

限制採購危害國家資通安全產品



依行政院112年6月20日院授數資安字第1121000202號函(重申各公務機關使用資通訊產品原則)

禁止使用及採購大陸廠牌資通訊產品(含軟體、硬體及服務)

1)本校資通安全管理專區不定期更新最新禁止之廠牌

2)行政院未提供相關設備清單，以下廠牌僅供參考，包括但不限於：



普聯技術公司 (TP-Link)	華為 (Huawei)	廣東歐加控股公司／廣東行動通訊公司 (OPPO)
魅族(MEIZU)	Foscam	Penoval、Penoval App(觸控筆含其所屬軟體)
騰達(Tenda)	中興通訊(ZTE)	新加坡泛學科技(線上教學平台)
TOTOLINK	努比亞(Nubia)	杭州海康威視 (Hikvision)
美圖(Meitu)	海能達(Hytera)	浙江大華技術公司 (Dahua)
海信(Hisense)	極米(XGIMI)	深圳大疆創新科技公司 (DJI)
真我(REALME)	天璣(SUGAR、NIKO)	小米集團 (MI)
維沃(VIVO)	金立(GIONEE)	小米、紅米(Xiaomi、Redmi)(MI)
SUGAR	海能達(Hytera)	
酷派(Coolpad)	新華三(H3C)	
高巨創新(EMO)	卓普(ZOPO)	
黑鯊(Black Shark)	酷比(Koobee)	
聯想(lenovo)	影石科技(Insta360)	

如未列於上述，但仍屬中國廠牌產品，請勿購買

請勿採購

- 若因業務需求且無其他替代方案，仍需使用危害國家資通安全產品時，應具體敘明理由，並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關(數位發展部)核定，
產品未汰換前，應加強下列資安強化措施：

- 強化資安管理措施，例如：設定高強度密碼、禁止遠端維護等。
- 產品遇資安攻擊導致顯示畫面遭置換，應立即置換靜態畫面，或立即關機。
- 產品若為硬體，應確認其不具WiFi等持續連網功能(非僅以軟體關閉)。若需以外接裝置方式進行更新，須有專人在旁全程監督，於傳輸完成後立即移除外接裝置。
- 產品使用屆期後不得再購買危害國家資通安全產品。

- 各機關辦理採購案時，應注意以下事項：

- 採購案內涉資通訊軟體、硬體或服務等相關事務，機關可要求廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。
- 各機關自行或委外營運，提供公眾活動或使用之場地，不得使用危害國家資通安全產品，且應將相關限制事項納入委外契約或場地使用規定中。

資通安全管理專區

