政府資訊服務採購作業指引(草案)

112 年 8 月 V6.3

一、 預算編列

(一) 按比例編列資安預算並單獨列項：

1. 依「六大核心戰略產業推動方案」項下「資安卓越產業」之推動策略，各機關所提中長程計畫，應依其資訊建設經費編列一定比率之資安經費。
2. 依數位發展部(下簡稱數位部)「資通系統籌獲各階段資安強化措施」，機關辦理資訊服務採購，至少以資訊經費 5%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。

(二) 必要時先行辦理系統整體規劃：

建置新系統或系統重大變更時，應評估先行編列預算辦理系統整體規劃或(及)資安規劃之必要性，依三層式(資料底層、應用層、使用者介面層)資訊系統開發架構，自行或委託廠商規劃系統架構、分析功能需求、開發資料底層等前置工作，並納入安全系統開發生命周期(SSDLC)規劃，後續再另案委託其他廠商辦理應用層及使用者介面開發。

(三) 依個案特性編列預備費及物價調整費：

為因應系統開發過程可能發生之需求新增或變動而衍生必要費用，機關得預估可能所需之額外人月數，編列預備費，未來履約階段於該費用額度內，依實際使用數量結算給付；另如屬逾1年之長期服務契約，機關得於契約載明每年服務費用因應物價(如：軟體授權費用)或薪資指數調整之計算方式。

(四) 依法得洽廠商提供意見：

機關應就廠商履約工作內容、各類履約人員成本(得參考行政院主計總處薪情平臺、勞動部職類別薪資資料、政府電子

採購網資訊人員薪資資料等）、軟體維護、軟體授權費等項目，並參酌市場行情（包含國際市場）、物價水準等核實編列預算；編列後得依政府採購法（下稱採購法）第34條第1項但書規定，於政府電子採購網公開向廠商說明，並請廠商提供意見及參考資料。

二、廠商資格

（一） 評估是否允許陸資廠商參與：

涉及國家安全或資通安全之採購，機關應於招標文件規定不允許陸資廠商(含其分包廠商)及陸籍人士參與；陸資廠商包含大陸地區廠商、第三地區陸資廠商及在臺陸資廠商。請參閱行政院公共工程委員會(下簡稱工程會)107年12月20日工程企字第1070050131號函。

（二） 必要時限制廠商資金來源比例：

依「機關辦理涉及國家安全採購之廠商資格限制條件及審查作業辦法」，機關辦理涉及國家安全之採購，得依採購案件之特性及實際需要擇定廠商資格限制條件。例如：對廠商資金來源比例有特定限制者，應要求廠商提出廠商董監事、股東名冊、資金來源文件，如涉及僑外資者，應要求廠商提出授權查核同意文件，必要時洽目的事業主管機關協助查察。

三、需求文件

（一） 詳列機關招標需求：

資通系統或軟體開發前，應依個案性質於招標文件載明服務之項目及工作範圍，以明確描述系統需求；機關如能力或人力不足無法完成者，可委託專業廠商先行辦理系統整體規劃。請參閱工程會111年9月22日工程資字第1111500157號函檢送之「資訊服務採購需求確認之對策與作法」。

（二） 載明服務水準及資安要求：

1. 於招標文件中載明服務水準及品質需求，例如：正常運作時間百分比、運作資源消耗、修復時間、系統反應時間、錯誤率、系統與通訊保護完整性等資通系統防護控制措施、跨平台/跨瀏覽器支援程度、使用者感受等，依據個案的採購類型及需求妥適選擇必要項目，並於招標文件載明，以利廠商合理估價及遵循。(如附件 1)
2. 機關應依資通安全管理法相關規定、數位部相關規範與政策要求，及資通安全責任等級分級辦法第 11 條第 2 項：「各機關自行或委外開發之資通系統應依該辦法附表九所定資通系統防護需求分級原則完成資通系統分級，…」擇定資通系統防護需求(高、中、普)，並依「各類資訊(服務)採購共通性資通安全基本要求參考一覽表」(如附件 2)擇定涉及資安之履約項目，於招標文件中載明；資訊財物採購亦得參考上開一覽表擇定須符合之資安項目。

(三) 使用政府資料傳輸平臺及納入零信任架構：

1. 數位發展部以政府骨幹網路（GSN）為基礎，已建置跨機關資料傳輸專屬通道（T-Road）管理平臺。若資通安全責任等級 A 級公務機關其履約標的涉跨機關資訊傳輸，應評估透過上級主管機關介接或自行介接 T-Road 通道，由資料需求機關依規定向資料提供機關提出申請。經資料提供機關依權責核准後，依 OAS 標準格式進行資料提供，資料需求機關之管理責任應符「政府資料傳輸平臺管理規範」之規定。
2. 為推動國家資通安全政策，發展零信任網路資安防護環境，資通安全責任等級 A 級公務機關應依數位發展部規劃進程導入零信任網路，以完善政府網際服務網防禦深廣度。

(四) 要求廠商投標時載明執行規劃：

機關於招標時，依機關委託資訊服務廠商評選及計費辦法第5條第8款，依招標文件要求投標廠商提出資訊服務建議書之內容，應包括請廠商載明執行規劃方式，例如：需求訪談、

系統分析、系統設計、開發、測試作法及預計時程等，並於開標後審視及評估廠商是否確實了解及符合機關需要。

（五） 妥適訂定招標文件所載之主要部分：

依採購法第 65 條第 1 項、第 2 項規定，採購契約載明應由得標廠商自行履行之全部或主要部分，不得轉包(由其他廠商代為履行)。因資訊服務採購涉及多項專業分工，部分特定服務依市場慣例有分包予其他專業廠商辦理之必要時，機關於訂定招標文件主要部分時應妥為考量，不宜逕明列所有工作項目均為主要部分。

四、 招、決標作業

（一） 載明固定價格決標者議價時不議減價格：

依採購法第52條第2項規定，資訊服務採購以不定底價最有利標為原則，機關於招標文件應明定以固定費用決標，不議減價格。請參閱工程會112年05月16日工程企字第11200030081號函及「最有利標作業手冊」。

（二） 評選項目考量廠商資安實績及作為：

1. 就涉及廠商過去履約績效之評選項目，將廠商內部資安政策、資安人力配置、曾獲得之認證與獎項等納入評選考量；另為保障採購標的及履約過程之資通安全，應將「投標廠商資安作為」納入採購評選項目，且有一定比率之配分(如：10%，依採購個案中資通系統或服務占比合理考量)，如屬依政府採購法規定無須辦理評選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。
2. 依數位部「資通系統籌獲各階段資安強化措施」，資訊服務採購標的如涉及機關核心資通系統，且採用評選方式選任廠商時，評選委員應包含至少 1 位資安專業人員，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 1 位資安專業人員，協助受託者辦理選任相關作

業。

（三） 評選項目不得列「回饋」項目：

為提升採購效益及評選廠商服務之差異，評選項目得列「創意」項目納入評選，但不得列「回饋」項目。於採購評選委員會辦理評選時，亦不得於答詢過程中要求廠商提供機關優惠回饋。經採購評選委員會依招標文件規定評選出優勝廠商，即代表該廠商投標文件內容已被接受，不應再強制要求廠商修正。

五、 契約執行

（一） 依契約約定內容協助履約及落實管理：

履約項目如涉及機關既有資通系統之修改或資料介接，機關應善盡定作人之協作義務，提供必要之原始碼或協助廠商間之協調；另亦應落實要求廠商依約履行義務並交付成果(包含原始碼)。

（二） 強化履約使用產品及履約人員之管理：

履約標的或執行過程不得使用使用大陸廠牌產品，履約人員不得為大陸籍人員。請參閱行政院秘書長109年12月18日院臺護長字第1090201804A號函及行政院112年6月20日院授數資安字第1121000202號函。

（三） 反覆檢視需求訪談結果，確認後始進行開發：

為深化及細化需求，辦理需求訪談時應反覆檢視及要求廠商展示(例如：示意圖、流程圖或雛型等)，確認符合需要再允許廠商進行程式開發。

（四） 開發過程設定查核點，反覆檢視執行成果：

契約中應依系統開發各階段載明查核點，反覆檢視執行成果並要求廠商展示(如開發畫面、資料庫架構、使用流程、功能測試、整合測試等)，並定期(開會)追蹤檢討，查核時間不列入工期計算；如經查核有不符合契約約定及機關需要者，

應即要求廠商配合改善，非可歸責於廠商者，應依查核狀態調整履約期間。

（五） 機關新增需求應合理增加經費及期程：

履約過程如確屬機關需求改變或增加情形，應辦理契約變更，給予必要之工期與費用。

（六） 機關以取得授權利用為原則：

基於尊重著作人創作、成果能善加運用開發與鼓勵廠商參與政府採購之意願，機關與廠商約定履約標的著作權歸屬時，應考量機關與廠商間之平衡，機關應儘量以取得著作財產權之授權利用為優先，包括轉授權或再製權等，俾利後續維護可委由他廠協助，著作人保有著作權。

（七） 驗收時得請具資訊、資安專業人員協助確認成果：

機關辦理驗收時，為確認廠商履約成果符合產業實務且滿足機關需求，得邀請具資訊專業之專家學者協助確認成果；如採購個案涉及機關之核心資通系統，應優先考量聘請外部資安專家為顧問或委員，協助機關檢視履約(執行)程序與成果之相關資安管理作為。

六、 爭議處理

（一） 善用契約雙方約定之處理機制：

現行工程會提供之「資訊服務採購契約範本」第 19 條已載明多元之爭議處理方式，機關可善用雙方合意成立之爭議處理小組，並選擇具有資訊、資安專業之專家學者擔任小組委員，協助協調爭議。

（二） 機關成立採購工作及審查小組提供意見：

依採購法第 11 條之 1，機關辦理資訊服務採購得依採購特性及實際需要成立採購工作及審查小組，協助審查採購需求與經費、採購策略、招標文件等事項，及提供與採購有關事務之諮詢，開會時並得邀請具資訊、資安專業之專家學者列

席，協助審查及提供諮詢。

附件1　常見資訊服務等級協議(SLA)之參考項目

服務等級協議(SLA)係衡量服務可用性、可靠性、安全性等指標，常見SLA性能指標如下，機關可依個別系統之類型、重要性、複雜性、機敏性及使用情境選用項目：

一、 系統及服務可用性

(一)環境面						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
v	v	v	v	服務韌性:電力、水、網路、空調、濕度調節之備援與調節方式，確保系統正常運作於發生異常時有足夠之應變緩衝時間。		0
		v	v	Ÿ對外網路環境：骨幹網路、交換器、路由器異常故障，造成連線與服務中斷，其累計時間每月不得超過____小時(約為____%可用率)。		0
(二)服務面						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
v	v	v	v	服務可用性(Service Availability)：該指標衡量服務對用戶可用的時間百分比，其計算應考慮到其他須排除之因素，如計畫中維護和升級；例如，SLA 可能規定該服務必須 99.9%的時間可用。(計算公式： 服務可用性 =（本月總小時數-停機時間）/ 本月總小時數 × 100%)	0	
v	v	v	v	正常運行時間百分比(Uptime percentage)：正常運行時間通常按每個日曆月或結算週期進行追蹤及報告。	0	
		v	v	平均故障間隔時間（Mean Time between Failure, MTBF）：服務故障之間的平均時間。	0	
		v	v	平均修復時間（Mean Time to Recovery, MTTR）：恢復服務故障的平均時間。	0	
			v	系統穩定度：每月每項服務中斷次數之累計不超過次數。	0	
	v	v	v	反應時間：使用者在端末設備輸入應用系統所需資料，自按功能鍵至應用系統將處理結果傳回作業端止的時間，其作業量之____%系統反應時間應在____秒內。	0	
	v	v	v	批次作業時間：自該批次作業工作啟動至作業完成之時間應於____小時內完成____筆資料。	0	
	v	v	v	檔案傳輸時間:在工作天之作業時間(上午 8 時	0	

				~下午 5 時)內，傳送____GB 檔案應於____分鐘內完成。		
			v	滿意度調查：定期對終端使用者就系統使用上，調查滿意度評分，每次調查應不低於____分。		0
(三)永續維運與管理						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
v	v	v	v	營運異地備份/備援：備份數、儲存媒體種類、異地備份數等，以及備份還原測試頻率、備援演練次數。		0
		v	v	系統備份/備援恢復作業時間 (RTO):每次操作系統備份/備援回復作業應於____(時間)內完成。		0
		v	v	資料回復可接受之時間點(RPO):可允許的最回溯落差____(時間)。		0
		v	v	最大可忍受中斷時間(MTPD)：最大可忍受系統中斷服務____小時。		0
		v	v	備品供應:涉及硬體提供者，廠商應至少準備____(例如 1/3)之備品，以利於故障時及時更換。		0
		v	v	Ÿ　網路、資安、資料庫或伺服器等設備若具備高可用性(HA)架構，需依合約規範的時間頻率，執行本地端的 HA 切換演練，確保設備切換可於時限內正常使用，每月至少切換測試一次，未能成功者計罰____元，且應於____日內再測試，直至成功為止。		0
(四)資訊安全品質：						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
v	v	v	v	風險評鑑與風險管理計畫：依照政府資安等級規定進行風險評鑑並依評鑑結果訂定風險管理計畫。	0	
		v	v	資安事件發生數量：可採用每月的資安事件發生數量，當接獲通報後，一定時間內修補漏洞的百分比等。	0	
		v	v	實體及遠端登錄管制與稽核:避免帳號洩漏或破解致影響系統安全與正常運作，應有效管控並定期稽核有無不允許或異常的登錄情形。	0	
			v	漏洞修補:避免因疏漏造成整體服務暴露於風險之中，廠商應就所提供服務涉及之軟硬體、作業系統及開發之程式，定期檢查更新並予掃描、測試及調整，確保整體運作穩定、高效及	0	

				安全。		
			v	資訊安全政策執行品質:分別計算每月及每季未依機關或契約資通安全規定執行之次數。	0	
			v	資安測試之改善：定期執行資安測試，包括安全通訊協定、系統弱點掃描、應用程式弱點掃描、App 資安檢測，其有需改善者而未能於契約約定期限內改善完成者，每月/不得超過____%。	0	
			v	安全防護計畫執行：定期檢視監控資安日誌如防火牆、入侵偵測系統、應用程式防火牆、安全資訊與管理系統等並訂定防護計畫與措施，每季未能執行次數不得超過____次。	0	
			v	資安事件之通報及應變：自知悉或接獲資通安全事件通知或即時警示後，應至遲於____分鐘內通報機關，並於____小時內提供資通安全事件等級評估、處理應變規劃及建議。	0	
			v	調查及處理資安事件之時效：資安事件發生後需依照合約規範的時限內的完成損害控制或復原作業，並於____日內送交調查、處理及改善報告（或協助機關調查處理）。	0	
			v	外部稽核：廠商需配合機關進行_____(如：ISO 27001、ISO 20000，機關視需要載明)國際資安認證外部稽核驗證，其每次稽核所列缺失不得超過____項。	0	

二、廠商之服務品質

（一） 設計與開發階段:						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
	v	v		未依機關同意之流程或設計準則開發之比率:除屬機關需求變更者外，廠商疏漏或未依機關確認之內容進行開發之比率，可依展示次數逐步降低，提升系統完善及整體性。	0	
	v	v		未依限回應問題之次數：可依不同階段及態樣規範機關所詢問題之回應時間。	0	
(二)測試驗證階段						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
		v		單元測試流程通過比率:在單元測試(驗證程式碼的每個獨立部分是否正常運作)中，通過測試的數量與總測試數量的比率應達____%以上。	0	

		v		整合測試通過比率：在整合測試(驗證程式碼的各個部分是否能夠正確地協同工作)中，通過測試的數量與總測試數量的比率應達____%以上。	0	
		v		效能調教次數：廠商應於____次內調教效能，達成契約約定之具體的績效基準(Specific performance benchmarks)。	0	
(三)上線前準備階段						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
		v		壓力測試：系統能同時、瞬時支援使用人數的上限，系統上線前應使用正式環境進行壓力測試。	0	
		v		資料移轉時間及正確率：可分階段訂定，移轉時間應每次縮短；資料漏失或錯誤率應逐次下降，且同一資料錯誤情形不得超過____次。	0	
		v	v	上線演練作業之次數與所需時間:可分次訂定，切換所需時間應每次縮短；超過機關指定之時間應紀錄為失敗(可分模組或功能計算)，上線前成功比率應逐步提升。	0	
		v	v	客服準備情形:依機關同意之問答內容進行抽測與實作，抽測通過比率應達____%以上。	0	
		v	v	人員之教育訓練：經協助受訓人員完成機關指定之測試項目應達____%；受訓人員滿意度應達__%(前開比率可分階段調高)。未能達成前開比率者，廠商應再辦理一次，仍未達成者，按差距部分每____%計罰____元。	0	
(四)建置及維運階段						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
			v	事故發生通報時間：異常事件發生時，廠商應於____(時間)內通知機關聯絡窗口。	0	
			v	Ÿ 廠商反應時間(Service provider response time)：廠商應於____(時間)內回應使用者問題或請求。	0	
			v	解決時間(Resolution time)：場商記錄問題後應於____(時間)內解決問題。	0	
			v	Ÿ 錯誤率(Error rate)：在____(時間)內，資訊系統服務中出現錯誤的次數與總次數的比率。錯誤可以是系統錯誤、應用程式錯誤、網路錯誤等。	0	
			v	軟硬體設備修復時限：軟硬體設備發生異常時，廠商於知悉或機關通知後應於____(時間)內到達現場，於____(時間)內內修復；若無法於時限內修復，應無償提供同等(含)以上替代品供使用。		0
			v	舊系統資料儲存：新系統上線後，舊系統資料		0

				應儲存於可存取環境並保留____月/年。		
			v	軟硬體設備維修妥善率：任一設備於一定期間內連續發生____次異常問題至需更換或維修者，視為未達妥善率要求。		0
(五)其他						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
v	v	v	v	交付文件及品質:廠商按照契約規範交付非屬履約成果之文件者(如工作日誌、每周報告)，因內容缺漏、不足及錯誤至退件之次數，每件不得超過____次。	0	
v	v	v	v	召開履約關理相關會議：未依契約約定召開會議者，每季不得超過____次。契約約定之廠商人員未出席會議次數，每季不得超過____次。	0	
v	v	v	v	服務團隊成員要求：廠商提供服務團隊成員資格、證照與人數要求，每季更新統計，若低於契約要求之____%者(如 95%)，依差異之每____%計罰____元。	0	

三、 使用者體驗

規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
v	v			跨瀏覽器支援：使用者端網頁介面須支援之瀏覽器類型，如：Microsoft Edge、Google Chrome、Firefox、Apple Safari。	0	
v	v			行動裝置支援：使用者端網頁介面須支援之跨平台行動裝置，如：適用 Android、iOS 作業系統。	0	
v	v			響應式網頁設計(Responsive Web Design；RWD)：讓使用者能夠在各種不同尺寸或解析度的裝置上都能夠輕鬆地瀏覽、使用網站，而不需要因為裝置不同而產生閱讀體驗上的問題。	0	
v	v			通過無障礙標章認證。	0	
	v			使用者填寫資料：使用者建立資料時，每頁面填寫平均時間應在____分鐘內。	0	
	v			提供友善列印、字體大小調整、暗色等模式供使用者選擇。	0	

附件2　各類資訊(服務)採購共通性資通安全基本要求參考一覽表