗局林科長
行政院消費者保護處王消保官
行政院資通安全辦公室(技術服務中心) 陳組長
台灣三星電子股份有限公司洪總監
台灣三星電子股份有限公司高經理
台灣三星電子股份有限公司葉資深專員
宏達國際電子股份有限公司陳副總經理
宏達國際電子股份有限公司巫經理
台灣威瑞特系統科技股份有限公司吳總經理
香港商立德國際商品試驗有限公司蕭經理
台灣檢驗科技股份有限公司張經理

研究團隊出席代表(詳見簽到表)：

中華民國資訊軟體協會楊蕙如組長
安華聯網科技股份有限公司洪光鈞總經理
安華聯網科技股份有限公司林昱廷專案經理
安華聯網科技股份有限公司林維展工程師
安華聯網科技股份有限公司陳漢平工程師
財團法人台灣電子檢驗中心宋孟曉經理
財團法人台灣電子檢驗中心葉錫勳工程師

記錄：中華民國資訊軟體協會姚人鳳專員

壹、 會議議程：

13：45 - 14：00	報到
14：00 - 14：30	「我國智慧型手機系統內建軟體資通安全檢測技術規範草案」說明
14：30 - 16：00	規範草案意見交流
16：00 - 16：15	「第三方檢測實驗室認可規定訂草案」說明
16：15 - 17：00	檢測實驗室修訂草案意見交流
17：00	散會

貳、 會議決議：

1. 規範分級應以使用者角度重新劃分與定義，並以一般民眾容易理解之論述重新定義。

參、 意見交流

一、 規範討論：

Q1. P 9 建議補充層級、等級說明之關係圖(可套用 PPT 內容)。

A1. 謝謝先進意見，團隊將後續修改。

Q2. P 7 請明確定義何謂「內建軟體」，如一個有圖示的 APP 即稱為內建軟體，或未呈現成圖示的 service 即可稱之？

A2. 內建軟體應包含以下三種屬性:

(1)出廠預載程式：智慧型手機出廠時預設搭載安裝之應用程式，且使用者可透過圖示啟動。

(2)銷售商加載程式：智慧型手機銷售時預設搭載或首次以行動網路上網後自動安裝之應用程式，且使用者可透過圖示啟動。

(3)無圖示程式/程序：於上述兩種情況所安裝之應用程式/程序，手機開啟後即預設為啟動狀態，且將資料回傳至後端伺服器。

Q3. P61 請明確定義何謂「可信任來源」;p64 檢測項目 9.4.1.6.2 檢測方法提到「是否在適當期間」，亦請定義期間範圍。

A3. (1)可信任來源：廠商於系統內建軟體說明書宣告之 IP、網域名稱或網址，將在文件中增加定義說明
(2)已於新版中移除該檢測項目。

Q4. P65 技術要求中提到「應在說明書中明示使用者當不能保證內建軟體安全的更新帶來的安全風險」等描述，不夠明確，請再調整。

A4. 已刪除該檢測項目。

Q5. 安全等級的標準須和國際主要國家的資安標準方向一致，避免各主要品牌手機未來在各國間差異太大。

A5. 本規範主要參考 OWASP Mobile Security Project、NIST800-164.163 及 ITU-T YDT2407-2013. 2048-2013，應能符合各國間之規範要求，並於檢測規範文件中附上與國際間對應關係表。

Q6. 對於手機測試需要多少時間?

A6. 以去年底檢測經驗，一支手機約 30 個人天工時，目前規劃估計 L1 之檢測時間控制於 2 週內可完成，也因此 L1 設計概念是檢測時間短、成本低、以不造成手機商與檢測實驗室負擔為考量，而確切檢測工時將於規範完成後，試測時進行評估。

Q7. 對於去年 12 款手機的檢測是否皆有符合今日的標準?

A7. 去年檢測範圍主要是參考中國大陸規範，針對網路行為、資料儲存及敏感性資料權限為主，今年的檢測項目皆有涵蓋當初內容，並且更完整。

Q8. 目前規範只有程序沒有標準，如果有爭議時該如何處理，因每家公司有自己的設計邏輯與概念，若檢測判別為不符合該如何解決?

A8. 規範設計上一定有判定標準，但程序與方法較難有強制

統一做法，但會將檢測要求清楚定義，以達成檢測實驗室認知共識。

Q9. P29「磁區檢測工具」無明確定義，容易造成爭議，若在不限定品牌的原則上，建議須註記「如什麼工具」之描述。

A9. 由於規範若標示工具名稱將造成品牌限定問題，後續會調整規範內容，並考量跨平台間之問題明確定義。

Q10. 規範中將作業系統層定義為拍照、錄音等，是否與 APP 層有所混淆，請再區分清楚。

A10. 拍照、錄音等將於應用程式層檢測項目做調整。

Q11. 是否有個參考基準可判斷等級區分是否合適，如市面上手機哪些是已符合 L1。

A11. 市面上手機可通過多少的檢測項將後續會由 ETC 協助後測並整理，就現階段而言，尚無法進行全面性普查。

Q12. 內建軟體功能說明書內容過細，容易造成手機商的送測時間上的負擔，或完整性不全造成來回退/送件的時間成本過高，影響檢測時間，若說明書內容對檢測實驗室幫助不大，建議簡化書審流程，直接由檢測實驗室判斷可減少時間成本問題。

A12. 內建軟體說明書的填寫項目與深度會再進行調整，並考量簡化書審流程。

二、 規範等級(Level)討論：

Q1. 等級分類目的須釐清，建議以使用者為區分標準，例如針對消費者、企業、政府的資安需求程度進行區分。

A1. 將依會議共識以使用者角度進行調整。

Q2. 分級的說明對於民眾較難理解，建議改為民眾容易理解之描述。

A2. 等級名稱與說明將以民眾容易理解之論述重新定義。

Q3. 層級區分應該是五層皆有 L1~L5，建議可用橫縱表格呈現。

A3. 目前規劃是手機五層對應五個 Level，層級越淺如資料層，則對應 L1，越深如硬體層，則對應 L5，但後續則考慮以使用者角度重新劃分，並以表格或圖示明確呈現。

Q4. Level 問卷第 4 點「功能式提示(具連網行為)」，因 LEVEL1 目前規劃是屬半強制型，應以民眾角度考量網路行為；第 5 點「提供不同意的選項設定(具連網行為) 」與敏感性資料有關；第 12 點「付費功能安全提示」屬於隱私權原則之同意與選擇權原則；第 14 點「聯網行為安全性功能」與民眾安全性相關；第 17 點「提供資料備份機制」與民眾安全性相關；第 18 點「提供安全回報機制」；第 21 點「作業系統安全機制」，一般手機出廠時皆會考量還原機制，應符合隱私權原則之公開透明原則，故上述皆建議改為 L1。

A4. 將依本次會議共識，以使用者角度進行調整。

三、 檢測實驗室討論：

Q1. 檢測實驗室有提到 ISO 15408，手機是否會需要參考到。

A1. 此為原先資通安全檢測實驗室之規定，非在此次手機範圍內。

Q2. P3 行動裝置安全檢測實驗室的要求，檢測智慧型手機實際經驗是否等同檢測 APP?如否，差異性為何?目前草案似乎以 APP 為檢測標的，建議用字放寬，加上內建軟體。

A2. 目前草案之檢測標的為完整智慧型手機；執行實績之要求將改為檢測智慧型手機相關資安實務經驗，須具備檢測報告備查。

Q3. 為何資通設備是要求技術主管，而行動裝置是要求實驗室

主管?

A3. 在 ISO 17025 中為實驗室主管。

Q4. 目前全球無針對手機的檢測實驗室認可標準，未來台灣的實驗室能力是否得到國際認可須考量。

A4. 本規範參考目前主流國際標準與規範來訂定之，盡量相容於國際規範的趨勢，如果未來國際有相關手機檢測實驗室認可標準，可另行考量對應內容調整之。

Q5. 檢測實驗室在申請資格時，需要兩種皆有具備才能申請還是分開申請，若分開表示方式請明確。

A5. 檢測實驗室的資格申請是資通設備安全與手機安全分開申請，後續會再調整呈現方式更加明確。

Q6. 在實驗室的資格僅限制人員條件，測試能力上不限制條件嗎?

A6. 由於設備上的條件規定容易造成品牌限定，因此手機檢測實驗室的限制目前僅針對人員資格。

Q7. 證書應該要資通安全及手機分開設計。

A7. 將另外設計手機的實驗室認可證書。

Q8. 簡報上敘述後端檢測實驗室待 NCC 核發認可證書，應是 TAF 核發，NCC 應是轉發認可證書。

A8. 主管機關有權利可採「認可實驗室」的方式，或「採納 TAF 認證的實驗室」方式，若用認可方式，可發認可證書或用函覆方式發認可證明，將以 NCC 再行決定。

Q9. 為什麼要訂立 ISO 17025，ISO 9001 不行？

A9. ISO9001 主要針對管理系統，注重管理系統的適合性、充分性、有效性；ISO17025 針對實驗室規定，注重實驗室的準確性與經密性，因此檢測實驗室主要通過 ISO17025，而國際上檢測實驗室亦要求須通過

ISO17025，考慮規範與國際接軌，因此規定須通過 ISO17025 資格。

FIPS140-2 檢測實驗室由 NVLAP(National Voluntary Laboratory Accreditation Program)規範，其基本要求包含 ISO17025 等。

Q10. 若有考量 ISO17025 規定不夠詳細，建議改訂立方法為：區分兩條規定，1.須通過 ISO 17025，2.建議在什麼狀況下(如 ISO17025 某條文不夠完全)則再可參考 ISO 9001 的哪個條文之類說明。

A10. 謝謝先進意見，團隊將納入修改方法參考。

Q11. 流程上有些要改，NCC 法規訂立完成後，TAF 須接受 NCC 法規，檢測實驗室直接與 TAF 申請，TAF 再邀請 NCC 專家或外部專家一同資格審查，核可後 TAF 納入特殊服務計畫項目，NCC 可再認可 TAF 之審核，發給實驗室認可證書。

A11. 謝謝先進之建議，團隊將進行後續修改。

Q12. 實驗室主管要求資安相關經驗三年以上實屬嚴苛，建議不限定資安領域之經驗或刪除此條，而報告簽署人可維持。

A12. 實驗室主管之資格訂立，團隊擬從寬規範。

Q13. 因 CEH、CISSP 等證照提到手機層面占少部分，因此建議應以其他資安證照作為門檻要求。

A13. 將會進行增加與調整。

Q14. 實機測試要求三年內有兩件以上的檢測經驗，該經驗是什麼應該要說明或規定。

A14. 將再納入實驗室客觀條件，以利相關資格要求。

四、 政策面討論：

Q1. NCC 是否有強制要求等級?要求等級有怎麼樣的規定?

A1. 未來 NCC 會在官網上公告送測通過之手機牌子與等級供民眾參考，主管機關不會強制規定業者要通過多少等級，但希望用軟性方式促進民眾買更安全手機、刺激業者主動檢測。

Q2. 要求取得該規範認證之時間性規劃?(如上架後要取得或一個月前等),並須考量手機商直接上市之手機檢測時程。

A2. 未來 NCC 規劃與通訊業者協商，將綁約手機與上市手機之間的時間空檔訂立檢測時間上的要求。

Q3. 手機更新後對於手機商是否需要再進行一次檢測？

A3. 目前規劃一開始檢測會核發認證標章，若更新後再進行一次檢測，並另再發一次標章，而市面上流通版本與送測版本是否相同，則可由 NCC 以抽測方式檢驗，以上建議還需與 NCC 討論。

Q4. 未來檢測會是強制性嗎?預計什麼時候會實施?

A4. 將以專案完成時程考量，完成後將盡快實施，而目前是屬於自願性受測，不強制要求，但規劃從電信業推動。

Q5. 通過檢測手機會公告在哪?貿易 e 網還是 NCC 網站?

A5. 貿易 e 網亦屬 NCC 持有，後續會考慮為公告網站。

Q6. 標章建議盡量簡易，兩個版本即可，如 full testing 或 patial testing 而更新則不要再用一個標章。

A6. 目前規畫是 2 個標章，如 full testing 或 incremental 之類，主要會在標章編碼原則上明確標示通過 Level 或版本等。

Q7. 對於該手機測試規範 NCC 的期望是?

A7. 對於此規範的期望，希望民眾在使用手機時能更加保障使用安全性，並且依照安全需求選擇合適手機。

Q8. 目前手機 APP 規範很多，工業局和本規範一樣皆有等級之分，而眾多規範間是否要有編號，能否跟國際接軌?是否各自獨立?

A8. 工業局規範是只針對應用程式層(APPs)，本規範亦有納入參考，兩規範於應用程式層與資料層是可互通，與國際上規範相比，針對中國大陸規範而言也是本規範的參考之一，因此通過台灣的規範於國際上應該能符合大部分安全要求。

Q9. 資安規範是否是一個標準?

A9. 本規範實為 NCC 所公布之標準，可由行政機關認定是否為國家標準，並如需成為正式國家標準則建議於施行一段時間後由 NCC 進一步申請成為國家標準。

五、 文件格式建議：

Q1. 草案「五層級」皆改成「五層」；p9「欄位定義與分類表格如下」改成「用語定義如下」；檢測類別中的「敏感性資料的使用」改成「敏感性資料的蒐集使用」；「刪除」改成「刪除傳輸」；「檢測項目」改成「檢測內容」；「檢測目的」改成「檢測安全需求與期望」。

A1. 謝謝先進意見，團隊將後續修改。

Q2. P20 第 9 點，「第 1 類」改成「第 1 型」以此類推；「類別」改成「型別」。

A2. 謝謝先進意見，團隊將後續修改。

Q3. P20 第 9 點，「第 1 類」改成「第 1 型」以此類推；「類別」改成「型別」；第 1 類的資料內容中「包含但不限於」移置「通訊錄」前。

A3. 謝謝先進意見，團隊將後續修改。

Q4. P70「類型」改成「型別」，「第一類」改成「第一型」

以此類推。

A4. 謝謝先進意見，團隊將後續修改。

Q5. P11「敏感性資料修改」後面加上「或刪除」。

A5. 謝謝先進意見，團隊將後續修改。

Q6. P21 判斷標準用與要統一，如：是否、不可、有沒有等請統一。

A6. 謝謝先進意見，團隊將後續修改。

Q7. P45「protocal」拼錯請改為「protocol」。

A7. 謝謝先進意見，團隊將後續修改。

Q8. P21 起表格皆建議再加一個欄位標記是屬於哪一型資料。

A8. 謝謝先進意見，團隊將後續修改。

Q9. 手持式行動台、智慧型手機、行動裝置，應該要統一名詞。

A9. 謝謝先進意見，團隊將後續修改。

Q10. 檢測實驗室標題要改為：資通設備及智慧型手持行動台之資通安全實驗室管理要點。

A10. 謝謝先進意見，團隊將後續修改。

Q11. 檢測實驗室第一條建議寫法源，例如引用 NCC 組織法，而目前第一條內容從「包含」起則改為第二條，並改敘述為「檢測實驗室包含」，最後「特訂定本要點」前移至「執行檢測實驗室認可與管理」後方。

A11. 謝謝先進意見，團隊將後續修改。

肆、 散會：下午 17 時 00 分

國家通訊傳播委員會

104 年度「手機系統內建軟體資安檢測」計畫

第三場學者專家座談會會議紀錄

時間：中華民國 104 年 10 月 2 日(星期五) 14:00~17:00
地點：中華民國資訊軟體協會 (台北市承德路二段 239 號 6 樓)
主席：計畫主持人 中華民國資訊軟體協會喻維貞副秘書長
出席代表(詳見簽到表)：

國家通訊傳播委員會蘇勇吉科長
國家通訊傳播委員會李福懿技正
經濟部工業局曾技正
經濟部標準檢驗局林科長
行政院資通安全辦公室(技術服務中心)陳組長
國家發展委員會資管處楊科長
宏達國際電子股份有限公司巫經理
台灣威瑞特系統科技股份有限公司吳總經理
台灣國際商業機器股份有限公司曾技術顧問
香港商立德國際商品試驗有限公司蕭經理
台灣檢驗科技股份有限公司陳技術經理

研究團隊出席代表(詳見簽到表)：

睿明知通股份有限公司鍾榮翰協同計畫主持人
中華民國資訊軟體協會楊蕙如組長
安華聯網科技股份有限公司洪光鈞總經理
安華聯網科技股份有限公司林昱廷專案經理
安華聯網科技股份有限公司林維展工程師
安華聯網科技股份有限公司陳漢平工程師
財團法人台灣電子檢驗中心宋孟曉經理
財團法人台灣電子檢驗中心葉錫勳工程師
財團法人電信技術中心許任銘資深工程師

記錄：中華民國資訊軟體協會姚人鳳專員

壹、 會議議程：

13：45 - 14：00	報到
14：00 - 14：30	「我國智慧型手機系統內建軟體資通安全檢測技術規範草案」與「規範安全等級」說明
14：30 - 16：00	意見交流
16：00 - 16：15	「第三方檢測實驗室認可規定修訂草案」說明
16：15 - 17：00	意見交流
17：00	散會

貳、 會議結果：

1. 安全等級請以消費者容易理解之說明再次調整，並明顯區隔 5 等級之差異。
2. 檢測實驗室要點可用章節完全區分「資通設備安全檢測實驗室」與「智慧型手持行動臺安全檢測實驗室」。
3. 檢測實驗室資格要求建議研究團隊與 TAF、檢測實驗室及 NCC 共同討論。
4. 請依今日會議討論共識，進行規範與檢測實驗室資格之修調。

參、 意見交流

一、 規範等級討論：

Q1. L2-L5 的差異性不大，Level 的名稱建議以民眾有感的用語呈現，另現行等級分類建議需有最小通過基本門檻。

A1. 研究團隊會再針對名稱以民眾容易理解角度加以調整，並且會以 L1 做為最小通過基本門檻。

Q2. 檢測上是要排在什麼時間點上。

A2. 目前是希望業者與電信商同步推動，規劃於綁約手機上市前進行檢測。

Q3. P50 附件二的資料處理欄位不清楚該如何填寫。

A3. 資料處理欄位是以個資蒐集原則作列點，將考慮另用實

際範例讓業者了解填寫方法。

Q4. 規範上應該要說明是整機測試。

A4. 將於 3.適用範圍內加以描述。

Q5. 應該要有個測試報告格式。

A5. 測試報告格式非目前計畫執行面向，計畫將於規範草擬完成後進行試測作業，該試測作業即會呈現測試報告格式，經 NCC 同意後，可於未來提供實驗室參考。

Q6. NCC 五個 LEVEL 第 3 級對消費者而言比較無感，是否不要用階級概念定義 5 級，而是由選項概念。

A6. 等級劃分研究團隊將再思索如何區隔，然而是否分 5 級或是用選項方式進行，研究團隊將與 NCC 後續討論再行定義。

Q7. 要考量檢測時間，若檢測時間太久可能會造成手機業者的反彈。

A7. 現規劃於 2 週內完成 L1 的要求。

Q8. P7 用語釋義「共同準則」建議將 EAL1~EAL7 規定列出。

A8. 研究團隊將會補上 EAL1~EAL7 之說明。

Q9. P10 的 FIPS140-2 可加註等級說明。

A9. 研究團隊將補充 FIPS140-2 等級說明。

Q10. P15 與 P25(D5.D6)手機系統內建軟體敏感性資料儲存應以密文方式儲存(1)(2)建議釐清或於需要時合併。

A10. 研究團隊將重新調整用語，避免造成誤會。

Q11. P30 A4 的技術要求建議改為「避免可透過 replay 攻擊利用交談識別碼」。

A11. 謝謝委員指導，研究團隊將調整文字用語。

Q12. P31 建議於 SSL 部份納入目前信任的核發機構 CA。

A12. 謝謝委員指導，研究團隊將於測項中補充說明。

二、 檢測實驗室討論：

Q1. 對於檢測實驗室而言，主管皆為公司老闆，工作經驗並非完全是資安業務，對於主管資格是否可再調整。

A1. 實驗室人員資格目前是依照 CNS 17025 規定訂立，然而實驗室主管部分將會與 TAF、預計申請之檢測實驗室及 NCC 加以討論。

Q2. P2 的 VoIP 建議納入 h.323

A2. 研究團隊將會納入 h.323。

Q3. 建議可將「資通設備安全」與「行動裝置安全」完全分開撰寫，以免造成規定模糊不清現象，如第七、八容易不清屬於哪個實驗室之要求。

A3. 目前暫以章節型式完全區分「資通設備安全」與「行動裝置安全」，以免造成誤會。

Q4. 資格若將證書一一列出，可能會列的不夠完善，造成 TAF 難以判斷，是否要列證書可再討論

A4. 此部分研究團隊將與 NCC 或 TAF 後續討論。

三、 文件格式建議：

1. 所有的數字請接以阿拉伯數字撰寫，包括年份、「共 5 個等級」等；等級表達請皆以「第 1 級」描述撰寫。
2. 表格文字描述若超過一句，請於最後加上「。」結尾。
3. 編碼號 5.1.請將最後的「.」捨去。
4. 文件編碼原則為 A→(A)→a→(a)；規範正式用語為點→項→款→目，編碼與用詞請統一調整。
5. 圖表名與附件名之表達請統一「表 1」中間不空格，而 1 與後方圖表名中間空一格。附件表格請皆左右置中、上下置中。

➢ 規範格式與用語建議

1. P5 表格「目的」請改為「要求」之類名詞。
2. P7 請加入 WLAN、DN 之釋義，規範本文中則可免去中文解釋。
3. P8 國際行動用戶辨識碼，請改為「識別碼」。
4. P10 的 CertificationAuthority 請於中間空一格；「Leve 4」應改為「Level 4」。
5. P11「私人密碼鑰匙」建議改用語。
6. P12 請將(1)(2)(3)內文第二行與第一行字對齊；附件與 1 中間不需空格；請刪除附件 2 後面文字「智慧型手機隱私自我宣告表(範例)」。
7. P12 建議拿掉「程序」。
8. P13「相關之文件」請刪除「之」；P13「本規範將智慧型手機」後方加上「安全」。
9. P13 自我宣告表中，申請安全等級少了第 2 級，建議與第 1 級共同說明，並且表格呈現。6.1.3 文句說明與列點說明建議精簡合併即可。
10. P14 五階層內容敘述統一以「等安全」結尾；檢測項目裡請將「研擬」改為「訂立」；請將表格內技術要求與檢測項目皆編號；p22~p46 亦於技術要求進行編號。
11. P17「手機系統內建軟體之執行」請改為「手機系統內建軟體與背景之執行」類似描述。
12. P18 作業系統層之技術要求，「受測標的系統應支援開機時設定螢幕所訂密碼等...」，建易改為「應支援開機時設定保護機制」。
13. P21 第 1 型範例「但不限於」改為「包含但不限於」；「電子郵件」請改為「電子郵件帳號、內容」。
14. P30 的 A.3 預期結果，「有提示使用者認證與授權機制」

請改為「有使用者認證與授權之提示機制」。

15. P31 遺漏 A5。
16. 聯邦資訊處理標準應為 140-2，請統一更正。
17. P47 參考文獻請刪除網址；〔2〕的 NIST 前方空一格；p48。〔10〕、〔11〕開頭請勿空格。
18. p49 第一行第六列請補上「檢附文件」。

➢ 檢測實驗室要點格式建議

1. P1 第三點，「應審查」請改為「並審查」；第三點第三款「取得本國實驗室...」請刪除「取得」；第三點第三款第 1 目(與 p5)標準簡稱請刪除，並改為「CNS 17025」與「ISO/IEC 17025」;「國際標準化組織所訂標準」改為「國際標準組織」。
2. 文章請統一名稱為「資通設備安全檢測實驗室」與「智慧型手持行動臺安全檢測實驗室」。
3. P6「前項第三點及…」刪除「前項」；第五點「另前項」請刪除；「取消認證資格」請改為「退件」。
4. P7 第七點第一款「條件」皆改為「規定」；第三款「無正當」改為「不正當」。
5. P8「等級分為第一級費用、第二級費用…第五級費用」請改為「訂立各分級費用」。
6. 附件一與附件二請皆將檢附文件第 3 條調整為一行。
7. 附件三與附件四請將「機構名稱」取消字元間距；證書號碼皆勿跨列。

肆、 散會：下午 18 時 00 分

國家通訊傳播委員會

104 年度「手機系統內建軟體資安檢測」計畫

3 場專家座談會-意見研析

一、　會議時間：

場次	日期	地點
第一場	2015/8/18(二)15:30~16:50	台大國際會議中心 401 會議室
第二場	2015/9/18(五)14:00~17:00	中華軟協大會議室
第三場	2015/10/2(五)14:00~17:00	中華軟協大會議室

二、　三場座談主要討論議題：

場次	議題
第一場	1. 目前就政府機關而言，對使用手機處理公務的政策為何？對手機資料傳輸、使用權限、網路存取上，機關目前最在意的問題是什麼？於資安部分考量的面向有哪些？ 2. 依據本計畫現階段研究了解國際間針對手機資安的制訂並無共通的檢測標準，各國的規範制定內容也不盡相同，現階段計畫主要參考規範包含 OWASP TOP10 Mobile Risk、美國 NIST SP800-163、164、DOD-DISA、NSA-IAD 及中國大陸手機檢測規範，想請教各檢測實驗室，目前手機檢測部分皆屬上市前型式認證，執行上較困難的地方為何?就手機資安檢測部分是否可提供具體執行建議？ 3. 智慧型手機已是現代人生活常備物品，然而手機內儲存許多個人資料與檔案，新聞媒體也常報導 Apps 涉及洩漏個人隱私資料，是否可提供手機端與 App 端一些資安

場次	議題
	技術面與使用面的建議？
第二場	1. 「我國智慧型手機系統內建軟體資通安全檢測技術規範草案」說明，針對規範訂立之安全等級與檢測項目進行討論。 2. 由研究團隊進行「第三方檢測實驗室認可規定修訂草案」說明，針對檢測實驗室之資格要求進行討論。
第三場	1. 依據第二次座談會議決議修訂後內容，針對「我國智慧型手機系統內建軟體資通安全檢測技術規範草案」修改項目說明，並針對規範訂立之安全等級與檢測項目進行討論。 2. 依據第二次座談會議決議修訂後內容，針對「我國智慧型手機系統內建軟體資通安全檢測技術規範草案」修改項目說明，並針對規範訂立之安全等級與檢測項目進行討論。

三、 共同討論意見之研析

議題討論	決議	採納與否
1. 手機更新後，對於手機商是否需要再進行一次檢測。	目前規劃上市前檢測採取核發認證標章方式辦理，若版本更新則於次一支上市手機進行檢測並核發認證標章，已於市面上流通版本與送測版本是否相同，則規劃由 NCC 以抽測方式檢驗，上述建議將草擬於期末報告中提交 NCC 後續研議。	□採納 □不採納 ■規劃後待 NCC 決議 □政策面討論
2. 此規範是強制性嗎?	未來 NCC 會在官網上公告送測通過手機品牌與等級供民眾參	□採納 ■不採納

議題討論	決議	採納與否
	考，目前未有法源依據，故主管機關無法強制規定業者要通過哪一等級之檢測，但希望以資訊公開方式促使手機原廠主動檢測提升安全性，並可使民眾買到更安全手機。	□規劃後待 NCC 決議 □政策面討論
3. 安全等級分類須區分清楚，建議以使用者角度為思考點，並針對使用者進行明確區分。	而安全等級目前規劃以使用者角度為出發點，並區分 2 級，第 1 級為基礎型，以使用者隱私相關的資料安全為主，第 2 級為進階型，包含使用中、儲存及傳輸中的資料，確保所有資料在各狀態下可被安全使用。	■採納 □不採納 □規劃後待 NCC 決議 □政策面討論
4. 層級區分應該要有表格呈現。	已於附件中將各檢測項目隸屬之等級用表格逐一呈現。	■採納 □不採納 □規劃後待 NCC 決議 □政策面討論
5. 應明確定義何謂「內建軟體」，並說明檢測範圍。	已於規範中說明內建軟體包含出廠預設程式、銷售商加載程式、無圖示程式/程序三種，並有說明個程式之定義。 已於規範中說明檢測費為包含資料安全、行動應用程式安全、作業系統安全以及通訊安	■採納 □不採納 □規劃後待 NCC 決議 □政策面討論

議題討論	決議	採納與否
	全。	
6. 安全等級的標準須和國際主要國家的資安標準方向一致。	本規範參考 OWASP Mobile Security Project、NIST 800-164.163 及 ITU-T YD 2407-2013.2408-2013，並於規範文件中附上與國際間對應關係表。	■採納 □不採納 □規劃後待 NCC 決議 □政策面討論
7. 等級檢測內容除了安全性考量外，應考量檢測時間。	目前規劃將 L1 之檢測時間控制於 2 週內，但確切時間須等規範測試後再行研議。	■採納 □不採納 □規劃後待 NCC 決議 □政策面討論
8. 資料的型態建議改以「型別」做說明，如「第 1 型資料」，以免造成混淆。	資料型態已改為「型別」，並以是否屬於敏感性資料，以及是否為使用者輸入作為判定標準，將資料區分 4 種型態。	■採納 □不採納 □規劃後待 NCC 決議 □政策面討論
9. 內建軟體功能說明書內容過細，容易造成手機商送測時間，建議簡化書審流程及說明書之填寫項目內容。	書審內容目的讓手機業者自行闡述各 APP 須索取之個資權限要求，以利檢測實驗室與民眾判斷是否有不合適之權限要求狀況，避免索取過多個資，基於消費者資料保護與安全考量仍需納入完整自評表。	□採納 ■不採納 □規劃後待 NCC 決議 □政策面討論
10. 檢測是否可規	目前檢測規範未來將適用於規	■採納

議題討論	決議	採納與否
範大陸白牌手機與大陸APP。	範通訊商將手機上市前進行檢測，並未區分是否屬白牌手機。	□不採納 □規劃後待NCC決議 □政策面討論
11. 關於APP或手機權限等自我宣告的內容建議應該也要檢測。	自我宣告屬於本規範之書審重點，並試測作業後於期末報告中明確擬定廠商自我宣告範本，告知各欄位須填寫之深度。未來期望透過公開廠商自我宣告表及實驗室檢測結果，讓民眾可上網審視手機權限要求是否與廠商自行聲明相符與妥適性。	■採納 □不採納 □規劃後待NCC決議 □政策面討論
12. 檢測實驗室之資格要點，若兩種身分是分開判定，請分開撰寫，以免混淆。	目前用章節方式區隔「資通設備資通安全檢測實驗室」與「智慧型手持式行動臺安全檢測實驗室」，待期末審查後可另提供完全分開之兩份要點予NCC。	■採納 □不採納 □規劃後待NCC決議 □政策面討論
13. 實驗室的資格僅限人員條件，測試能力不規定嗎?	目前擔心設備上之限制會造成品牌限定，故僅針對人員進行規定，待後續與NCC、TAF與各檢測實驗室再商議。	□採納 □不採納 ■規劃後待NCC決議 □政策面討論
14. 流程上應為NCC法規訂	與NCC及TAF共同討論過，流程將依照建議訂立。	■採納 □不採納

議題討論	決議	採納與否
立完成後，檢測實驗室直接與 TAF 申請，TAF 再邀約 NCC 專家或外部專家一同資格審查，核可後 TAF 納入特殊服務計畫項目，NCC 可再認可 TAF 之審核並核發證書。		□規劃後待 NCC 決議 □政策面討論
15. 實驗室主管要求資安關經驗三年以上實屬嚴苛，建議不限定資安域之經驗或刪除此條，而報告簽署人可維持。	實驗室主管之資格要求該訂立多嚴謹，須再與 NCC、TAF 與檢測實驗室共同討論，瞭解目前國內檢測實驗室現況，再修訂資格條件。	□採納 □不採納 ■規劃後待 NCC 決議 □政策面討論
16. 報告簽署人部分提及須取得 CEH、CISSP 等證照，然而	報告簽署人之證照要求目前訂立為 CEH、CISSP 須取其一，並在取得其他資安相關證照(已名列於要點中)。	□採納 □不採納 ■規劃後待 NCC 決議

議題討論	決議	採納與否
該證照提到手機層面占少部分，建議應以其他資安證照作為門檻要求。	然而多場次反應證照有更新、種類涵蓋不完全，以及取得時間成本問題，因此該如何擬定還須與 NCC、TAF 與檢測實驗室共同討論。	□政策面討論

附件 7 說明會會議紀錄與相關會議資料

國家通訊傳播委員會

104 年度「手機系統內建軟體資安檢測」計畫

說明會 會議紀錄

一、會議名稱：智慧型手機系統內建軟體資安檢測技術規範推廣說明會

二、時間：105 年 2 月 19 日(星期五) 上午 10 時 00 分~12 時 00 分

三、地點：集思北科大會議中心 205 會議室(瑞特廳)（台北市忠孝東路三段 193 巷旁<台北科技大學億光大樓>）

四、議程：

時間	議題	主講人
09:30 - 10:00	與會者報到	
10:00 - 10:10	主辦單位/執行單位致詞	
10:10 - 10:40	手機系統內建軟體資通安全檢測技術規範要點說明	安華聯網科技(股)公司 洪光鈞總經理
10:40 - 11:00	手機系統內建軟體資通安全試測結果說明	台灣電子檢驗中心 葉錫勳組長
11:00 - 11:15	休息時間	
11:15 - 11:30	手機系統內建軟體資通安全檢測制度說明	中華民國資訊軟體協會 楊蕙如組長
11:30 - 12:00	意見交流	
12:00	會議結束	

五、主席：中華民國資訊軟體協會 喻維貞 副秘書長

記錄：姚人鳳

六、出席代表(詳如簽到表)：

國家通訊傳播委員會吳銘仁簡任技正
國家通訊傳播委員會蘇勇吉科長
國家通訊傳播委員會李福懿技正
中華民國資訊軟體協會喻維貞副祕書長/計畫主持人
中華民國資訊軟體協會鍾榮翰協同計畫主持人
中華民國資訊軟體協會楊蕙如組長

中華民國資訊軟體協會姚人鳳專員
安華聯網科技股份有限公司洪光鈞總經理
台灣電子檢驗中心葉錫勳組長

七、座談議題：

八、與會者討論(依發言先後排序)：

(一)與會者提問：

1.美國 FBI 要求 APPLE 手機提供手機解碼後門，遭受 APPLE 拒絕，該規範上路後是否會遇到類似問題？
2.檢測天數 60 人天，對於手機商而言有些過長，可否再請壓縮檢測時間？
3.制定規範的單位，是否會有規範版本更新的規劃？
4.之前有聽說初級是強制性，那現在最終的規劃會是強制性嗎？
5.APP 開發時會分架上版與內建版，然而內建 APP 可以透過 STORE 進行更新，而更新後的版本可能會出現問題，那更新後產生的問題與工業局的規範是否有共同的管控機制？而版本更新該如何管控？
6.因現在是屬於自願性檢測，60 人天數對廠商而言成本大，因此若以檢測實驗室的角度而言，那市場規模有多大？效益多大？
7.是否有計畫多久之後會更新技術規範，進而推動強制性要求？
8.是否會有英文版規範內容？

(二)與談者回覆：

1.就國家而言，NCC 目前是以安全檢測角度提出檢測制度，然而涉及到刑法問題，則由刑事單位(內政部警政署、調查局、司法機關等)著手進行，依照法律要求與權責進行刑事調查。(通傳會 吳銘仁簡正)
2.目前 60 人天是一支手機與一個檢測人員所計算之工作天，若有時程上要求，建議手機業者送測時提供多支手機以利檢測實驗室多工同步測試，以利縮短天數。(軟協 楊蕙如組長)

3.研究單位目前所提供的內容是屬於草案，仍可因應各位今日所反應之意見調整之，提交後由通傳會於 3~5 月間舉行公聽會以及內部法令程序，定案後則為公告版本，目前規範的初級是屬於手機的基本功能保護層面，改變程度應該不大，正式公告後，應該會維持 1~2 年，然智慧型手機功能多更有其他穿戴式裝置陸續發展，則建議通傳會依據市場發展現況進一步新增檢測技術規範。(軟協 楊蕙如組長)

4.通傳會委託中華軟協訂立技術規範草案，後續將先推動試辦期，希望手機商與檢測實驗室可以於此試辦期調整時程安排，因此目前此規範推動先以廠商自願性檢測為主，將來會看整個市場發展情況決定是否要強制規定。(通傳會 吳銘仁簡正)

5.若開機有連網行為後立即更新 APP，則此更新版本為檢測的第一版本，若 APP 連網後未有更新，則以送測版本進行檢測。若是使用一段時間後才於 APP store 更新者，則屬於工業局 APP 規範之範疇。若手機於取得標章後仍有內建軟體之更新，應由送測單位提供手機依據更新部分內容進行檢測，通傳會也會規劃以抽測方式管理已核發之標章是否皆符合規定。(軟協 楊蕙如組長)

6.目前雖是以推動手機業者自願性檢測，通傳會也會從電信業者著手推動，於電信業者通路中銷售之綁約手機須先經過資安檢測，因此市場一定會有檢測需求。(通傳會 吳銘仁簡正)

7.該技術規範參考多國之規範內容進行擬定，因此通傳會希望先由電信業者綁約手機須經資安檢測作為第一步，手機業者則為自願性檢測，規範後續之更新規劃，將端看國際潮流以及國內運作狀況而定。(通傳會 吳銘仁簡正)

8.在規範草案提交予通傳會審查通過後，會依據審查通過版本提交規範英文版。(軟協 楊蕙如組長)

國家通訊傳播委員會

104 年度「手機系統內建軟體資安檢測」計畫

說明會 會議紀錄

一、會議名稱：智慧型手機系統內建軟體資安檢測技術規範推廣說明會

二、時間：105 年 2 月 19 日(星期五) 下午 02 時 00 分~04 時 00 分

三、地點：集思北科大會議中心 205 會議室(瑞特廳)（台北市忠孝東路三段 193 巷旁<台北科技大學億光大樓>）

四、議程：

時間	議題	主講人
13:30 - 14:00	與會者報到	
14:00 - 14:10	主辦單位/執行單位致詞	
14:10 - 14:40	手機系統內建軟體資通安全檢測技術規範要點說明	安華聯網科技(股)公司 洪光鈞總經理
14:40 - 15:00	手機系統內建軟體資通安全試測結果說明	台灣電子檢驗中心 葉錫勳組長
15:00 - 15:15	休息時間	
15:15 - 15:30	手機系統內建軟體資通安全檢測制度說明	中華民國資訊軟體協會 楊蕙如組長
15:30 - 16:00	意見交流	
16:00	會議結束	

五、主席：中華民國資訊軟體協會 喻維貞 副秘書長

記錄：姚人鳳

六、出席代表(詳如簽到表)：

國家通訊傳播委員會吳銘仁簡任技正
國家通訊傳播委員會蘇勇吉科長
國家通訊傳播委員會程奕翔科員
中華民國資訊軟體協會喻維貞副祕書長/計畫主持人
中華民國資訊軟體協會鍾榮翰協同計畫主持人
中華民國資訊軟體協會楊蕙如組長

中華民國資訊軟體協會姚人鳳專員
安華聯網科技股份有限公司洪光鈞總經理
台灣電子檢驗中心葉錫勳組長

七、座談議題：

八、與會者討論(依發言先後排序)：

(一)與會者提問：

1.檢測時間 60 天是否太長？

2.請問 TAF 關於工業局、經管會等，皆有要求檢測實驗室需有 ISO 17025，但各規範內容要求皆不同，那這部分的認證是要依照各機關要求進行認證，還是有共通法則？

3.軟體銷售版本的認證，提到更新需要重新進行送測，因軟體開發會有上千個 bugs，對手機業者實務作業而言較難配合，若開發後是否有其他方法符合規範？

4.上市後的版本更新之送測該如何進行?

(二)與談者回覆：

1.於檢測規範中要求送測單位至少提供 2 支手機，可有效縮短檢測時程，若送測單位可提供多支手機，加上實驗室人力配合，則可更加縮短檢測時間。(軟協 楊蕙如組長)

2.TAF 會有個特定服務計畫，會依照各主管機關的要求進行每個特定服務計畫的審查制度，若有單位想要同時間申請多主管機關的要求，可同時間一起申請，並申請時勾選欲申請的主管機關之特定服務計畫，TAF 可依據申請要求同步作業，縮短實驗室申請時間。(TAF 盛念伯組長)

3.整體規範制度的訂定是希望保障消費者拿到智慧型手機時是屬於安全的狀態，因此送測手機即應為上市手機，對於版本更新的檢測，希望手機業者能針對軟體更新的部分進行檢測，無須整支手機重新檢測。建議手機業者應於手機製作期間與上市前將檢測時程

納入整體排程，才得以兼顧手機上市與資安檢測之時程。(軟協 楊蕙如組長)

4.若手機於取得標章後仍有內建軟體之更新，應由送測單位提供手機依據更新部分內容進行檢測，通傳會也會規劃以抽測方式管理已核發之標章是否皆符合規定。(軟協 楊蕙如組長)

附件 8 所辦說明會之紀錄及研析意見

智慧型手機之安全使用宣導資料

你知道嗎?手機已不在是年輕人的專利了!近年來越來越多中高年齡者開始使用智慧型手機,手機的使用率在台灣非常普及,資策會 FIND 公佈最新調查結果顯示，國內 12 歲以上使用智慧型手機或平板電腦者已達到 1604 萬人，約每 4 人便有 3 人為行動裝置使用者。其中智慧型手機普及率約 73.4%，推估約 1525 萬用戶。調查也發現中高齡層普及率逐漸提高,50 歲以上族群擁有行動裝置比率達 26.6%,行動裝置已普遍走入台灣各年齡層的生活中。

但當大家普遍使用手機的同時,使用手機上卻有著很多資安風險,一個不小心容易造成照片、電話簿外洩,或是帳號被盜用盜刷卡等狀況,以下彙整一些使用手機可能遇到的資安問題以及該注意的事項給民眾參考，讓大家可以愉快又安全的使用手機。

一、手機使用習慣之潛在風險：手機中毒徵兆

在台灣智慧型手機已成為人們生活必需品，然而在享受行動裝置便利有趣的同時，民眾於手機資安防護意識卻非常薄弱，防毒大廠卡巴斯基的實驗室研究發現，Android 木馬病毒可透過藍芽或 Wifi 快速傳播，不僅回傳手機的相關資訊，更會自動傳送簡訊至手機所有聯絡人，然而這類型病毒卻是看不到、刪不掉，因此許多民眾手機中毒卻渾然不知。

其實手機中毒仍有跡可循，當手機出現下列幾點徵兆，民眾便可懷疑手機是否感染病毒，盡快尋求專業援助，降低受害可能性。

- 使用效能無故變差
- 電池壽命突然變短

- 莫名其妙通話中斷
- 電信費用突然暴增
- 出現自動下載軟體

二、手機資安事件與犯罪手法：常見手機詐騙手法

手機的方便性已與民眾的生活密不可分，行動網路已成為人人生活中的必需品，手機快速上網更是多數民眾嚮往，傳輸速度快，各裝置間同步連結、資料傳輸方便，但卻衍生更多個人資料安全問題。

對於有心人士而言，竊取資料盜賣是門穩賺不賠的生意，資料量越大獲取價金越高，因此在現代人手一機的社會中，手機犯罪手法不斷推陳出新，目的便是為了竊取個人資料，多變的手機犯罪手法，不外乎可區分為三種媒介：連結網址、APP 及 Wifi 連線，在此提供三種媒介常見的攻擊手法，提醒使用者注意。

攻擊媒介與方法	攻擊管道	結果
連結網址 含有惡意程式或網站的連結被點選 1. 社交工程 2. 釣魚網站 3. 勒索軟體	1.透過簡訊、通訊軟體(Line 或 what's app 等)誘發使用者點選惡意連結 2.民眾上網點選惡意連結	● 小額付費 ● 下載惡意程式 ● 自動加密手機內資料要求付費解密
APP 含有惡意程式之	從未知來源下載 APP	● 自動傳送惡意簡訊給朋友造成小額付

攻擊媒介與方法	攻擊管道	結果
APP 直接或間接被下載		費或使朋友遭受詐騙 ● 竊取手機內個人資料造成資料外洩
Wi-Fi 偽裝正常免費 Wi-Fi 吸引民眾連結	透過免費提供的誘因吸引民眾連結惡意 Wi-Fi	● 竊取姓名、密碼 ● 獲得手機控制權

綜合上述的攻擊媒介，其實不外乎可區分為三種詐騙型態：結合社群網站與社交工程進行手機簡訊詐騙、網路釣魚惡意連結，以及偽冒惡意 APP 軟體下載，看看以下新聞案例，就知道有多嚴重了！

(一)結合社群網站與社交工程進行手機簡訊詐騙

手機簡訊認證碼小額付款詐騙事件，不僅是最傳統的簡訊詐騙，過往的即時通訊(如 Skype)、許多社群網站(如 Facebook)，以及通訊 APP 軟體(如 Line、What's App 等)皆常出現此類型詐騙手法，駭客假冒手機使用者的親朋好友的方式要求使用者點選具吸引力的連結(例如投票網站、影片等)，進而造成社交攻擊事件，手機因此遭受木馬程式攻擊，或是騙取手機簡訊認證碼，進行網路小額扣款付費的交易行為，輕則損失幾千元，重則被當成詐騙人頭帳戶。

- 新聞事件 1：【刑事局查獲橫跨兩岸的惡意簡訊詐騙集團！國內近 10 萬手機遭感染！】2015/10

從民國 102 年 8 月開始，不少民眾先後收到詐騙簡訊，犯罪

集團以「聚會相片」、「宅急便通知」、「電費通知」、「快遞簽收單」、「新北市政府警察局通知」等名義發送簡訊，利用社交工程手法誘騙民眾點擊簡訊中的連結網址，使手機被植入惡意程式，民眾收到高額電信帳單才知受害。

根據警方查獲該集團在國內的機房，清查 6 台中繼伺服器遭感染後的手機，也就是俗稱的「肉機」，活動中的肉機約有 98525 支，攔截近一週簡訊內容數量達 1600 萬則。潛在被感染的手機及民眾私人簡訊被攔截數量難以估計，使國內 2300 萬人曝露在詐騙簡訊的風險中。

資料來源：iThome

圖1　詐騙集團常以快遞簽收單等名義發送惡意簡訊，誘導民眾點選連結

- 新聞事件 2：【「你有一條新留言」他點開網址被盜刷 2.4 萬超傻眼】2015/12

  收簡訊也可能會被盜刷信用卡，有一名莊姓男子收到手機簡訊，內容為「你有一條新留言 http://cht.tw/****/6qa39」，他沒有多想點進去看之後，結果手機自動下載一個安裝程式，他誤以為是電信業者贈送的遊戲軟體，竟陸陸續續收到銀行

通知信用卡消費簡訊，最後總共被盜刷了 2.4 萬元。

(二)網路釣魚惡意連結

現今的手機功能已等同一般電腦，該有的功能幾乎都有，然而因使用者介面關係，手機瀏覽器所提供的資訊卻無法像電腦一樣能完整呈現，例如顯示 SSL 資訊的功能常因手機螢幕大小現制而難以完整呈現，許多網站該跳出警示訊息要求使用者進行驗證時，手機版網頁為求畫面簡約性通常會跳過此步驟，行動版瀏覽器所提供的資訊往往不足以讓使用者判斷該網站是否有潛在的危險。

- 新聞事件：【小心被詐！搜尋 LINE 首連結疑似釣魚網站】2014/5

  網友發現，知名台灣搜尋網站雅虎奇摩（Yahoo）在搜尋欄打 LINE 後，最初的連結疑似是釣魚網站，並非官網的正式連結，點選至釣魚網站時，首先會發現背景與實際的 LINE 官網相當雷同，且會跳出一個視窗，與電腦版 LINE 登入畫面極為相似，疑似為詐騙集團設的陷阱，假設民眾不小心輸入了帳密，很可能就會被詐騙集團盜用。

  假如點到正確的官方網站，便不會出現要使用者登入的畫面，兩個網站的網址相當類似，釣魚網站為（http://line.pm/zh-hant/）正確的官方網站則是（http://line.me/zh-hant/），民眾如果未注意到此異同，很可能你的帳號不久後就會被詐騙集團拿去使用，再盜取周遭親友個資。

資料來源：自由時報

圖2　惡意網站常用極相似網址以假亂真，誘導民眾登入網站進而竊取帳密資料

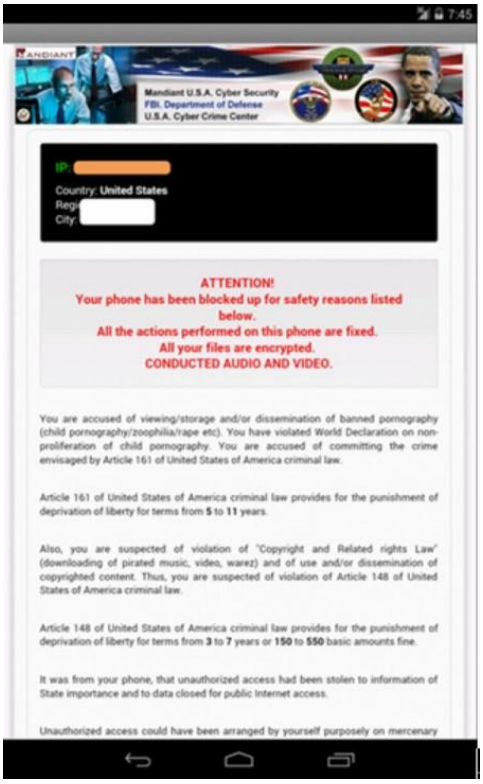
(三)勒索軟體綁架手機重要資料

大部分的勒索軟體是透過釣魚網站入侵，大多經由特定的網址來散布，內容不外乎使用引起好奇心之字眼，引導使用者點選網址或免費廣告(內含惡意連結)。勒索軟體顧名思義屬於勒索行為，當使用者受到勒索軟體攻擊，該軟體會自動加密鎖住手機或儲存資料，並要求使用者特定期間內支付相當費用，否則將永遠無法使用手機或資料。

- 新聞事件：【小心勒索軟體入侵！不給錢手機變磚頭！】

2014/5

趨勢發現，過去以綁架個人電腦為主的 Roveton 勒索程式，現在將目標轉移到手機，使用者手機一旦被入侵取得控制權，就會被勒索支付 300 美元贖金，才能使手機恢復正常功能。目前國外已出現類似綁架的案例，駭客在入侵手機取得手機控制權後，便會根據使用者所在地的不同，假冒為當地執法單位向使用者恐嚇勒索贖金，威脅不支付贖金便無法繼續使用手機。



資料來源：iThome

圖3　一旦使用者的手機遭入侵，手機螢幕便會顯示假冒的執法單位向使用者要求支付贖金，否則無法正常使用手機

(四)偽冒惡意 APP 軟體下載

手機 APP 商店裡有琳瑯滿目的免費 APP 供民眾下載，然而

這之中包含許多含有惡意程式的 APP，魚目混珠難以分辨。當使用者不知 APP 的真實性，下載到含有惡意程式的 APP 時，最容易造成下列二種情況，讓使用者難以察覺。

1.直接或間接幫使用者安裝廣告或不想安裝的 App

多數的免費 APP 都含有廣告內容，並在使用者不知道的情況下，直接或間接取得手機中的某些資訊，例如手機內的通訊錄名單、啟動相機功能或 GPS 功能等，或是與社群網站 APP 取得連結，更能獲得更多好友名單。有許多則是當使用者啟動多含有惡意廣告的 APP 時，系統會自動連回特定網址，多數網址皆有可能為含有惡意程式的網址。

- 新聞事件：【惡劣色情 App：偷拍照片再鎖機，然後勒索 500 美金！】2015/9

  安全公司 Zscaler 發現一款名為 Adult Player 的 Android App 偽冒成播放色情影片的 App，騙取使用者下載開啟後，要求使用者同意開放管理員權限，使用者按啟動後出現假的更新網頁，下載另一個名為 test.apk 的惡意程式，下載後則開始偷拍使用者相片並鎖機，基於安全理由手機遭到鎖定，資訊也被加密，然後向用戶勒索高達 500 美元的贖金。

圖4　資料來源：iThomeAdult Player 的 Android App 偽冒成播放色情影片的 App

2.隱身在正常的 App 中

有一些惡意 App 則偽裝或隱身在正常的 App 中，通常是需要透過深入的檢測分析，否則很難察覺這些惡意 App，然而當使用者觸及到某些行為或某些動作進行達到一定的次數，可能造成資料直接回傳至外部伺服器等，或直接於系統背景中啟動監聽/監視行為，這些狀況皆是使用者難以察覺的。

- 新聞事件：【XcodeGhost 災情比原先預期嚴重：可能有上千款 app 受感染，數量持續增加】2015/9

日前資安業者 Palo Alto Networks 指出，中國開發者在不知情下使用遭駭客竄改含有 XcodeGhost 惡意程式的蘋果開發工具 Xcode，導致不少知名合法 app 受到感染，竊

取用戶裝置、app 資料，自動幫使用者接受駭客指示跳出警示視窗，誘騙使用者輸入帳號及密碼等個資，或是開啟 URL 利用釣魚網頁取得個資，以及存取剪貼簿的資料，如果使用者習慣將密碼儲存在剪貼簿就可能被竊。如果再進一步修改惡意程式碼，甚至可能以釣魚手法取得 iCloud 密碼，截至目前為止，資安業者檢視受影響 app 數量高達到上千款，而且數量可能還會再增加。

趨勢科技指出，XcodeGhost 可能引導使用者在 App Store 下載特定的 app，或是傳送訊息給使用者，透過詐欺或釣魚的方式騙取個資。雖然 XcodeGhost 災情最嚴重為中國地區，但部份知名 app 開放國外下載，北美洲也是受害的地區。APP 開發者也可運用簡單的指令檢查自己所使用的 Xcode 是不是含有上述惡意程式。

三、正確使用手機小撇步

網路上的詐騙方式很多種，所有的詐騙方法不外乎皆是運用民眾好奇心與求一時的方便心態進行攻擊，以下提供幾個正確使用手機的小撇步，避免手機對話紀錄、照片、密碼等隱私資料外洩，以保障個人隱私。

(一)僅從信賴的來源下載 APP

下載 APP 務必要從信可信賴的來源(例如 Google Play 或是 Apple Store)進行下載，千萬別貪圖方便或是特殊性，從未知的來源進行下載，因這些 APP 流通在網路上大多未經過審核機制，極有可能夾帶惡意程式，若下載該類型惡意 APP 程式，容易讓資料在不知不覺中洩漏。

(二)下載 APP 必須停看聽

每個 APP 市集都會有評價等級，下載有興趣的 APP 前，請先停看聽，停：暫停下載的衝動，看：查看 APP 評分，有些是以五顆星星做為表達，當然越多人給的評分數越高越好，代表 APP 在民眾使用的評價越好，越穩定也越可靠，聽：聽聽使用者的評價，評價一定會有正反二面，若使用者多數都是好評價，那麼就可考慮下載囉！

(三)要了解每支 APP 可以取得哪些個資

APP 下載時或是使用時，都會要求取得您的授權，您可判斷使用該 APP 所要索取的權限是否合理，例如：下載修圖軟體的 APP 卻要求索取您聯絡簿(聯絡人)權限，則可初步判斷此為不太合理的現象，建議您不要使用該 APP，則可有效防止第 3 方透過 APP 蒐集個資。

(四)檢查定位設定

「常用位置」(Frequent Locations)的功能是用以追蹤使用者經常造訪的地點，例如：辦公室、購物中心、咖啡店等，再根據資料提供通勤時間等有用的訊息給使用者，但這功能所記錄的內容包括地點、到訪次數及逗留時間等。原本貼心的功能卻容易被駭客盜取利用，故建議將定位功能預設為關閉，可以防止手機把您家、工作場合及常去地點紀錄下來。

以 iPhone 手機為例，如何設定關閉路徑：設定（setting）→私隱（privacy）→定位服務（location services）→系統服務（system services），就可以將常用位置功能關閉。

(五)點選網址請三思

網址是一般民眾最不會去注意的資訊，其實魔鬼藏在細節裡，有些網址是可以看出端倪的，在這提醒大家點選網址該注意的事：

- 大多惡意網址會讓民眾連結至非台灣的網站，因此若網址中出現其他國家的代碼，則要特別注意，別點選比較好。
- 有些網址會以假亂真，除了辨識國家代碼外，大多很難識別真假，但這些網址在手機上會以簡訊、通訊軟體作為媒介，再以吸引人的標題要民眾點選，因此若看到看似投票、聳動的新聞、官方網站的通知信等，除了能跟本人確認網站是否正確外，官方網站的通知信最好從官網登入查詢，以免被騙。

(六)別把個資用通訊軟體傳出去

所有的通訊軟體資料的傳輸過程無法保證是否是安全並且加密過，也無法保證聊天的對象是否電腦是安全的，駭客可利用簡訊或電子郵件等方法來破解手機或電腦安全設定，因此建議民眾不要將個人重要資訊(如身分證、銀行帳號密碼等)資料或照片用通訊軟體傳送出去。

(七)即時更新作業系統

部分手機作業系統的更新頻率高，除為了修改系統功能外，另外則是為了修補資安漏洞，因此建議務必即時更新作業系統，避免手機因系統漏洞而造駭客利用入侵，保護個人資料安全。

(八)避免資訊自動儲存

現代人皆具備多個網路帳號與密碼，多數使用者為了省去記憶，都使用瀏覽器自動儲存密碼的功能，相關密碼皆儲存手機或電腦中，若設備遭駭客入侵則遭盜取。除了避免使用帳號密碼自動儲存功能外，亦建議所有使用者，不同之雲端硬碟、社群軟體或購物平台等皆避免使用同一組帳號或密碼，降低帳號密碼遭竊時之風險，才能確實保護個人資料。

(九)當心免費無線上網熱點

現在許多公眾場合都有提供免費 Wi-Fi，對於使用者來說是再方便不過了，然而這卻也是駭客最好利用的管道之一，駭客建置惡意 Wi-Fi，蒐集民眾個資。提醒使用者在連結前需先確認場地提供的 Wi-Fi 全稱，若需輸入個人資料則避免連線，才能有效將使用風險降到最低。

(十)手機使用複雜密碼與遠端刪除資料

即便使用者已小心翼翼使用手機，卻無法避免手機遺失造成手機內部資料外洩，因此手機的開機密碼是防範外人使用的第一道防護，若能使用圖形密碼、多位數字的開機密碼，或是複雜的編碼原則，例如英文+數字，則可有效避免手機遭快速解密，並設定遠端刪除資料，即時刪除重要資料。

四、正確使用手機方式與注意事項-手機操作十大步驟

對於智慧型手機之使用，參考美國聯邦通信委員會分別針對 Android 及 iOS 及 Windows phone 作業系統建議，十大安全操作步驟，摘述如後：

(一)設定手機的個人識別碼及通行碼(Set PINs and passwords.)

(二)請不要修改您的智慧型手機的安全設定(Do not modify your smartphone’s security settings.)

(三)請備份並保護您的資料(Backup and secure your data.)

(四)僅從信任之來源安裝 apps(Only install apps from trusted sources.)

(五)請在安裝 Apps 前確認並明瞭軟體所要求的授權(Understand app permissions before accepting them.)

(六)請安裝或啟用允許遠端定位及刪除資料之安全程式(Install security apps that enable remote location and wiping.)

(七)請更新系統或軟體之更新程式(Accept updates and patches to your smartphone’s software.)

(八)請謹慎使用開放的無線網路(Be smart on open Wi-Fi networks.)

(九)請在捐贈、轉售或回收您的舊智慧型手機之前，應將資料確實刪除(Wipe data on your old phone before you donate, resell, or recycle it.)

(十)向警察機關或電信公司回報遭竊之手機(Report a stolen smartphone.)

五、參考指引要求之使用者防護安全

多數國家均在協助使用者的立場，藉由正確的設定智慧型行動裝置之相關安全機制，達到初期對於智慧型行動裝置基本使用安全之保護，因此本計畫歸納前述所有關於保護使用者

資料安全之相關指引，將其彙整如下列 10 項使用者指引，以期防範資訊安全問題於未然。

表1　使用者指引參考表

項次	項目	說明
1	設定 PIN 碼、行動裝置密碼與多重身分驗證機制(例如:指紋辨識)。	避免行動裝置因送修或失竊而遭到未授權的存取內部資訊。
2	定期檢查並安裝原廠提供之更新與修補程式。	藉由原廠提供的修補機制，提升行動裝置安全性。
3	不移除行動裝置預設的安全機制。	不應對行動裝置進行”破解”、”越獄”或”取得 root 權限”，卸除行動裝置預設安全機制。
4	僅從受信任的來源安裝應用程式。	避免安裝來源不明的程式造成安全威脅，應從正式的官方管道取得 Apps。如: Apple App Store, BlackBerry World or Google Play。
5	不使用之行動裝置應刪除所有儲存之資料並恢復出廠預設值。	當不使用的行動裝置要移轉他人使用、廢棄、捐贈、轉賣、送修前，應刪除所有行動裝置上之資料，並恢復出廠預設值。
6	應透過建立信任安全的連線與機制傳送機敏資料。	使用點對點的安全通道(例如:SSL/TLS/HTTPS)與金鑰加密機制，對欲傳送之機敏資料(如:網路銀行之帳號、密碼)加以保護。
7	所有介面在不使用的狀況下應關閉，並避免建立不信任連線。	防止不經意的狀況下，在公共場合主動連線或被不明連線。例如:藍芽的探索模式應於使用後立即關閉，並盡

項次	項目	說明
		可能避免使用。以及不連線到公共場合中不明的無線基地台(或無線熱點)。
8	特別留意軟體蒐集使用者資料要求。	在行動裝置軟體提示並要求時，應注意盡可能避免不必要之資訊之上傳。例如:不任意依據軟體指示上傳通訊錄資訊。
9	不任意相信並點選可疑的郵件或簡訊所提供之連結位址。	對不明簡訊內容應提高警覺，以防範簡訊詐騙與避免遭受安裝惡意程式之威脅。
10	對於任何應用程式執行過程所產生的錯誤代碼應加以求證。	那有可能是惡意程式欲繞過系統防禦機制所導致，應對不明訊息代碼向原始供應商進一步求證。

資料來源：本計畫彙整

附件 9 專案工作會議會議紀錄

104 年 NCC「手機系統內建軟體資安檢測」計畫

會議紀錄

一、會議名稱：起始會議(第一次工作會議)

二、時間：104 年 08 月 04 日(星期二)下午 2 時 00 分

三、地點：NCC 5 樓會議室（台北市濟南路二段 16 號 5 樓）

四、會議主持人：吳銘仁 簡任技正

五、出席人員：

通傳會：李福懿

中華軟協：喻維貞計畫主持人、楊蕙如專案經理、姚人鳳專員

安華聯網：洪光鈞總經理、劉建宗協理、林昱廷經理

TTC：蔡志明組長

ETC：宋孟曉經理、葉錫勳工程師

六、記錄：姚人鳳

七、結論：

請示事項	決議
1. 評選會議中委員提及應進行手機晶片檢測，因與 RFP 不符，故提請刪除該建議項目	硬體檢測部分實非 RFP 要求項目，請再參考各國作法，提供後續處理建議。
2. 檢測實驗室管理作業要點修正方向 (1)重新編撰一份實驗室認可規定 (2)於現行規定文件中區分不同類型	請於現行檢測實驗室管理作業要點文件中區分不同類型進行修正。
3. 本案進度規劃是否合宜	合宜，依照 RFP 規定時間交付項目即可。
4. 推廣說明會規劃是否合宜	屆時須蒐集與會者意見作為未來修改之參考依據。
5. 座談會出席代表名單是否合宜	1. 名單須依 RFP 規定，邀請政府機關

請示事項	決議
	單位 4 個以上(至少包括行政院消費者保護處、行政院資通安全辦公室及經濟部附屬單位等)、經我國型式認證手機之廠商、本會電信設備驗證機構、資安設備檢測實驗室，及資安防護專家學者(至少 5 人以上參加)等。 2. 三場座談會名稱請依循 RFP 規定訂為： (1)國際智慧型手機行動裝置資通安全檢測發展現況及各國規範探討 (2)第三方檢測實驗室認可規定修訂草案初稿架構討論 (3)智慧型手機系統內建軟體資通安全檢測技術規範草案討論 3. 第一場座談會(8/18)規劃方案可行 4. 座談會主持人請由軟協擔任

八、散會(下午 3 點 00 分)

104 年 NCC「手機系統內建軟體資安檢測」計畫

會議紀錄

一、會議名稱：第二次工作會議

二、時間：104 年 07 月 14 日(星期二)下午 4 時 00 分

三、地點：Conference call

四、會議主持人：楊蕙如 組長

五、出席人員：

協同計畫主持人：鍾榮翰(睿明知通)

專案顧問：洪光鈞(安華聯網)、蔡志明(TTC)、葉錫勳(ETC)

專案承辦：姚人鳳

六、記錄：姚人鳳

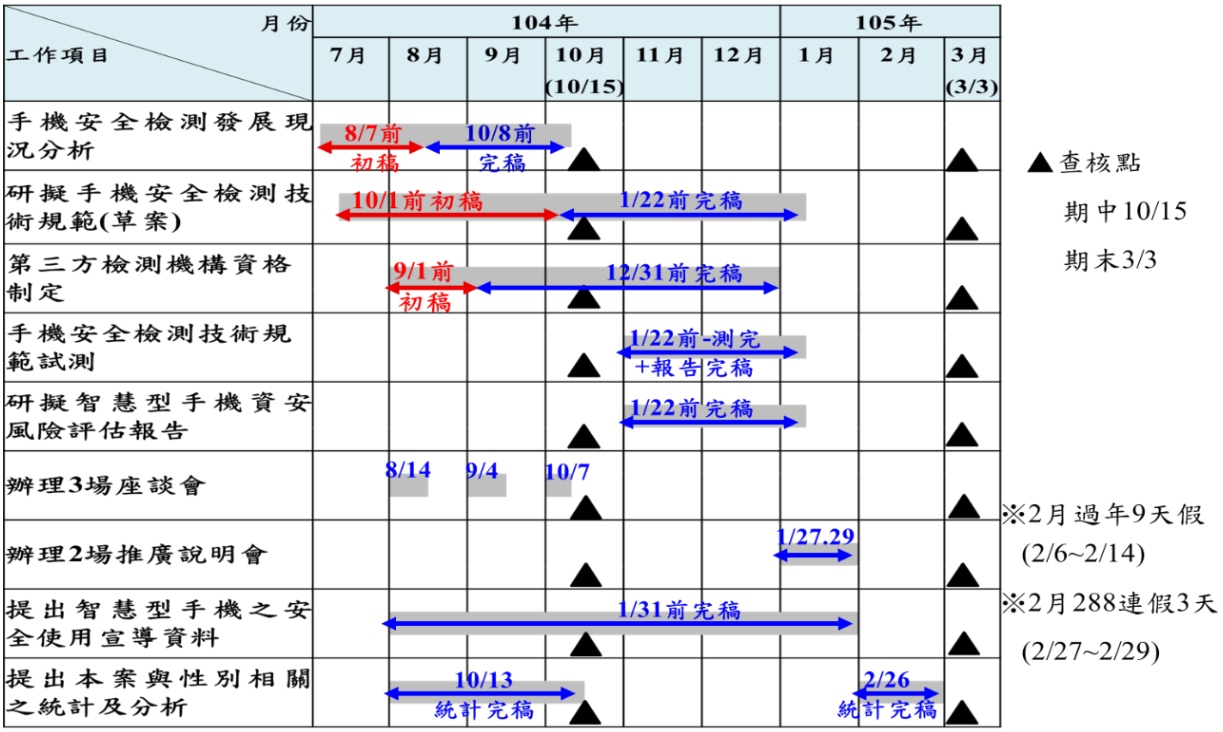
七、結論：

(一)目前國際參考資料彙整如下表，而規範主要參考文件如紅字所示，相關文件請 TTC 進行整理，並依本次會議結論，於 7/24 前提交文件彙整資料，以利座談會召開時使用。

地區	發佈單位	相關發佈文件
國際組織	OWASP	OWASP Mobile Security Project - Top Ten Mobile Risks (2014)
美國	CIO Council	Government Mobile and Wireless Security Baseline (2013/5)
	NIST	• SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations (2013/4) • SP-800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise (2013/6) • SP 800-142, Practical Combinatorial Testing (2010/10) • SP 800-164, DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices (2012/10)

地區	發佈單位	相關發佈文件
		• SP 800-163,Vetting the Security of Mobile Applications (2015/1)
	US-CERT	Cyber Threats to Mobile Phones (2011)
	DoD/DISA	• Commercial Mobile Device Implementation Plan (2013) • Mobile Device Strategy (2012) • Mobile OS Security Requirements
	FCC	• Ten Steps to Smartphone Security • Ten Steps to Smartphone Security (Android)
	NSA/IAD	• Mobility Security Guide v2.3 (2013/11) • Security Requirements for Mobile Operating Systems
中國大陸	工業和信息化部	• YD/T 2407-2013 移動智慧終端機安全能力技術要求 (2013/4) • YD/T2408-2013 移動智慧終端機安全能力測試方法 (2013/4)
英國	ERG	End User Device Strategy: Security Framework & Controls(2013/2)
	ICO	Personal information online small business checklist
	Ofcom	Safer smartphones–keeping your device secure(2013/10)
日本	JSSEC	Security Guideline for using Smartphones and Tablets(2011/12)
	IPA	10 Major Security Threats (2013/3)
韓國	KCC	KCC announces 'Comprehensive Plans for Smart Mobile Security‘ (2010/12)
歐盟	ENISA	• Smartphone secure development guidelines for app developers(2011/11) • Smartphones: Information security risks, opportunities and recommendations for users(2010/12)
	EC	Opinion 02/2013 on apps on smart devices(2013/02)
新加坡	MAS	Technology Risk Management Guidelines(2013/6)

(二)計畫時程規劃如下：



(三)軟協與各手機廠商詢問是否可先索取手機供前測使用，但與 ETC 後測部分無涉。

(四)第一場座談會主要討論方向為「國際手機行動裝置檢測發展現況、規範方向訂立」，時間暫定 8 月第一週，請 TTC 於 7/24 前先完成初稿，並提供給安華參考，以訂立規範方向訂立之基準。

(五)將與羅處長請示之議題如下：

1. 評選會議中委員提及檢測晶片一事因與 RFP 不符，故將提請建議刪除。

2. 檢測實驗室管理作業要點修正方向。

3. 本專案是否參酌技術處研發成果，互為應用。

八、散會(下午 4 點 40 分)

104 年 NCC「手機系統內建軟體資安檢測」計畫

會議紀錄

一、會議名稱：第三次工作會議

二、時間：104 年 10 月 5 日(星期一) 14:00~17:00

三、地點：國家通訊傳播委員會 (台北市濟南路二段 16 號 5 樓）

四、主席：國家通訊傳播委員會羅金賢處長

五、出席人員：

國家通訊傳播委員會：蘇勇吉科長、吳銘仁簡任技正、李福懿技正、程奕翔科員

中華軟協：楊蕙如組長、姚人鳳專員

安華聯網：洪光鈞總經理、林昱廷專案經理、林維展工程師、陳漢平工程師

六、記錄：姚人鳳

七、會議結論：

(一)檢測規範

1. 資安等級(Level)改劃分 3 級，3 個等級為累加制，第 1 級內容為基本隱私保護、使用者操作安全性功能及傳輸安全為主，第 2 級內容增加本機安全保護方法、傳輸安全等級強化，第 3 級內容增加硬體與作業系統底層安全性，名稱請另定義，再呈報 NCC 定奪。
2. 自我宣告表應包含 APP 權限蒐集宣告，請調整附件表格表達方式，並額外提供實例範本，供未來手機商送測填寫時參考。
3. 規範中不宜用「預期結果」，請修改為「判定標準」。

(二)檢測實驗室

1.實驗室報告簽署人資格應比照工業局訂立方式，列出證照。

2.實驗室主管則依據現行規劃辦理，資格不應放寬，建議實驗室可指派適合人選擔任。

3.手機檢測實驗室資格則改以 3 個等級分別訂立，並於資格中列出軟、硬體所需設備，而第 3 等級中人員資格需具備 ISO/IEC 15408 資訊技術安全評估共同準則之評估能力。

(三)計畫要求

1.請彙整目前各檢測項目依據之國際標準內容，做為期中報告附件參考。

2.檢測實驗室要點期中報告請先提供「資通設備安全」和「智慧型手持式行動台安全」合併版本。

3.期中報告先以第三次座談會內容加上今日會議指示修改方向交付，後續再另提交版本呈報 NCC。

八、散會(下午 4 點 40 分)

104 年 NCC「手機系統內建軟體資安檢測」計畫

會議紀錄

一、會議名稱：第四次工作會議

二、時間：104 年 11 月 12 日(星期四) 16:00~17:30

三、地點：國家通訊傳播委員會 (台北市濟南路二段 16 號 5 樓）

四、主席：國家通訊傳播委員會羅金賢處長

五、出席人員：

國家通訊傳播委員會：吳銘仁簡任技正、蘇勇吉科長

中華軟協：楊蕙如組長、姚人鳳專員

安華聯網：洪光鈞總經理、劉建宗協理、鄭雯真協理

電子檢驗中心：宋孟曉經理、葉錫勳工程師

立德國際商品試驗：蕭經理

六、會議記錄：姚人鳳

七、會議結論：

(一)「檢測實驗室主管」資格要求

1.檢測實驗室主管之要求請依照原訂定標準不予變動。

2.品質主管之要求中「從事品質管理、專案管理或稽核關工作經驗 3 年以上」請更改為 2 年以上。

(二)檢測實驗室

1.請依照工業局辦法制訂試辦期間，建議 105/4/1~105/7/31 為試辦期、105/8/1~105/9/30 為 NCC 調整期、105/10/1 起正式執行，並於目前檢測實驗室要點辦法中，加訂試辦期間之資格要求。

2.檢測實驗室資格請依照安全等級區分訂立，L1 與 L2 為一種資格要求，L3 則另訂資格要求，而目前訂立之要求可列為 L1 和 L2

之內容。

(三)功能權限聲明之驗證

1.請定義出 L1 基礎型與 L2 進階型之 Slogan，讓民眾能清楚了解差異性。

2.在需 root 之檢測項目中(功能權限聲明之內容)，可維持於 L1，並將檢測方法進行區分為基礎型「未提供管理者權限之檢測方法」與進階型「使用管理者權限之檢測方法」，而檢測報告中於該檢測項目註記是否使用管理者權限手機檢測。

3.A.8.2 手機系統「關閉」內建軟體之功能檢測，因即便使用者關閉軟體後，手機背景程式依舊在執行，因此請將「關閉」替換其他更適當之用詞，避免造成誤解。

4.A.9.2 手機系統內建軟體背景執行之檢測，檢測方法若是使用廠商自我宣稱，請於判定標準中清楚明訂。

(四)後續執行

1.試測手機部分建議納入中低階手機，目前規劃之小米、HTC D728、Windows phone 640XL 屬中階手機，Sony Xperia z4、Samsung Galaxy s6 edge、iPhone 6 皆屬高階手機，低階手機部分請依時程再行考量(EX: ASUS、Infocus…等)。

2.L3 之晶片檢測內容請與 TTC 一同擇日與羅處長共同討論。

3.請於 12 月初前提供一支檢測手機之完整測試結果報告與羅處長討論。

4.期末報告中請包含工業局之檢測項目與 NCC 之檢測項目差異比對。

八、散會(下午 5 點 30 分)

104 年 NCC「手機系統內建軟體資安檢測」計畫

會議紀錄

一、會議名稱：第五次工作會議

二、時間：105 年 1 月 5 日(星期二) 09:30~12:10

三、地點：國家通訊傳播委員會(台北市濟南路二段 16 號 5 樓)

四、主席：國家通訊傳播委員會羅金賢處長

五、出席人員：

國家通訊傳播委員會：徐國根副處長、吳銘仁簡任技正、蘇勇吉科長、李福懿技正、程奕翔科員

中華軟協：楊蕙如組長、姚人鳳專員

安華聯網：洪光鈞總經理、林昱廷專案經理、陳漢平工程師

電子檢驗中心：宋孟曉經理、葉錫勳工程師

會議記錄：姚人鳳

六、會議結論：

(一)檢測項目之調整

1.檢測項目以各平台通用為原則，因此檢測項目(例：D.2.1)請修調技術要求之說明，以系統有呈現個資宣告並經使用者同意，即可代表通過，並不侷限於每個 APP 要個別索取使用者同意之條件，請重新檢視類似測項。

2.請將無法跨平台之檢測項目設計為 Level 2 之 option 檢測項目，例如檢測項目 A.8.2 與 A.9.2 請合併，併列為 option 項目，檢測項目 D.4.1、D.4.2、D.4.4、A.1.1、A.9.1 皆可考量納入 option 項目。

3.檢測項目 D.7.1 請將技術要求請修調為有備份功能即可之說明(本機備份或雲端備份)，則 windows 系統即可適用。

4.檢測項目 O.1.3 因 Windows 不支援該功能，可列為 windows 系統不適用之項目；檢測項目 P.5.1 可將 NFC 之檢測條件刪除；檢測項目 A.12.1 請設計為 3 個平台皆須於自我宣告進行說明。

5.自我宣告表請加入欄位讓廠商填寫手機衛星定位系統，並註記是否可雙向傳輸，作為後續參考使用。

(二)檢測實驗室要點之調整

1.請納入 CC 測試所需之檢測工具，並於報告簽屬人之證照要求增加「NCC 認可之資安證照」彈性化之說明文字，並於設備項目中列出清單。

2.試辦期內容請額外成為一份資料文件，並納入與 TAF 討論項目。

(三)檢測結果報告之調整

1.報告調整為結果摘要內容簡單扼要說明，詳細之檢測結果內容(如數據畫面等)皆放置報告之附件作為輔助說明，未來附件以外之內容可做為對外公告之版本。

(四)後續執行

1.邀請資策會共同討論規範及檢測實驗室要求，包含實驗室資格要點規定、試辦期間作法等。

2.邀請 TAF 共同討論特定服務計畫內容，包含現行檢測實驗室要點與 NCC 後續配合事項、試辦期間要求資格等。

3.規範依據前述要求修調完成後，再開一次工作會議進行全面性討論。

4.上述事項請於 1 月底以前完成。

七、散會(下午 12 點 10 分)

104 年 NCC「手機系統內建軟體資安檢測」計畫

會議紀錄

一、會議名稱：第六次工作會議

二、時間：105 年 1 月 12 日(星期二) 09:30~13:20

三、地點：國家通訊傳播委員會(台北市濟南路二段 16 號 5 樓)

四、主席：國家通訊傳播委員會羅金賢處長

五、出席人員：

國家通訊傳播委員會：徐國根副處長、吳銘仁簡任技正、蘇勇吉科長、李福懿技正、程奕翔科員

中華軟協：楊蕙如組長、姚人鳳專員

安華聯網：劉建宗協理

全國認證基金會：盛組長、林專員

會議記錄：姚人鳳

六、會議結論：

(一)檢測實驗室作業要點文句順修，結案時請提交資通設備與智慧型手持式行動臺之檢測實驗室管理作業要點合併版及分開版兩種版本。

(二)檢測實驗室資格請依照檢測項目區分 3 類作為能力分類。

(三)建議試辦期與正式資格準備作業同步進行，6/1~9/30 訂立為試辦期，4/1~5/31 NCC 須完成委員會審定程序，內容包含：檢測技術規範、試辦期說明文件、實驗室作業要點及審驗作業要點等文件；檢測實驗室於試辦期即可進行申請，自 6/1 起同步由 TAF 協助配合特定服務計畫之修訂，待完成即可開放檢測實驗室正式資格申請，並統一訂於 10/1 生效，於試辦期通過 NCC 與 TAF 認可之檢測實驗室於試辦期間

同時申請正式資格之檢測實驗室。

七、散會(下午 1 點 20 分)

國家通訊傳播委員會「手機系統內建軟體資安檢測計畫」交流討論會議紀錄

一、**時間**：105 年 1 月 21 日(星期四) 上午 9 時 30 分

二、**地點**：通傳會 2 樓會議室(台北市濟南路二段 16 號 2 樓)

三、**主持人**：通傳會羅金賢處長　　記錄：姚人鳳

四、**出席人員**：

通傳會：徐國根副處長、蘇勇吉科長、李福懿技正、程奕翔科員

中華軟協：楊蕙如組長、姚人鳳專員

安華聯網：黃光鈞總經理、林昱廷專案經理

資策會：林主任、林組長、汪經理

五、**報告事項**：

(一) 行動應用 App 基本資安規範辦理情形(資策會報告，略)。

(二) 手機系統內建軟體資安檢測計畫委託研究案辦理情形(中華軟協報告，略)

六、**結論**：

(一) 請中華軟協將手機系統內建軟體資安檢測實驗室資格分類由 3 類簡化為 2 類，並研議修正之類別名稱。有關實驗室之專業能力要求，須將檢測方法及設備等 check list 納入檢測實驗室管理作業要點，以利後續實驗室資格認可。

(二) 請中華軟協將手機系統內建軟體資安檢測項目之非必測項目名稱改為選測項目。

(三) 請中華軟協於本案結案報告中建議如何推廣手機系統內建軟體資安檢測，如建議政府採購之手機均須通過手機系統內建軟體資安檢測技術規範。

(四) 請中華軟協及資策會合力比對雙方檢測項目及內容文字(如：將相同檢測內容之文字調整為一致)，以避免混淆，並提供比對結果作為後續參考。

(五) 有關經濟部工業局行動應用 APP 資安規範之參考項目為檢測實

驗室無須檢測項目，本會建議工業局將前揭參考項目改為選測項目，並讓 APP 廠商得自行選擇檢測，如有檢測，則將檢測結果重點公開。

(六) 請中華軟協與資策會參考工業局作法，研議比照由「行動應用資安聯盟」辦理手機系統內建軟體資安檢測驗證及標章管理之可行性。

(七) 請中華軟協與資策會針對手機系統內建軟體資安檢測實驗室及行動應用 APP 資安規範檢測實驗室之資格，研議相互認可之可行性。

(八) 有關工業局規劃試辦實驗室於試辦期所核發之行動應用 APP 認證證書有效期為 1 年，請中華軟協研議規劃試辦手機系統內建軟體資安檢測報告及認證證書有效性之執行細節。

七、**散會** (下午 12 點 00 分)

國家通訊傳播委員會「手機系統內建軟體資安檢測計畫」交流討論會議紀錄

一、**時間**：105 年 2 月 3 日(星期三) 下午 4 時 40 分

二、**地點**：通傳會 2 樓會議室(台北市濟南路二段 16 號 2 樓)

三、**主持人**：通傳會羅金賢處長　　記錄：姚人鳳

四、**出席人員**：

通傳會：徐國根副處長、蘇勇吉科長、李福懿技正、程奕翔科員

中華軟協：楊蕙如組長、姚人鳳專員

安華聯網：劉建宗協理、林維展工程師

電子檢驗中心：宋孟曉經理、葉錫勳工程師

五、**會議結論**：

(一) 規範與檢測報告同步修改：

1. 檢測規範與檢測報告請同步將「技術要求編號」改為「類別」,「技術要求」改為「檢測項目」,「檢測項目」改為「檢測細項」，將檢測細項之編號增加 H/M/C 辨識安全等級高/中/普。
2. 請將檢測項目(原技術要求)中的文字說明精簡化，並同步修改至檢測實驗室作業要點之附件。
3. 安全等級「累進式」請詳述使閱讀者容易理解。
4. 請將「出廠預載程式、銷售商加載程式、無圖示程式」之程式改為軟體。
5. 刪除檢測範圍(第 1 類至第 3 類)，僅區分 3 種安全等級。

(二) 檢測報告請修改：

1. 檢測報告摘要及表 1 受檢設備受測目標資訊蒐集基本資訊檢測結果中，「廠牌名稱」改為「廠牌」,「廠牌型號」改為「型號」，檢測等級同步規範改為「普級/中級/高級」,「實驗室主管」改為「技術主管」並同步調整於檢測實驗室作業要點。

2. 將表 2 檢測結果摘要的檢測設備統一改為檢測儀器，並將 2.2 檢測儀器進行編碼，表 2.2 檢測儀器欄位同步對應其編碼。
3. 表 1 系統內建軟體數量請區分廠商自我宣告結果及實際查檢結果，表 1 名稱改為「受檢設備基本資訊檢測結果」。
4. 自我宣告表之說明移至 3.項目中，並將表 4 名稱改為「自我宣告表」。
5. 請增加測項與受測 APP 編號的對應總表。

(三) 規範內容請修改：

1. A12.1 具安全疑慮之 URL，由於該測項因網頁弱點掃描將關係到(1)Google 商之 server(2)通訊商之 server(3)第三方軟體開發商之 server，若執行此部分測項將關係到網頁伺服器檢測，會依使用工具不同而造成檢測通過與否，無法明確判定是否通過，且檢測範圍已超出手機本身範疇，非經同意進行網頁弱掃恐有被判定攻擊之疑慮，因此刪除此測項。
2. 檢測項目細項須檢測無圖示軟體者，請增列入中級選測項目中，並於規範中另起章節說明選測項目。

(四) 檢測實驗室作業要點，請將資通設備安全檢測實驗室與手持式行動臺資通設備安全檢測實驗室分 2 份文件撰寫。

(五) 檢測實驗室區分兩種為：第 1 型與第 2 型。

(六) 請設計安全等級標章。

六、**散會** (下午 7 點 40 分)

國家通訊傳播委員會「手機系統內建軟體資安檢測計畫」交流討論會議紀錄

一、**時間**：105 年 2 月 17 日(星期三) 下午 4 時 30 分

二、**地點**：通傳會 2 樓會議室(台北市濟南路二段 16 號 2 樓)

三、**主持人**：通傳會羅金賢處長　　記錄：姚人鳳

四、**出席人員**：

通傳會：蘇勇吉科長、李福懿技正、程奕翔科員

中華軟協：楊蕙如組長、姚人鳳專員

安華聯網：洪光鈞總經理

電子檢驗中心：宋孟曉經理、葉錫勳工程師

五、**會議結論**：

(一) 技術規範草案內容細部修改並定案

(二) 檢測實驗室作業要點內容細部修改並定案

六、**散會** (下午 8 點 30 分)