遙控無人機資安檢測規範

數位發展部　交通部
中華民國　113 年 12 月 1 日

版本修改紀錄

版本	日期	摘要
v1.0	2024/11/14	依據交通部113年11月14日修正發布「遙控無人機管理規則」修訂

1. 法令依據

依遙控無人機管理規則第17條、第31條及第32條規定訂定之。

2. 適用範圍

本規範適用於「遙控無人機管理規則」(下稱管理規則)之遙控無人機資安檢測及遙控無人機群飛系統資安檢測，申請者視需求可個別選擇測試。

(1)第6章為遙控無人機資安檢測，係依據管理規則第17條、第31條及第32條規定之需求，針對遙控無人機與地面控制站制訂資安檢測項目。

(2)第7章為遙控無人機群飛系統資安檢測，係依據管理規則第32條規定之需求，針對遙控無人機群飛系統制訂安全要求，基於風險管理角度進行系統資安防護評估。

(3)第8章為遙控無人機資安檢測之增項測試，針對遙控無人機與地面控制站增訂一般安全要求與特殊安全要求，由申請者依其需求選測。

第6章遙控無人機資安檢測範圍如圖1所示，包含實線方框內遙控無人機之飛行控制系統、通訊模組，以及地面控制站(含 APP)與實線表示之通訊介面，其中虛線表示之定位資訊來源、通訊介面及其定位模組則不在第6章適用範圍。

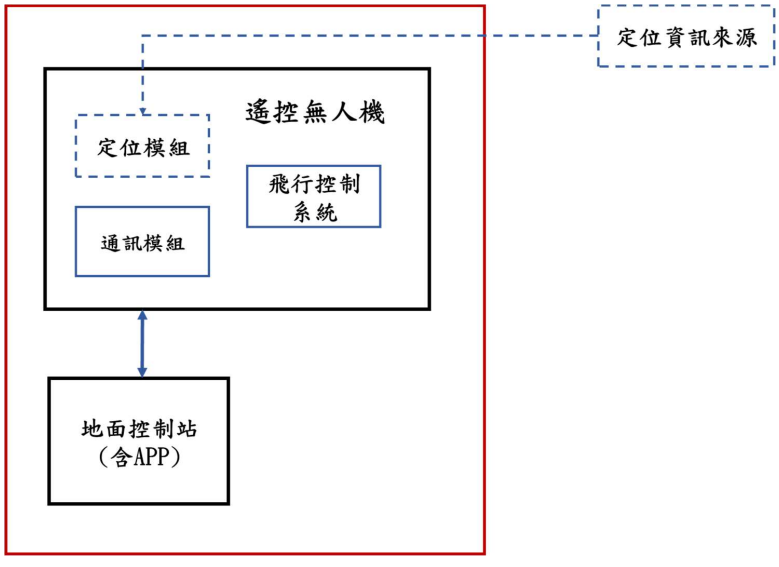

圖 1、第6章適用範圍

遙控無人機酬載係遙控無人機為執行任務外加裝備，如巡檢、群飛等活動，其產生之資料不會輸出至飛行控制系統，爰未列入第6章適用範圍，建議具連網功能之酬載設備可參考業界常用之相關資安標準（詳見表1），亦可透過取得財團法人全國認證基金會依前揭資安標準認可之資安檢測實驗室執行資安測試，取得測試報告或檢測通過證明，以強化遙控無人機資安防護作為。

表 1、酬載設備資安測試建議參考標準

具連網功能酬載類型	資安標準
網路攝影機	「影像監控系統安全－第1部：一般要求事項」(標準總號：CNS 16120-1)
無線寬頻設備	TAICS TS-0040 v1.0-無線寬頻分享器資安標準 TAICS TS-0041 v1.0-無線寬頻分享器資安測試規範
其他連網設備	TAICS TS-0045 v1.0-消費性物聯網產品資安標準 TAICS TS-0046 v1.0-消費性物聯網產品資安測試規範

第7章遙控無人機群飛系統資安檢測範圍如圖2所示，包含紅色實線圓框內遙控無人機之「具網路連線能力之酬載」與遙控無人機群飛系統地面控制站之「交換器」、「路由器」、「防火牆」及「其他設備（如無線寬頻分享器等）」，並包含紅色實線框與紅色實線如設備具有「網頁管理介面」及「無線通訊介面」等附加功能介面，若無該設備或介面者則該項免測。

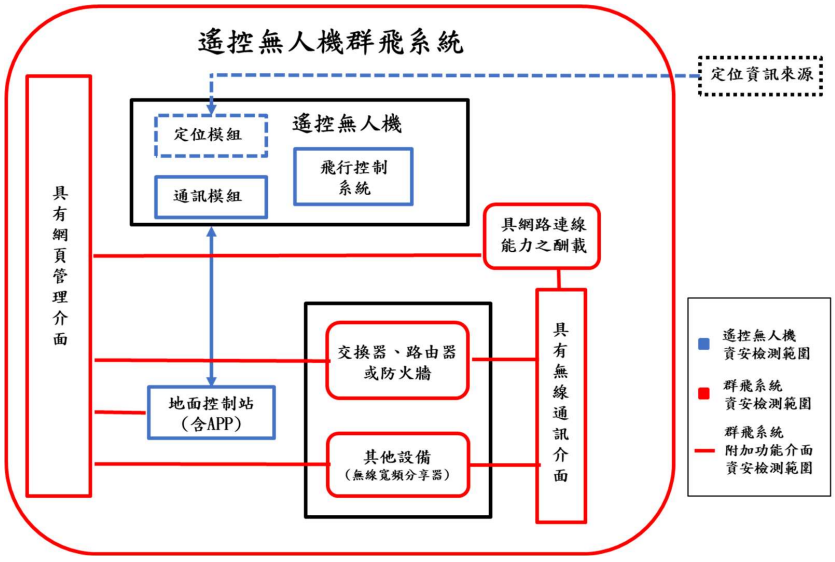

圖2、第7章適用範圍

第8章遙控無人機資安檢測之增項測試範圍如圖3所示，包含實線方框內遙控無人機之飛行控制系統、定位模組、通訊模組、定位模組，以及地面控制站（含 APP）與實線表示之通訊介面，其中虛線表示其定位資訊來源不在第8章適用範圍。

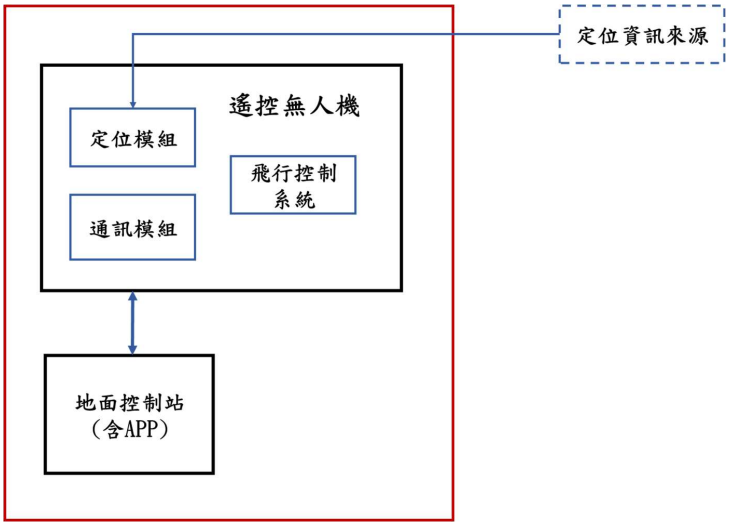

圖 3、第8章適用範圍

3. 引用標準

下列標準為本規範所引用，亦成為本規範之一部分。

標準編號	標準名稱
TAICS TR-0022 v2.0	物聯網場域資安防護評估指引 v2
TAICS TS-0041 v1.0	無線寬頻分享器資安測式規範
ANSI/CTA-2088-A	Baseline Cybersecurity Standard for Devices and Device Systems
ANSI/CTA -2088.1	Baseline Cybersecurity for Small Unmanned Aerial Systems
ANSI/CAN/UL 2900-1	Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations
U.S. Department of Homeland Security CISA	Protecting against the threat of unmanned aircraft system (UAS)
U.S. Department of Homeland Security CISA	Cybersecurity best practices for operating commercial unmanned aircraft systems (UASS)
U.S. Department of Homeland Security CISA	Secure Your Drone Privacy and Data Protection Guidance
U.S. Department of Homeland Security CISA	Be Air Aware UAS Cybersecurity
Association for Uncrewed Vehicle Systems International (AUVSI)	Green UAS Frameworks

4. 用詞及定義

本規範之用詞及定義如下：

4.1.遙控無人機（drone or unmanned aerial vehicle）

本規範所稱「遙控無人機」，指自遙控設備以信號鏈路進行飛航控制，或以自動駕駛操作，或其他經交通部民用航空局公告之無人航空器。

4.2.飛行控制系統（flight control system）

飛行控制系統為遙控無人機運作之核心，其主要功能包括執行起飛、航行及降落等動作。

4.3.地面控制站（ground control station）

大部分位於地面，用來控制遙控無人機飛行的軟硬體整合系統，包含通訊系統及應用程式等。此處地面控制站係指與遙控無人機之間建立命令與控制連結（Command & Control Link, C2 Link），且具上行與下行鏈路之地面控制站，並可預先設定遙控無人機飛行路徑以執行飛行任務。地面控制站應用程式亦可採行動應用 APP 之形式，惟其通訊架構需符合上述條件。如行動應用 APP 未具上述形式或無法設定執行任務飛行模式，而僅作為影像傳輸之用，則非屬本項定義之地面控制站應用程式。

4.4.遙控無人機系統（unmanned aerial system）

由遙控無人機、地面控制站、通訊系統及其相關應用程式等組合而成，可執行飛行任務的系統。

4.5.通用漏洞評分系統（common vulnerability scoring system, CVSS）

由資安事件應變小組論壇（Forum of Incident Response and Security Teams, FIRST）提供的漏洞評分系統，以衡量軟體漏洞的特徵和嚴重性進行評分，目前發展至第3版。

4.6.受測物（unit under test）

本規範所稱受測物為待測之軟體、韌體、硬體、系統或通訊協定等之統稱。

備註：

用詞及定義參考來源：

遙控無人機	https://www.caa.gov.tw/Article.aspx?a=3718&lang=1（交通部民用航空局）
飛行控制系統	https://www.caa.gov.tw/Article.aspx?a=3718&lang=1（交通部民用航空局）
地面控制站	https://www.faa.gov/documentlibrary/media/notice/n_8900.227.pdf（美國聯邦航空總署, FAA）
遙控無人機系統	https://www.faa.gov/faq/what-unmanned-aircraft-system-uas（美國聯邦航空總署, FAA）
通用漏洞評分系統	https://nvd.nist.gov/vuln-metrics/cvss（美國國家標準暨技術研究院, NIST）
受測物	https://www.3gpp.org/（3GPP, 第3代合作夥伴計劃）

5. 原文縮寫對照

縮寫	完整名稱	中文意思
AES	Advanced Encryption Standard	進階加密標準
ANSI	American National Standards Institute	美國國家標準協會
APP	Application	應用程式
CAN	Controller Area Network	控制器區域網路
CCMP	Counter Mode with CBC-MAC Protocol	計數器模式密碼塊鏈消息完整碼協議
CISA	Cybersecurity & Infrastructure Security Agency	美國網路安全與基礎設施安全機構
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
CVSS	Common Vulnerability Scoring System	通用漏洞評分系統
ETSI	European Telecommunications Standards Institute	歐洲電信標準協會
FAA	Federal Aviation Administration	美國聯邦航空總署
FIRST	Forum of Incident Response and Security Teams	資安事件應變小組論壇
HTTP	HyperText Transfer Protocol	超文本傳輸協定
IEEE	Institute of Electrical and Electronics Engineers	電機電子工程師學會
NIST	National Institute of Standards and Technology	美國國家標準暨技術研究院
RDP	Remote Desktop Protocol	遠端桌面通訊協定
OWASP	Open Web Application Security Project	開放式 Web 應用程式安全計畫
TAICS	Taiwan Association of Information and Communication Standards	台灣資通產業標準協會
TCP	Transmission Control Protocol	傳輸層控制協定
TLS	Transport Layer Security	傳輸層安全協議
UAS	Unmanned Aircraft System	無人機系統
UASS	Unmanned Aircraft Systems	無人機系統
UDP	User Datagram Protocol	使用者資料包通訊協定
UL	UL Standards	美國產品評估標準
UPnP	Universal Plug and Play	通用隨插即用
USB	Universal Serial Bus	通用序列匯流排
SMB	Server Message Block	網路檔案共享系統
SP	Special Publication	特別出版
WPA2	Wi-Fi Protected Access 2	Wi-Fi 存取保護加密協定
WPS	Wi-Fi Protected Setup	Wi-Fi 保護設定
3GPP	The 3rd Generation Partnership Project	全球行動通訊標準組織第三代合作夥伴計畫

6. 遙控無人機資安檢測

本章節係依據「遙控無人機管理規則」第17條第1項「遙控無人機之製造者或進口者於公開販售前，應於民航局指定資訊系統登錄下列事項：……五、數位發展部公告之專業機構或法人出具符合數位發展部會銜交通部訂定之遙控無人機資安檢測規範之遙控無人機資安檢測合格報告。」，及第31條第6項之「……，政府機關(構)、學校或法人從事第一項及第二項飛航活動所使用裝置導航設備之遙控無人機，應符合下列規定：一、應具有數位發展部公告之專業機構或法人所出具符合數位發展部會銜交通部訂定之遙控無人機資安檢測規範之遙控無人機資安檢測合格報告。……」之規定，以及第32條第4項之「……，政府機關(構)、學校或法人從事第一項飛航活動所使用裝置導航設備之遙控無人機，應符合下列規定：一、應具有數位發展部公告之專業機構或法人所出具符合數位發展部會銜交通部訂定之遙控無人機資安檢測規範之遙控無人機資安檢測合格報告。……」之規定，訂定相關測試項目。

6.1.安全要求

本節遙控無人機資安檢測係強化遙控無人機遭惡意使用或資料外洩的安全防護，其內容包含遙控無人機基本安全要求，主要針對身分鑑別、異常流量、軟體弱點、惡意程式及通訊安全，提供強化遙控無人機遭惡意使用或資料外洩的安全防護。

遙控無人機及地面控制站系統之檢測項目詳見表2，該表第1欄位為安全構面，內容包含系統安全、軟體安全、通訊安全、韌體安全，第2欄位為安全要求項目，第3欄位為遙控無人機，第4欄位為地面控制站。第3欄位及第4欄位所需檢測之安全要求項目以符號V表示。

表 2、遙控無人機及地面控制站之系統檢測項目表

安全構面	安全要求項目		遙控無人機	地面控制站
6.2系統安全	6.2.1	身分鑑別		V
	6.2.2	網路服務埠檢測		V
	6.2.3	系統異常流量	V	V
6.3軟體安全	6.3.1	惡意程式		V
	6.3.2	弱點掃描		V
6.4通訊安全	6.4.1	無線通訊安全	V	V
6.5韌體安全	6.5.1	韌體更新安全	V	

備註：本表以「V」標示表示對應之檢測項目

6.2.系統安全檢測

此節主要針對遙控無人機與地面控制站安全進行檢測，包含身分鑑別與存取控制、網路服務埠檢測及系統異常流量等面向。

6.2.1. 身分鑑別

6.2.1.1. 測試目的

查驗地面控制站之身分鑑別機制與通行碼強度是否具備防止暴力破解的能力，以及具備錯誤鎖定之防護功能。

6.2.1.2. 測試方法

(1) 於受測物登入介面輸入錯誤登入資訊。

(2) 連續輸入錯誤達廠商自我宣告次數，確認是否具有鎖定機制，於一定時限內不可再進行登入驗證。

(3) 登入受測物所使用的通行碼，且通行碼設置規則應具備高複雜度（符合8碼以上長度，且包含大小寫字母、特殊符號、數字設定），身分鑑別機制亦可採用生物特徵。

6.2.1.3. 判定標準：符合下列項目者為通過，否則為未通過

(1) 受測物須提供身分鑑別機制，如：每次登入需輸入帳號及通行碼(包含生物特徵)。

(2) 於受測物登入介面輸入錯誤登入資訊時，具有錯誤鎖定功能。

(3) 受測物通行碼具備高複雜度（符合8碼以上長度，且包含大小寫字母、特殊符號、數字設定）。

6.2.2. 網路服務埠檢測

6.2.2.1. 測試目的

確保地面控制站沒有存在非預期之網路服務埠。

6.2.2.2. 測試方法

(1) 將測試設備連接受測物，啟用受測物廠商所宣告之網路服務。

(2) 使用網路埠掃描工具，對受測物執行 TCP 與 UDP 之0～65535埠之掃描。

(3) 核對掃描結果所呈現之網路服務與對應埠。

(4) 比對受測物送審資料中所聲明之網路服務與對應埠。

6.2.2.3. 判定標準：符合下列項目者為通過，否則為未通過

受測物所開啟之網路服務與對應埠，與送測資料之內容相符。

6.2.3. 系統異常流量

6.2.3.1. 測試目的

確保遙控無人機與地面控制站之通訊無異常流量存在。

6.2.3.2. 測試方法

(1) 對受測物進行系統最大運行時間或至少24小時的流量側錄。

(2) 比對側錄結果是否與廠商宣告之對外連線對象相符。

6.2.3.3. 判定標準：符合下列項目者為通過，否則為未通過

與廠商宣告之對外連線對象相符。

6.3.軟體安全檢測

此節主要針對地面控制站之軟體安全進行檢測，遙控無人機如有適用項目亦可參考選測，包含惡意程式、弱點掃描等面向。

6.3.1. 惡意程式

6.3.1.1. 測試目的

確保地面控制站無惡意程式。

6.3.1.2. 測試方法

使用惡意程式檢測工具進行完整系統掃描。

6.3.1.3. 判定標準：符合下列項目者為通過，否則為未通過

未發現惡意程式。

6.3.2. 弱點掃描

6.3.2.1. 測試目的

查驗地面控制站是否具有 CVE 常見已知高風險漏洞，及是否為 CISA 所記載之可利用漏洞。

6.3.2.2. 測試方法

(1) 將測試電腦連接受測物。

(2) 使用具管理者權限之身分，透過具作業系統、裝置、應用程式評估之弱點掃描工具，對受測物進行弱點掃描。

(3) 查驗該弱點掃描工具所產生之報告，確認是否存有 CVSS 基礎評分7.0以上(含7.0)之重大、高風險等級漏洞，且該漏洞為是否為CISA所記載之可利用漏洞。

6.3.2.3. 判定標準：符合下列項目者為通過，否則為未通過

(1) 受測物弱點掃描報告不應存有 CVSS 基礎評分7.0以上(含7.0)之重大、高風險等級漏洞。

(2) 受測物掃描結果之 CVSS 基礎評分7.0以上(含7.0)弱點項目非為 CISA 所記載之可利用漏洞。

(3) 當檢測出之資安風險漏洞以其所具CVSS最新版本之評分為依據。

6.4.通訊安全檢測

此節適用於檢測遙控無人機與地面控制站間之通訊，包含無線通訊安全等測試項目。

6.4.1. 無線通訊安全

6.4.1.1. 測試目的

遙控無人機與地面控制站之間使用之無線通訊傳輸應加密，且應使用符合國際或區域標準規範（例如：3GPP、ETSI、IEEE 等或其他相當標準規範）所採用之加密方式。

6.4.1.2. 測試方法

(1) 查驗無線通訊使用符合國際或區域標準加密方式之規格文件。

(2) 若無線通訊使用 IEEE 802.11協定，則使用安全通道檢測工具或網路封包檢測是否使用 WPA2或以上版本之加密方式。

(3) 倘若無法對送測之遙控無人機使用之無線通訊傳輸進行加密，將確認其使用手冊或包裝外盒是否有明確說明無線通訊傳輸未加密造成之資安風險。

6.4.1.3. 判定標準：符合下列項目之一者為通過，否則為未通過

(1) 無線傳輸使用符合國際規範之加密機制。

(2) 如無法對送測遙控無人機使用之無線傳輸進行加密，使用手冊或包裝外盒有明確說明無線通訊傳輸未加密造成之資安風險。

6.5.韌體安全檢測

此節主要為遙控無人機之韌體更新安全要求檢測項目。

6.5.1. 韌體更新安全

6.5.1.1. 測試目的

查驗飛控模組是否具備韌體更新機制，並確認韌體有無驗證防止被置換之能力。

6.5.1.2. 測試方法

(1) 依據廠商使用說明文件中所提供之韌體安全更新方法進行更新，或請廠商提供相關安全更新方法之佐證資訊。

(2) 查驗受測物是否具備更新功能。

6.5.1.3. 判定標準：符合下列項目者為通過，否則為未通過

(1) 韌體具備更新功能。

(2) 韌體如具線上韌體更新管道，來源應提供與下載韌體一致之校驗碼(Checksums)供查核。

(3) 韌體更新具驗證防止被置換之能力。

7. 遙控無人機群飛系統資安檢測

本章節係依據「遙控無人機管理規則」第32條第1項後段之「……；同一時間控制二百架以上遙控無人機進行展演活動，應檢附數位發展部公告之專業機構或法人所出具符合數位發展部會銜交通部訂定之遙控無人機資安檢測規範之遙控無人機群飛系統資安檢測合格報告。」，訂定相關測試項目。

遙控無人機群飛系統（以下簡稱群飛系統）包含遙控無人機、地面控制站及具網路連線能力之設備等，其資安檢測適用安全要求項目，涵蓋弱點掃描、資料傳輸加密、機敏資訊保護、通行碼防護機制、網頁應用程式安全、授權機制、身分鑑別機制、安全的通訊方式、實體防護要求等面向之安全要求項目，如表3，其中群飛系統具備之設備所對應安全要求項目，以符號V表示。

表 3、遙控無人機群飛系統之安全要求項目表

安全構面	安全要求項目		遙控無人機群飛系統						
			遙控無人機設備		群飛系統地面控制設備				
			遙控無人機	具有網路連線能力之酬載	地面控制站	具有交換器、路由器或防火牆	其他設備（無線寬頻分享器）	具有無線通訊介面	具有網頁管理介面
6.2 系統安全	6.2.1	身分鑑別	-	-	V	-	-	-	-
	6.2.2	網路服務埠檢測	-	-	V	-	-	-	-
	6.2.3	系統異常流量	V	-	V	-	-	-	-
6.3 軟體安全	6.3.1	惡意程式	-	-	V	-	-	-	-
	6.3.2	弱點掃描	-	-	V	-	-	-	-
6.4 通訊安全	6.4.1	無線通訊安全	V	-	V	-	-	-	-

安全構面	安全要求項目		遙控無人機群飛系統						
			遙控無人機設備		群飛系統地面控制設備				
			遙控無人機	具有網路連線能力之酬載	地面控制站	具有交換器、路由器或防火牆	其他設備（無線寬頻分享器）	具有無線通訊介面	具有網頁管理介面
6.5 韌體安全	6.5.1	韌體更新安全	V	-	-	-	-	-	-
7.1 群飛系統安全	7.1.1	群飛系統弱點檢測	-	V	-	V	V	-	-
	7.1.2	群飛系統網路服務埠	-	V	-	V	V	-	-
	7.1.3	群飛系統遠端登入存取管理	-	V	-	V	V	-	-
	7.1.4	群飛系統遠端登入存取內容保護	-	V	-	V	V	-	-
	7.1.5	群飛系統高風險服務功能管理	-	V	-	V	V	-	-
	7.1.6	群飛系統網頁應用程式檢測	-	-	-	-	-	-	V
	7.1.7	群飛系統身分驗證機制	-	V	-	V	V	-	-
	7.1.8	群飛系統使用者通行碼強度與防護	-	V	-	V	V	-	-

安全構面	安全要求項目		遙控無人機群飛系統						
			遙控無人機設備		群飛系統地面控制設備				
			遙控無人機	具有網路連線能力之酬載	地面控制站	具有交換器、路由器或防火牆	其他設備（無線寬頻分享器）	具有無線通訊介面	具有網頁管理介面
	7.1.9	群飛系統網頁傳輸安全管理	-	-	-	-	-	-	V
	7.1.10	群飛系統網頁使用授權管理	-	-	-	-	-	-	V
	7.1.11	群飛系統無線網路通訊安全	-	-	-	-	-	V	-
	7.1.12	群飛系統實體安全防護	-	V	-	V	V	-	-

7.1.群飛系統安全檢測

7.1.1. 群飛系統弱點檢測

7.1.1.1. 測試目的

查驗受測物是否具有 CVE 常見已知高風險漏洞，及是否為 CISA 所記載之可利用漏洞。

7.1.1.2. 測試方法

(1) 使用具管理者權限之身分，透過具系統漏洞與設定評估之弱點掃描工具，對受測物進行弱點掃描。

(2) 確認受測物弱點掃描報告是否存有 CVSS 基礎評分7.0以上(含7.0)之重大、高風險等級漏洞。

(3) 確認 CVSS 基礎評分7.0以上(含7.0)之重大、高風險等級漏洞是否為 CISA 所記載之可利用漏洞。

7.1.1.3. 判定標準：符合下列項目者為通過，否則為未通過

(1) 受測物弱點掃描報告不應存有 CVSS 基礎評分7.0以上(含7.0)之重大、高風險等級漏洞。

(2) 受測物掃描結果之 CVSS 基礎評分7.0以上(含7.0)弱點項目非為 CISA 所記載之可利用漏洞。

(3) 當檢測出之資安風險漏洞以其所具 CVSS 最新版本之評分為依據。

7.1.2. 群飛系統網路服務埠

7.1.2.1. 測試目的

查驗受測物是否存在預期以外的網路服務埠。

7.1.2.2. 測試方法

(1) 使用網路服務埠掃描工具進行測試。

(2) 透過送測者提供之宣告使用網路服務埠資訊進行檢核。

(3) 如具非預期之網路服務埠須與受測單位確認是否為必要之服務功能需求。

7.1.2.3. 判定標準：符合下列項目者為通過，否則為未通過

受測物啟用之網路服務埠皆為群飛系統服務所需。

7.1.3. 群飛系統遠端登入存取管理

7.1.3.1. 測試目的

查驗具備遠端登入存取功能之受測物，是否使用不安全的傳輸存取服務。

7.1.3.2. 測試方法

(1) 查驗受測物網路服務埠之服務資訊描述是否存有常見 Telnet、FTP 網路服務埠，或非常見網路服務埠具有 Telnet、FTP 相關服務資訊描述。

(2) 透過終端連線工具連接（1）所發現之網路服務埠進行確認。

7.1.3.3. 判定標準：符合下列項目者為通過，否則為未通過

受測物未使用 Telnet、FTP 之不安全傳輸存取服務。

7.1.4. 群飛系統遠端登入存取內容保護

7.1.4.1. 測試目的

查驗受測物是否啟用遠端連線傳輸服務，且傳輸內容是否具有機敏資訊、身分驗證及是否採用安全加密通道演算法。

7.1.4.2. 測試方法

(1) 查驗受測物網路服務埠之服務資訊描述是否存有 SSH、RDP 或 SMB 網路服務埠。

(2) 如具備啟用如 SSH 遠端連線傳輸服務，確認是否採用具符合 NIST SP 800-140C 最新版本所核可或同等強度之加密演算法。

(3) 如具備啟用如 RDP 或 SMB 等遠端連線傳輸服務，需確認內容是否具有機敏資訊及身分驗證機制。

7.1.4.3. 判定標準：符合下列項目者為通過，否則為未通過

受測物無啟用遠端連線傳輸服務（SSH、RDP 及 SMB）、受測物傳輸內容之資訊不具有機敏性或受測物採用安全加密通道演算法。

7.1.5. 群飛系統高風險服務功能管理

7.1.5.1. 測試目的

查驗受測物是否啟用具備高風險之服務功能。

7.1.5.2. 測試方法

(1) 連接至受測物之管理介面。

(2) 查驗受測物是否開啟 UPnP 或 WPS 服務功能。

7.1.5.3. 判定標準：符合下列項目者為通過，否則為未通過

受測物未具備、未啟用或已關閉高風險之服務功能。

7.1.6. 群飛系統網頁應用程式檢測

7.1.6.1. 測試目的

查驗具備網頁管理介面服務之受測物，是否存在常見的最新版本 OWASP Top 10網頁應用程式之高風險且可利用之弱點。

7.1.6.2. 測試方法

(1) 使用具管理者權限之身分，透過網頁應用程式弱點掃描工具進行測試。

(2) 確認受測物是否存在最新版本 OWASP Top 10網頁應用程式之高風險且可利用之弱點。

7.1.6.3. 判定標準：符合下列項目者為通過，否則為未通過

受測物未存在最新版本 OWASP Top 10網頁應用程式之高風險且可利用之弱點。

7.1.7. 群飛系統身分驗證機制

7.1.7.1. 測試目的

查驗受測物是否具備身分驗證機制。

7.1.7.2. 測試方法

連接至受測物通訊傳輸介面，確認受測物是否具有通行碼或多因子等身分認證機制，並提供佐證資料進行查核。

7.1.7.3. 判定標準：符合下列項目者為通過，否則為未通過

受測物具有身分驗證機制。

7.1.8. 群飛系統使用者通行碼強度與防護

7.1.8.1. 測試目的

查驗具備通行碼驗證介面之受測物，是否具備使用者通行碼強度與防護機制。

7.1.8.2. 測試方法

(1) 進行登入或更換受測物所使用的通行碼，確認是否具備如下其中一項複雜度規則：

- 通行碼採以8個字元長度以上，且通行碼包含英文大寫字元、英文小寫字元、數字字元以及特殊符號字元其中三項以上字元類型。
- 通行碼採以15個字元長度以上，且通行碼不為完全重複或固定單一規則之類型。

(2) 透過已知使用者名稱並搭配常見通行碼，對受測物進行手動測試或字典檔攻擊。

(3) 查驗是否未提供錯誤鎖定機制，如：通行碼輸入錯誤超過廠商設定次數後，帳號是否進行鎖定。

7.1.8.3. 判定標準：符合下列項目者為通過，否則為未通過

受測物具有其他非通行碼驗證方式，或受測物具備使用者通行碼複雜度與防護機制。

7.1.9. 群飛系統網頁傳輸安全管理

7.1.9.1. 測試目的

查驗具備網頁管理介面之受測物，是否具備傳輸安全管理。

7.1.9.2. 測試方法

(1) 查驗受測物是否啟用 HTTP Method 中 PUT、TRACE 及 DELETE 功能。

(2) 查驗受測物是否未使用加密傳輸協定，或使用不安全的加密協定，如：TLSv1.1或查驗過程可降回 HTTP。

7.1.9.3. 判定標準：符合下列項目者為通過，否則為未通過

(1)受測物未啟用 HTTP Method 中 PUT、TRACE 及 DELETE 功能。

(2)受測物啟用 TLSv1.2以上之加密傳輸協定或受測物未啟用網頁管理介面。

7.1.10. 群飛系統網頁使用授權管理

7.1.10.1.測試目的

查驗具備網頁管理介面之受測物，是否具備使用授權管理機制。

7.1.10.2.測試方法

(1) 透過檢測工具確認受測物之網頁管理介面是否存在目錄跨越弱點(Directory Traversal)之頁面存在。

(2) 依照管理介面設置不同功能權限，使用具權限與非具權限之身分，對受測物進行權限操作之差異測試。

(3) 對受測物之網頁管理介面測試存取未經授權的頁面，如後台管理頁面、設定及新增資訊頁面等，是否皆具有權限要求。

7.1.10.3.判定標準：符合下列項目者為通過，否則為未通過

受測物具備頁面使用授權權限管理機制或受測物未啟用網頁管理介面。

7.1.11. 群飛系統無線網路通訊安全

7.1.11.1.測試目的

查驗受測物之無線網路通訊是否採用安全加密傳輸連線。

7.1.11.2.測試方法

(1) 具 Wi-Fi 傳輸連線之受測物，查驗是否使用 WPA2以上版本並且使用 AES 加密(Counter Mode with CBC-MAC Protocol, CCMP)模式。

(2) 具非 Wi-Fi 傳輸連線之受測物，採用書面審查檢視是否具加密傳輸模式。

7.1.11.3.判定標準：符合下列項目者為通過，否則為未通過

(1) 具 Wi-Fi 傳輸連線之受測物，採用 WPA2以上版本並且使用 AES 加密(Counter Mode with CBC-MAC Protocol, CCMP)模式或同等以上加密強度。

(2) 非 Wi-Fi 傳輸連線之受測物，具加密傳輸模式。

7.1.12. 群飛系統實體安全防護

7.1.12.1.測試目的

查驗受測物是否具有實體保護機制，以防可透過該受測物產生可能造成損害之風險。

7.1.12.2.測試方法

(1) 查驗群飛系統之網路或實體裝置的對外接入點是否具有限制存取機制，如：USB埠、RJ45埠、無線傳輸等，是否具有裝置本體、群飛系統內部或外部安全保護機制。

(2) 透過送測者提供之宣告實體安全保護機制資訊檢核是否與實際相符。

7.1.12.3.判定標準：符合下列項目者為通過，否則為未通過

受測物具有實體安全保護機制。

8. 遙控無人機資安檢測增項測試

本章節為選測，係配合遙控無人機政府採購案、軍用商規採購案等資安需求，參酌「無人機資安保障規範」v2.0版（下稱保障規範）之中階測試項目，訂定增項測試之8.1一般安全要求，及參酌保障規範之高階測試項目，訂定增項測試之8.2特殊安全要求，送測者得依需求選測本章節檢測項目。

8.1.一般安全要求

如欲申請8.1一般安全要求增項檢測，須搭配第6章進行檢測。

遙控無人機及地面控制站系統之一般安全要求增項詳見表4，該表第1欄位為安全要求項目，第2欄位為遙控無人機，第3欄位為地面控制站。第2欄位及第3欄位以符號 V 表示，代表所需檢測之安全要求項目。

表 4、遙控無人機及地面控制站系統之一般要求增項檢測項目表

安全要求增項		遙控無人機	地面控制站
8.1.1	衛星定位系統強化能力	V	
8.1.2	衛星定位系統干擾處理能力	V	
8.1.3	取得行動應用 App 基本資安標章		V
8.1.4	無線通訊失效處理能力	V	V
8.1.5	韌體已知漏洞檢測	V	

備註：本表以「V」標示表示對應之檢測項目

8.1.1. 衛星定位系統強化能力

8.1.1.1. 測試目的

查驗遙控無人機應具備定位強化機制，並非測試其定位精準度，而是確保衛星定位系統訊號異常時，具備妥善應變作為，以避免偽造衛星定位系統訊號使遙控無人機接收錯誤位置資訊，可能導致遙控無人機被劫持或影響遙控無人機本身衛星定位系統相關功能，包括禁航區限制（no-fly zone）、自動回航（Return to home）、跟隨（Follow me）、自動巡航（Waypoint）等。

8.1.1.2. 測試方法

(1)將受測物升空飛行，使用衛星定位系統訊號產生工具產生離目前定位差距高於100公里之異常距離衛星定位訊號，並發送予受測物以進行定位欺騙。

(2)確認受測物遭受攻擊後是否有偏離原有的飛行路線。

(3)確認受測物遭受攻擊後是否啟動故障處理機制進行迫降或返航模式。

8.1.1.3. 判定標準：符合下列項目者為通過，否則為未通過

(1)受測物不受偽造衛星定位系統訊號影響，仍維持正確的飛行路線。

(2)或者受測物啟動故障處理機制進行迫降，或進入返航模式強迫無人機返回起飛地。

8.1.2. 衛星定位系統干擾處理能力

8.1.2.1. 測試目的

確認遙控無人機在衛星定位系統訊號被干擾下仍可正常運行，或可啟動容錯轉移模式以抗干擾，或可啟動失效安全機制，以確保遙控無人機可正常運行。

8.1.2.2. 測試方法

(1)啟動受測物及其地面控制站，並開啟衛星定位系統干擾器確認無人機是否仍可正常運行。

(2)確認受測物是否具有無訊號迫降或返航等失效處理機制。

8.1.2.3. 判定標準：符合下列項目之一者為通過，否則為未通過

(1)受測物運行未受衛星定位系統訊號被干擾之影響，或啟動容錯轉移模式以抗干擾且可正常運行。

(2)若無項次（1）之抗干擾能力者，受測物應啟動無法正常運行之處理機制，進行迫降或進入返航模式返回起飛地。

(3)受測物若為定翼機機型且無項次（1）之抗干擾能力者，其地面控制站應顯示受測物接收衛星定位系統訊號異常，且出具訊號異常應變處置之佐證資料。

8.1.3. 取得行動應用 App 基本資安標章

8.1.3.1. 測試目的

避免地面控制站之行動應用 App 存在已知資安漏洞。

8.1.3.2. 測試方法

受測物之行動應用 App 廠牌及版本，是否已取得 MAS 標章。

8.1.3.3. 判定標準：符合下列項目者為通過，否則為未通過

受測物之行動應用 App 已取得 MAS 標章。

8.1.4. 無線通訊失效處理能力

8.1.4.1. 測試目的

確保遙控無人機在無線通訊失效下具有失效保護機制。

8.1.4.2. 測試方法

受測物於升空穩定後，在其地面控制站關閉無線通訊功能情況下，是否能依既定航線運作、啟動返航或迫降機制。

8.1.4.3. 判定標準：符合下列項目之一者為通過，否則為未通過

(1)受測物能維持既定航線正常運作。

(2)受測物具啟動通訊失效保護機制進行返航模式或迫降。

(3)受測物若為定翼機機型且無項次（1）維持既定航線、(2）通訊失效保護機制者，應出具通訊失效應變處置之佐證資料。

8.1.5. 韌體已知漏洞檢測

8.1.5.1. 測試目的

查驗飛控模組韌體是否具有 CVE 常見已知高風險漏洞，及是否為 CISA 所記載之可利用漏洞。

8.1.5.2. 測試方法

(1)依送測物開放原始碼之版本資訊，取得 CVE 漏洞資訊，或依下列(2)(3)進行檢測。

(2)使用韌體掃描工具，對受測物之韌體進行掃描。

(3)檢視韌體掃描工具掃描後之弱點掃描報告。

8.1.5.3. 判定標準：符合下列項目者為通過，否則為未通過

(1) 受測物韌體未檢出 CVSS 基礎評分7.0以上(含7.0)之重大、高風險等級漏洞。

(2) 受測物掃描結果之 CVSS 基礎評分7.0以上(含7.0)弱點項目非為 CISA 所記載之可利用漏洞。

(3) 當檢測出之資安風險漏洞以其所具 CVSS 最新版本之評分為依據。

8.2.特殊安全要求

如欲申請8.2特殊安全要求增項檢測，須搭配第6章與第8.1章進行檢測。

遙控無人機及地面控制站系統之特殊安全要求增項詳見表5，該表第1欄位為安全要求項目，第2欄位為遙控無人機，第3欄位為地面控制站。第2欄位及第3欄位以符號 V 表示所需檢測之安全要求項目，以符號 O 表示選測之安全要求項目。

表 5、遙控無人機及地面控制站系統之特殊要求增項檢測項目表

安全要求增項		遙控無人機	地面控制站
8.2.1	數據儲存安全	V	V
8.2.2	無人機命令連結（command link）之認證機制	V	V
8.2.3	工程除錯介面	V	
8.2.4	原始碼安全掃描	O	V
8.2.5	未公開揭露應用程式		V
8.2.6	軟體更新安全		V

備註：本表以「V」標示表示對應之檢測項目，以「O」標示表示選測項目

8.2.1. 數據儲存安全

8.2.1.1. 測試目的

查驗受測物之飛行紀錄等機敏資料，如有儲存至非揮發性記憶體儲存體應加密處理後儲存。機敏資料包括飛控紀錄，及廠商應提供機敏資料之定義說明。

8.2.1.2. 測試方法

(1) 連接受測物，依廠商提供之數據資料儲存位置，檢查儲存內容之數據資料部份是否經加密處理。

(2) 確認匯出受測物之飛行紀錄等資料，檢查是否經加密處理。

8.2.1.3. 預期結果

廠商提供之飛行紀錄等資料儲存位置，儲存內容之數據資料部分應採用 FIPS 140-2 Annex A 以上之版本所核可之加密處理機制進行加密。

8.2.2. 無人機命令連結（command link）之認證機制

8.2.2.1. 測試目的

測試對無人機之命令連結（command link）認證機制是否可被避開，讓攻擊者獲得無人機的控制與存取功能，或讓非法無人機完成認證。

8.2.2.2. 測試方法

廠商宣告受測無人機所使用之認證辨識機制，檢測人員依廠商宣告之認證辨識機制進行測試，並確認是否可完成認證並讓無人機與地面控制站相互識別。

8.2.2.3. 預期結果

驗證後與廠商宣告之認證方式相符且無人機與地面控制站相互識別。

8.2.3. 工程除錯介面

8.2.3.1. 測試目的

避免受測物之序列埠或任何存取介面存在未揭露或未受適當保護控制介面。

8.2.3.2. 測試方法

(1) 依廠商提供說明文件及工具，與可連接之序列埠或存取介面進行連接。

(2) 分析是否存在工程除錯介面或未受適當保護之控制介面。

8.2.3.3. 預期結果

經測試未檢出未公開揭露或未受適當保護之工程除錯或控制介面，包含序列埠如UART、JTAG、USB 等。

8.2.4. 原始碼安全掃描

8.2.4.1. 測試目的

避免受測物存在軟體設計缺陷。

8.2.4.2. 測試方法

(1) 使用原始碼安全掃描工具，對受測物之原始碼進行掃描。

(2) 檢視該原始碼安全掃描工具所產生之報告，確認原始碼是否存在 CWE/SANS TOP 25最新版本軟體缺陷。

8.2.4.3. 預期結果

受測物之原始碼不存在 CWE/SANS TOP 25最新版本軟體缺陷。

8.2.5. 未公開揭露應用程式

8.2.5.1. 測試目的

避免受測物存在資安漏洞或未揭露應用程式。

8.2.5.2. 測試方法

依廠商提供說明文件及工具如軟體物料清單，內容欄位應包括但不限於組件名稱、供應商、版本、組件唯一識別碼、與其他組件關聯、建立清單作者及時間戳記，分析是否存在資安漏洞或未揭露應用程式（未公開揭露，但卻存在的應用程式）。

8.2.5.3. 預期結果

經檢驗受測物具備說明文件或軟體物料清單且內容包括但不限於組件名稱、供應商、版本、組件唯一識別碼、與其他組件關聯、建立清單作者及時間戳記，且未檢出資安漏洞或未公開揭露應用程式。

8.2.6. 軟體更新安全

8.2.6.1. 測試目的

查驗地面控制站之軟體是否有經過加密保護，以及查驗模組之軟體更新採用安全通道，同時能鑑別安全通道所使用憑證之正確性及有效性。

8.2.6.2. 測試方法

(1) 使用具軟體拆解功能之工具，對模組之軟體進行拆解。

(2) 檢視該軟體更新檔是否可被解析出檔案系統目錄。

(3) 若軟體更新檔無法被解析出檔案系統目錄，審閱可證明所使用加密演算法之書面資料。

(4) 若軟體更新檔未加密，確認系統通行碼資料的保密機制是否採用 FIPS 140-2 Annex A 以上之版本所核可之安全功能、是否存在金鑰、是否存在所宣告之外的 email 資料、是否存在所宣告相連伺服器外之 IP 資料、是否存在所宣告相連伺服器外之 URL 資料。

(5) 使用安全通道掃描工具，對更新伺服器進行掃描。

(6) 比對掃描結果，檢視伺服器所支援的密碼套件，是否符合附錄 A 之要求。

(7) 將測試電腦（或行動裝置）連接模組，並啟動更新。

(8) 側錄更新伺服器與模組間之封包，檢視所側錄之封包是否採用安全通道。

(9) 再次啟動更新。

(10) 使用中間人攻擊方式進行通訊攔截，並嘗試竄改封包。

(11) 發送已竄改之封包，並檢視受測物是否接收。

(12) 如軟體更新採用非線上更新之方式，廠商可說明其軟體更新方式，檢測人員將依其方式確認是否可確保更新軟體受到適當保護以維持其正確性。

8.2.6.3. 預期結果

(1) 軟體具備更新功能。

(2) 軟體更新檔案無法被解析出檔案系統目錄，且加密演算法採用 FIPS 140-2 Annex A 以上之版本所核可之安全功能。

(3) 軟體之程式碼與安裝檔內其他檔案，無檢出通行碼資料、無檢出加解密演算法之金鑰，或加解密金鑰不能被解密回復、不存在非公開 email 資料、不存在所宣告相連伺服器外之 IP 資料、不存在所宣告相連伺服器外之 URL 資料。

(4) 模組之線上更新路徑通過安全通道，且安全通道僅支援附錄 A 中所建議之密碼套件。

(5) 若通訊封包被竄改，受測物應拒絕通訊或安全通道建立不成功。

(6) 檢測人員依廠商提供之更新方式，確認軟體更新過程受到適當之保護。

附錄 A
安全通道建議使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

A.1 TLSv1.2

TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305

TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES256_SHA384

TLS_ECDHE_RSA_WITH_AES256_SHA384

TLS_ECDHE_ECDSA_WITH_AES128_SHA256

TLS_ECDHE_RSA_WITH_AES128_SHA256

A.2 TLSv1.3

TLS_AES_128_GCM_SHA256

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_CCM_SHA256

TLS_AES_128_CCM_8_SHA256

附錄 B
安全要求項目與引用標準表

安全構面	安全要求項目	引用標準
6.2系統安全	6.2.1身分鑑別	• ANSI/CTA-2088-A • AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS) • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance • U.S. Department of Homeland Security CISA, UAS Cybersecurity • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity
	6.2.2網路服務埠檢測	• ANSI/CTA-2088-A • ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements • AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance • U.S. Department of Homeland Security CISA, UAS Cybersecurity
	6.2.3系統異常流量	• AUVSI, Product and Device Security • ANSI/CTA-2088-A • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance

安全構面	安全要求項目	引用標準
6.3軟體安全	6.3.1惡意程式	• ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements • AUVSI, Product and Device Security • NIST SP 800-53 • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity
	6.3.2弱點掃描	• ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements • AUVSI, Product and Device Security • NIST SP 800-53 • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity • U.S. Department of Homeland Security CISA, UAS Cybersecurity
6.4通訊安全	6.4.1無線通訊安全	• ANSI/CTA-2088-A • AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA, Protecting against the threat of unmanned aircraft system (UAS) • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity • U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems (UASS) • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance

安全構面	安全要求項目	引用標準
6.5韌體安全	6.5.1韌體更新安全	• ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements • ANSI/CTA-2088-A • AUVSI, Product and Device Security • NIST.SP.800-53r5 • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity
7.1群飛系統安全檢測	7.1.1群飛系統弱點檢測 7.1.2群飛系統網路服務埠 7.1.3群飛系統遠端登入存取管理 7.1.4群飛系統遠端登入存取內容保護 7.1.5群飛系統高風險服務功能管理 7.1.6群飛系統網頁應用程式檢測 7.1.7群飛系統身分驗證機制 7.1.8群飛系統使用者通行碼強度與防護 7.1.9群飛系統網頁傳輸安全管理 7.1.10群飛系統網頁使用授權管理 7.1.11群飛系統無線網路通訊安全 7.1.12群飛系統實體安全防護	TAICS TR-0022 v2.0:2023 物聯網場域資安防護評估指引 v2 TAICS TS-0041 v1.0 無線寬頻分享器資安測式規範
8.1一般安全要求	8.1.1衛星定位系統強化能力	• AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA, Protecting against the threat of unmanned aircraft system (UAS) • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance

安全構面	安全要求項目	引用標準
	8.1.2衛星定位系統干擾處理能力	• AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA, Protecting against the threat of unmanned aircraft system (UAS) • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance
	8.1.3取得行動應用 App 基本資安標章	• AUVSI, Product and Device Security • 行動應用資安聯盟行動應用 App 基本資安規範 V1.4 • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance
	8.1.4無線通訊失效處理能力	• ANSI/CTA-2088-A • AUVSI, Product and Device Security
	8.1.5韌體已知漏洞檢測	• ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements • AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance
8.2特殊安全要求	8.2.1數據儲存安全	• ANSI/CTA-2088-A • AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS) • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity • U.S. Department of Homeland Security CISA, UAS Cybersecurity

安全構面	安全要求項目	引用標準
	8.2.2無人機命令連結（command link）之認證機制	• ANSI/CTA-2088-A • AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS) • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity
	8.2.3工程除錯介面	• ANSI/CTA-2088-A • AUVSI, Product and Device Security • ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity
	8.2.4原始碼安全掃描	• ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements • AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity
	8.2.5未公開揭露應用程式	• ANSI/CTA-2088-A • AUVSI, Product and Device Security • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity
	8.2.6軟體更新安全	• ANSI/CTA-2088-A • ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements • AUVSI, Product and Device Security • NIST SP 800-53 • U.S. Department of Homeland Security CISA, Secure Your Drone Privacy and Data Protection Guidance • Blue UAS, Product and Device Security • U.S. Department of Homeland Security CISA,Be Air Aware UAS Cybersecurity

附錄 C

遙控無人機資安檢測自我宣告表

送測者/受測單位須檢附產品自我宣告表，以供測試實驗室參閱：

<table>
<tr><th colspan="6">產 品 自 我 宣 告 表</th></tr>
<tr><td>產品名稱/產品廠牌/
產品型號/機型</td><td colspan="3">產品名稱：
產品廠牌：</td><td colspan="2">產品型式(型號)：
機型：如四軸多旋翼無人機、定翼機等</td></tr>
<tr><td rowspan="3">送測者/受測單位</td><td colspan="5">公司、商號名稱</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="5">☐製造商 ☐進口商 ☐經銷商</td></tr>
<tr><td>軟體版本資訊</td><td colspan="5">軟體名稱：
軟體版本：
軟體雜湊值：需標明雜湊演算法
若為 App 應提供 APK、IPA 或對應下載連結以及操作之詳細流程，若為桌面應用程式應提供應用部署與操作之詳細流程</td></tr>
<tr><td>韌體版本資訊</td><td colspan="5">韌體名稱：
韌體版本：
韌體雜湊值：需標明雜湊演算法
應提供無人機本體之韌體檔案，另需詳細說明韌體更新方式</td></tr>
<tr><td>行動應用 APP
基本資安標章</td><td colspan="5">若為 App 型式，則須提供 MAS 認證標章</td></tr>
<tr><td rowspan="4">預設啟用之 TCP/UDP
網路通訊埠與
對應服務</td><td>類型</td><td colspan="2">通訊埠</td><td>對應服務</td><td>目的</td></tr>
<tr><td>例如:TCP</td><td colspan="2">22</td><td>SSH</td><td>維運使用</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td>預期內部及對外流量</td><td colspan="5">內部連線如 UAV 與 GCS 若有相對應 IP 需列出
對外連線如圖資伺服器、影像傳輸伺服器等</td></tr>
</table>

<table>
<tr><td rowspan="2">身分驗證方法之說明與佐證</td><td colspan="3">通行碼/非通行碼登入方式說明與佐證資訊</td></tr>
<tr><td colspan="3">☐通行碼
☐非通行碼：
可擷取系統佐證資訊畫面</td></tr>
<tr><td rowspan="5">作業系統及網頁管理介面權限身分驗證鑑別資訊</td><td>身分權限</td><td>帳號/名稱</td><td>通行碼/非通行碼</td></tr>
<tr><td>例如:root (OS)</td><td>root</td><td>!QAZ3edc</td></tr>
<tr><td>例如:user (OS)</td><td></td><td></td></tr>
<tr><td>例如:admin (Web)</td><td>AdminManager</td><td>!QAZ3edc</td></tr>
<tr><td>例如:user (Web)</td><td></td><td></td></tr>
<tr><td rowspan="2">通行碼鑑別機制強度及參照依據</td><td colspan="3">通行碼強度要求規則</td></tr>
<tr><td colspan="3">說明通行碼複雜度規則，如字元長度、英文大小寫字元等
可擷取系統佐證資訊畫面</td></tr>
<tr><td rowspan="2">通行碼輸入頻率、錯誤次數限制</td><td>錯誤鎖定時間</td><td colspan="2"></td></tr>
<tr><td>錯誤鎖定次數</td><td colspan="2"></td></tr>
<tr><td>無線通訊加密傳輸佐證資訊</td><td colspan="3">☐ Wi-Fi WPA2 (Counter Mode with CBC-MAC Protocol, CCMP)
☐ 其他_____：
請擷取加密佐證資訊畫面</td></tr>
</table>

附錄 D

遙控無人機群飛系統自我宣告表

送測者/受測單位須檢附產品自我宣告表，以供測試實驗室參閱：

<table>
<tr><th colspan="5">群 飛 系 統 自 我 宣 告 表</th></tr>
<tr><td>產品名稱/產品廠牌/
產品型號</td><td colspan="4"></td></tr>
<tr><td rowspan="3">送測者/受測單位</td><td colspan="4">公司、商號名稱</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">☐製造商 ☐進口商 ☐經銷商</td></tr>
<tr><td rowspan="6">預設啟用之 TCP/UDP
網路通訊埠與
對應服務</td><td>類型</td><td>通訊埠</td><td>對應服務</td><td>目的</td></tr>
<tr><td>例如:TCP</td><td>22</td><td>SSH</td><td>維運使用</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">身分驗證方法
之說明與佐證</td><td colspan="4">通行碼/非通行碼登入方式說明與佐證資訊</td></tr>
<tr><td colspan="4">☐通行碼
☐非通行碼：
可擷取系統佐證資訊畫面</td></tr>
<tr><td rowspan="4">作業系統及網頁管理
介面權限身分驗證
鑑別資訊</td><td>身分權限</td><td>帳號/名稱</td><td colspan="2">通行碼/非通行碼</td></tr>
<tr><td>例如:root (OS)</td><td>root</td><td colspan="2">!QAZ3edc</td></tr>
<tr><td>例如:user (OS)</td><td></td><td colspan="2"></td></tr>
<tr><td>例如:admin
(Web)</td><td>AdminManager</td><td colspan="2">!QAZ3edc</td></tr>
</table>

<table>
<tr><td></td><td>例如:user
(Web)</td><td></td><td></td></tr>
<tr><td rowspan="2">通行碼鑑別機制強度及參照依據</td><td colspan="3">通行碼強度要求規則</td></tr>
<tr><td colspan="3">說明通行碼複雜度規則，如字元長度、英文大小寫字元等
可擷取系統佐證資訊畫面</td></tr>
<tr><td rowspan="2">通行碼輸入頻率、錯誤次數限制</td><td>錯誤鎖定時間</td><td colspan="2"></td></tr>
<tr><td>錯誤鎖定次數</td><td colspan="2"></td></tr>
<tr><td>閒置權限管理機制</td><td>閒置管理時間</td><td colspan="2"></td></tr>
<tr><td>無線通訊加密傳輸佐證資訊</td><td colspan="3">☐ Wi-Fi WPA2 (Counter Mode with CBC-MAC Protocol, CCMP)
☐ 其他_____：
請擷取加密佐證資訊畫面</td></tr>
<tr><td>群飛系統實體安全防護機制</td><td colspan="3">請提供群飛系統場域中，相關隔離措施或設備接入點保護辦法。
例如:展演範圍與非工作人員之隔離辦法、企業專網使用與對應數量之申請證明、實體連接埠關閉資訊、實體隔離佐證圖示等。</td></tr>
</table>

參考資料

[1] 交通部「民用航空法」。

[2] 交通部「遙控無人機管理規則」。

[3] ANSI/CAN/UL 2900-1: “Standard for Software Cybersecurity for Network-Connectable Products”, Part 1: General Requirements.

[4] ANSI/CTA -2088.1: “Baseline Cybersecurity for Small Unmanned Aerial Systems”.

[5] Association for Uncrewed Vehicle Systems International (AUVSI), “Green UAS Frameworks”.

[6] Code of Federal Regulations: “§ 89.320 Minimum performance requirements for remote identification broadcast modules”.

[7] ETSI TS 103 701 V1.1.1 (2021-08): “CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements”.

[8] FAA 14 CFR Parts 89: “Remote Identification of Unmanned Aircraft”.

[9] IEC 62443-2-1: “Establishing an industrial automation and control system security program”.

[10]IEC 62443-3-3 “System security requirements and security levels”.

[11] SEMI E187: “Specification for Cybersecurity of Fab Equipment”.

[12]ITU-T X.1521: “Cybersecurity Information Exchange Vulnerability/State Exchange Common Vulnerability Scoring System (CVSS)”.

[13]NIST 800-171A: “Assessing Security Requirements for Controlled Unclassified Information”.

[14]NIST SP 800-53 “Security and Privacy Controls for Information Systems and Organizations”.

[15]NIST SP 800-38A “Recommendation for Block Cipher Modes of Operation: Methods and Techniques”.

[16] U.S. Department of Homeland Security CISA, “Protecting against the threat of unmanned aircraft system (UAS)”.

[17]U.S. Department of Homeland Security CISA, “Cybersecurity best practices for operating commercial unmanned aircraft systems (UASS)”.

[18]U.S. Department of Homeland Security CISA, ”Secure Your Drone Privacy and Data Protection Guidance”.

[19]U.S. Department of Homeland Security CISA, “Be Air Aware UAS Cybersecurity”.

[20]台灣資通產業標準協會「TAICS TR-0022 v2.0:2023物聯網場域資安防護評估指引」。