資通系統籌獲各階段資安強化措施

一、依據資通安全管理法(以下簡稱本法)第九條規定，公務機關或特定非公務機關於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。為協助公務機關及特定非公務機關於本法適用範圍內委外辦理相關作業，補充說明委託機關依本法施行細則第四條規定選任或監督受託者之相關行政流程及應注意事項，特訂定本措施。

二、本措施所稱資通系統籌獲，指委託機關辦理本法第九條所定委外辦理資通系統之建置、維運或資通服務提供，其執行方式[1]包含但不限於：

(一)採購[2]：包含工程之定作、財物之買受、定製、承租及勞務之委任或僱傭等，不論是否依據政府採購法辦理，只要經由工程、財物或勞務性質採購取得或其執行時使用資通系統者皆屬之。

(二)委任：依行政程序法第十五條第一項規定委任所屬下級機關執行業務，取得或其執行時使用資通系統者皆屬之。

(三)委託：依行政程序法第十五條第二項或第十六條規定，委託不相隸屬之行政機關執行業務，或委託民間團體或個人辦理業務，取得或其執行時使用資通系統者皆屬之。

---

[1] 「無客製化之套裝軟體」、「網路及資安等資通訊設備購買」不適用本措施相關規範，惟「例行性或不定期之系統維護案」仍應視契約要求(新功能增修、弱點修補、版本更新等)，適用本措施之「維運階段」各項規定。

[2] 參考政府採購法第七條之定義，所稱工程，指在地面上下新建、增建、改建、修建、拆除構造物與其所屬設備及改變自然環境之行為，包括建築、土木、水利、環境、交通、機械、電氣、化工及其他經主管機關認定之工程；所稱財物，指各種物品（生鮮農漁產品除外）、材料、設備、機具與其他動產、不動產、權利及其他經主管機關認定之財物；所稱勞務，指專業服務、技術服務、資訊服務、研究發展、營運管理、維修、訓練、勞力及其他經主管機關認定之勞務。

三、委託機關於資通系統籌獲時應依下列作業方式辦理：

(一)需求階段

1. 資通系統取得前即應評估並標註所需之資通系統防護需求等級：

(1) 涉資通系統籌獲，於徵求時應由委託機關依資通安全責任等級分級辦法附表九所定資通系統防護需求分級原則評估等級，標示資通系統之防護需求等級供受託者知悉。

(2) 前述資通系統防護需求等級評估結果應經委託機關資通安全長確認。

2. 應估算資安資源需求：委託機關除應評估訂定受託者應配置之資通安全專業人員人數及所需能力等相關需求外，應至少以資通系統籌獲案資訊經費百分之五估算資安經費；如因實務作業無法達成上開要求，應敘明原因及擬採行之資安作為，視執行方式依下列程序辦理：

(1) 採購：報請委託機關資通安全長核准後依擬採行之資安作為辦理。

(2) 採購以外之其他執行方式：報請委託機關核准後依擬採行之資安作為辦理。

委託機關並應於資通系統籌獲案之內部成本分析及請受託者提報之估價單等投標文件中明列資安經費。(範例如附件一)

3. 依政府採購法辦理之採購，應將投標廠商之資安作為應納入評選項目，依下列規定辦理；如屬依政府採購法規定無須辦理評選/評審之採購或採其他執行方式者，應以適當方式檢視受託者之資安作為：

(1) 涉資通系統籌獲，以採最有利標，不訂底價為原則，並以評選方式選任受託者，將委託案之相關資安作為

納入評選項目(評選表範例如附件二)，配分至少占總分之百分之十;如籌獲案中之資通系統或服務占比低於百分之十，配分至少占總分之百分之五。

(2) 評選時應要求投標廠商說明履約之資安作為。(廠商自我評估表範例如附件三)

(3) 依資通系統防護需求等級，機關得參考「資通系統防護基準驗證實務」指引，於規劃(招標)階段訂定對應之廠商專業能力需求資格，俾選任合適受託者。

4. 資通系統籌獲涉及委託機關之**核心**資通系統[3]，且採用評選方式選任受託者時，評選委員應包含至少一位資安專業人員，並符合下列資格之一：

(1) 至少取得資安主管機關認可之國內外發證機關(構)所核發之資通安全專業證照。

(2) 從事資安實務作業三年以上。

(3) 資安教學經驗六年以上。

(4) 為行政院公共工程委員會公告之評選委員會專家學者建議名單資料庫中之資訊安全委員[4]。

如不採用評選方式選任受託者時，委託機關辦理資通系統籌獲案之團隊應至少包含一位資安專業人員，協助受託者辦理選任相關作業。

5. 為強化各機關資通訊相關採購案之資安防護，機關辦理資訊服務採購時得參考行政院秘書長一百十年七月十三日院臺護長字第一一〇〇一七七四八三號函檢附之 「資訊服務採購案之資安檢核事項」(如附件四)辦理，據以確認採購案各項資安要求。

6. 委託機關對於可能選任之受託者及其所供應之財物(軟硬

[3] 指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。

[4] 指在評選委員會專家學者建議名單資料庫中類別為「資訊類」，科別為「資訊安全」之專家學者。

體設備)或勞務之資料存取、儲存、備份及備援等作業，其實體設備所在地及資料傳輸是否跨境等相關議題,得要求其以書面方式揭露，並納入選任評估參考。

(二)建置階段：

1. 委託機關之資通安全專責人員應以適當方式協助資通系統籌獲需求單位監督、確認開發團隊於系統開發時遵循安全軟體開發生命周期(SSDLC)[5]。
2. 資通系統籌獲案之重點里程碑,應有委託機關之資通安全專責人員協助資通系統籌獲需求單位確認。
3. 委託機關之**核心**資通系統籌獲案,應聘請外部資安專家為顧問或委員,協助機關於專案重點里程碑中,檢視履約(執行)程序與成果之相關資安管理作為。
4. 為確保**核心**資通系統品質,針對受託業務包括委託機關之核心資通系統且委託金額達新臺幣一千萬元以上者,委託機關應評估導入獨立驗證與認證機制(IV&V)，評估結果應經委託機關資通安全長確認。

(三)維運階段：

1. 落實資安管理:委託機關之資通安全專責人員應協助資通系統管理單位,確認資通系統維運作業確實依委託機關之資安管理措施落實辦理，例如登入維護、資料備份、效能調校、主機環境及系統版本更新等。

委託機關資通系統籌獲專案資安作業分工

	管理及需求單位	資通安全專責人員
SSDLC	監督、確認	(第二線)勾稽確認
履約(執行)及專案里程碑資安管理	訂定、監督、確認	(第二線)勾稽確認

[5] 本項作業應至少包含資通安全責任等級分級辦法附表十資通系統防護基準之「系統與服務獲得」構面對應防護需求等級之各項控制措施。

2. 受託者應配置適當之資通安全專責人員：協助確認履約(執行)階段作業符合委託機關及受託者雙方之資安管理規範。
3. 在契約有效期間內(委任、委託關係期間)之資安稽核作業：
   (1) 委託機關得依資通系統籌獲案之規模及性質，要求受託者應就受委託範圍自行辦理資安稽核作業。
   (2) 資通系統防護需求等級為「**高級**」之資通系統籌獲，委託機關應以適當方式定期或不定期對受託者辦理資安稽核；資通系統防護需求等級為「中級」之資通系統籌獲，委託機關得視需求以適當方式定期或不定期對受託者辦理資安稽核，確認受託者落實資安要求。
   (3) 受託者執行受託業務知悉資安事件，且經審核為重大資安事件[6]時，委託機關應辦理資安稽核，並應將稽核結果送交資安主管機關。
   (4) 廠商聯合稽核：委託機關得依行政院一百十年十二月十四日院臺護字第一一〇〇一九四九六〇號函訂定之「受託者資通安全聯合查核指引」辦理聯合稽核，集結相關委託機關之查核資源與能量，監督受託者之資通安全維護情形，以減少受託者受機關查核之頻率。

[6] 指資通安全事件通報及應變辦法第二條第四項及第五項規定之第三級及第四級資通安全事件。