

資訊服務採購案之資安檢核事項

行政院資通安全處

110 年 6 月 8 日

一、109.03.23 版之投標須知範本

項次	條文內容	說明
1 (第 3-6 頁)	<p>十六、本採購：</p> <p><input type="checkbox"/> (1) 適用我國締結之條約或協定；其名稱為：</p> <p><input type="checkbox"/> 下列外國廠商可以參與投標：</p> <p> 1. 國家或地區名稱：_____ (未列明者即不允許)</p> <p> 2. 是否允許大陸地區廠商參與：(未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定)</p> <p> <input type="checkbox"/> 是 <input type="checkbox"/> 否</p> <p><input type="checkbox"/> (2) 不適用我國締結之條約或協定，外國廠商：</p> <p><input type="checkbox"/> 不可參與投標。但我國廠商所供應標的 (含工程、財物及勞務) 之原產地得為下列外國者：</p> <p> 1. 國家或地區名稱：_____ (未列明者即不允許)</p> <p> 2. 是否允許供應大陸地區標的：(未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定)</p> <p> <input type="checkbox"/> 是</p>	<p>1、採購案如適用我國締結之條約或協定者，針對「是否允許大陸地區廠商參與」，應勾選「否」(亦可不勾選)。</p> <p>2、採購案如不適用我國締結之條約或協定者，針對外國廠商：</p> <p>(1) 如勾選「不可參與投標。但我國廠商所供應標的 (含工程、財物及勞務) 之原產地得為下列外國者」，針對「是否允許供應大陸地區標的」，請各機關依行政院公共工程委員會 107 年 12 月 20 日工程企字第 1070050131 號函釋，視其個案特性及實際需要逕行評估是否勾選「否」(亦可不勾選)。</p> <p>(2) 針對「是否允許大陸地區廠商參與：(未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定)」，應勾選「否」(亦可不勾選)。</p>

項次	條文內容	說明
	<input type="checkbox"/> 否 <input type="checkbox"/> 下列外國廠商可以參與投標： 1. 國家或地區名稱：_____（未列明者即不允許） 2. 是否允許大陸地區廠商參與：（未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定） <input type="checkbox"/> 是 <input type="checkbox"/> 否	
2 （第 12 頁）	<p>六十四、投標廠商之基本資格及應附具之證明文件如下 ……</p> <p><input type="checkbox"/>本採購屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購，廠商不得為大陸地區廠商、第三地區含陸資成分廠商及經濟部投資審議委員會公告之陸資資訊服務業者。（上開業務範疇及陸資資訊服務業清單公開於經濟部投資審議委員會網站 http://www.moeaic.gov.tw/）。（註：適用條約或協定之採購案，如勾選本項者，請依 GPA 第 3 條規定，妥適考量本須知第 16 點之勾選）。</p> <p><input type="checkbox"/>本採購內容涉及國家安全，不允許大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與。（註：適用條約或協定之採購案，如勾選本項者，請依 GPA 第 3 條規定，妥適考量本須知第 16 點之勾選）</p>	<p>1、採購案如屬具敏感性或國安(含資安)疑慮之業務範疇 (https://www.moeaic.gov.tw/download-file.jsp?do=BP&id=ZbdrLAtDiew=)，應勾選本項，以限制大陸地區廠商、第三地區含陸資成分廠商及經濟部投資審議委員會公告之陸資資訊服務業者參與投標。</p> <p>2、採購案如涉及國家安全，應勾選本項，以限制大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與投標。</p>

二、110.04.09 修正之資訊服務採購契約範本

項次	條文內容	說明
1 (第 4 頁)	<p>第二條 履約標的</p> <p>.....</p> <p>(二)廠商應給付之標的及工作事項(由機關於招標時載明)</p> <p>.....</p> <p><input type="checkbox"/>資訊業務線上服務</p> <p>.....</p> <p>2. 廠商提供資訊業務線上服務，除契約另有約定外，應於契約約定時間內提出資訊業務線上服務建議書，就資訊業務線上服務具體範圍、服務水準、測試方式、資通安全管理機制及防護措施等向機關提出建議。上述建議書之內容，不得減損契約約定事項，並經機關核定後執行。如有減損者，無效。</p>	<p>如該採購案履約標的包含資訊業務線上服務，則應要求其提報之服務建議書內容應包含資通安全管理機制及防護措施。</p>
2 (第 16-17 頁)	<p>第八條 履約管理</p> <p>.....</p> <p>(二) 契約執行期間</p> <p>.....</p> <p>1. 工作計畫 (或建議書):</p> <p>.....</p> <p>(1)廠商應於得標後○○日 (由機關於招標時載明；未載明者，20日) 提出工作計畫 (或建議書)</p> <p>.....</p> <p><input type="checkbox"/>資通安全及保密之計畫。</p>	<p>應勾選本項(資通安全及保密之計畫)，要求廠商於得標後，所提出工作計畫 (或建議書)，應包含資通安全及保密之計畫。</p>
3	<p>第八條 履約管理</p> <p>.....</p>	<p>1、應勾選第 1 項(保密同意書/保密切結書)，要求廠商團隊成員簽署並</p>

項次	條文內容	說明
(第 18 頁)	<p>(三)廠商提供服務之團隊</p> <p>4. 廠商團隊成員應於到任當日，將已簽署之以下文件提交機關：</p> <p><input type="checkbox"/>附件 保密同意書/保密切結書</p> <p><input type="checkbox"/>附件 由所屬公司享有著作財產權與著作人格權同意書</p> <p><input type="checkbox"/>附件 適任性查核同意書(受託業務涉及國家機密者)</p>	<p>提交保密同意書/保密切結書</p> <p>2、如採購案涉及系統開發設計，則第 2 項亦應勾選</p> <p>3、如採購案涉及國家機密者，則第 3 項亦應勾選</p>
4 (第 20-21 頁)	<p>第八條 履約管理</p> <p>.....</p> <p>(六)轉包及分包</p> <p>.....</p> <p>12. 廠商將契約之部分交由其他廠商代為履行時，應與分包廠商書面約定，分包廠商應遵循政府採購法令及本契約關於分包與禁止轉包之內容；並應約定分包廠商應遵循之事項，其至少包括廠商受稽核時，如稽核範圍涉及分包部分，分包廠商就該部分應配合受稽核。</p>	<p>廠商應與分包廠商書面約定遵循本款關於轉包及分包之約定，及分包廠商就分包範圍應遵循之有關規定。</p>
5 (第 25 頁)	<p>第八條 履約管理</p> <p>.....</p> <p>(二十三)廠商履約內容涉及資通安全者，應符合下列國家標準(由機關於招標時載明)：</p> <p>.....</p> <p><input type="checkbox"/>CNS 27001；</p> <p><input type="checkbox"/>CNS 27018；</p> <p><input type="checkbox"/>其他：.....。</p>	<p>依資通安全管理法施行細則第 4 條規定，各機關委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證；爰請機關依採購案之性質，建議勾選合適選項，如要求廠商應符合 CNS27001[資訊技術-安全技術-資訊安全管理系統-要求事項]、CNS 27018[資訊技術-安全技術-公用雲 PII 處理者保</p>

項次	條文內容	說明
		護個人識別資訊(PII)之作業規範]或其他資通安全管理措施。
6 (第 25 頁)	<p>第八條 履約管理 (二十四)其他(由機關視個案實際需要者於招標時載明):</p> <p><input type="checkbox"/>本案委託業務涉及國家機密保護法所稱之國家機密者，廠商執行本案且可能接觸國家機密之人員，應接受適任性查核，並依國家機密保護法之規定，管制出境。</p> <p><input type="checkbox"/>本案涉及資通訊軟體、硬體或服務等相關事務，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。</p>	<p>1、如採購案涉及國家機密者，應勾選此項，執行適任性查核，並依國家機密保護法之規定，管制出境。</p> <p>2、如採購案內涉資通訊軟體、硬體或服務等相關事務，應勾選該項，主要係依 109 年 12 月 18 日行政院資通安全會報第 36 次委員會議紀錄有關資通訊產品使用原則之決定：「.....(2)各機關辦理採購案時，考量資安疑慮，應確實於招標文件規定不允許大陸地區廠商及陸籍人士參與，並不得採購及使用大陸廠牌資通訊產品。」</p>
7 (第 26 頁)	<p>第九條 履約標的品管 (十)廠商作業之檢查與稽核</p> <p>1. 機關得定期或不定期派員檢查或稽核廠商提供之服務是否符合本契約之規定，廠商應以合作之態度在合理時間內提供機關相關書面資料，或協助約談相關當事人。上述提供機關相關書面資料，以法令規定或契約約定者為限，其檢查或稽核得以不預告之方式進行之，廠商不得拒絕。</p> <p>2. 機關得委由專業之第三人稽核廠商提供之服務，費用由機關負擔。</p> <p>3. 廠商作業經機關檢查或稽核結果不符合本契約規定者，需於接獲機關通知期限內改善。</p>	<p>機關得定期或不定期稽核廠商提供之服務是否符合本契約之規定，稽核結果不符合本契約規定者，需於接獲機關通知期限內改善。</p>

項次	條文內容				說明
8 (第 36-38 頁)	<p>第十五條 違約及服務績效違約金</p> <p>(二)履約期間內廠商未達機關所定服務水準及績效，除有不可抗力或不可歸責於廠商事由外，依本款約定計算違約金。屬遲延性質之損害賠償，且已依第 14 條計算逾期違約金者，不再依本款計算違約金。但屬遲延性質之項目依本款計算違約金數額較高者，改依本款計算。依本款計算違約金之總額，以契約價金總額之○○%(由機關於招標時載明，未載明者，為 20%)為上限。服務水準及績效違約金如下：(擇實際需求項目納入，或刪除無需求之項目)。</p> <p>服務水準及績效，列舉如下(同一評估項目具有二種(含)以上之評斷方式者，如廠商同時違反二種(含)以上時，其違約金係採罰責較重者)(註：考量資訊服務採購契約樣態眾多，各機關應衡酌契約實際情況調整資安指標)：</p>				<p>1. 考量資訊服務採購契約樣態眾多，爰於第 2 款新增註解文字，各機關應視契約實際情況調整資安指標，以利後續履約管理。</p> <p>2. 為改善廠商於資安事件之管理、通報及處理情形，爰於第 2 款增訂廠商應依契約辦理資安事件之通報應變等項目及基準，及未依約辦理之計點方式。</p>
	評估項目	評斷方式	要求基準	違約金計點	
	資安指標	對於所維護之系統，未於規定期限取得認證日數	每次認證超過期限	每逾○○日計○點	
		知悉發生資安事件之通報、損害控制或復原作業時效	應於 1 小時內通知機關(或接獲機關通知 1 小時內)，並採取適當之應變措施	每逾○○小時計○點	
	完成損害控制或復原作業之	應於知悉資通安全事件後 72 小時(重	每逾○○小時計○點		

項次	條文內容			說明
	時效	大資安事件為 36 小時)內完成損害控制或復原作業		
	調查及處理資安事件之時效	完成損害控制或復原作業後，應於 1 個月內送交調查、處理及改善報告（或協助機關調查處理）	每逾○○日計○點	
	機關資料之機密性及完整性	機關所擁有之敏感資料應採取適當之防護措施，以避免不當外洩或遭竄改	廠商於本契約承接範圍內，因未採取適當防護，致機關敏感資料外洩或遭竄改時，按受影響資料筆數，每筆計○點/按次數計○點	
	個人資料之機密性及完整性	機關所擁有之個人資料應採取適當之防護措施，以避免不當外洩或遭竄改	廠商於本契約承接範圍內，因未採取適當防護，致機關個人資料外洩或遭竄改時，按受影響資料筆數，每筆計○點/按次數計○點	
9 (第 43-44 頁)	<p>第十六條 權利及責任 (十七)資通安全責任： 1. 廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規定。此外機關保有依機關與廠商同意之適當方式對廠商及其分包廠商以派員稽核、委由資通安全管理法主管機關籌組專案團隊稽核或其他</p>			1、明訂機關辦理資安稽核業務，得標廠商及其分包廠商應予配合；另考量部分機關尚乏自行辦理資安稽核之專業人力或能力，爰允其委託資通安全管理法主管機關(現為行政院)協助辦理，並得依稽核結果通知

項次	條文內容	說明
	<p>適當方式執行相關稽核或查核的權利，稽核結果不符合本契約約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲機關通知後應於期限內完成改善，未依限完成者，依第 14 條第 1 款約定核計逾期違約金。</p> <p>2. 廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，提出安全性檢測證明，涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。廠商於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。</p> <p><input type="checkbox"/> 本案金額達新臺幣一千萬元以上，廠商交付之軟硬體及文件，應接受委託機關或其所委託之第三方進行安全性檢測：..... (其項目由機關於招標時載明)。</p> <p>3. 契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還或移交之，並保留執行紀錄。</p> <p>4. 廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。</p> <p>5. 廠商提供服務，如違反資通安全相關法令、知悉機關或廠商發生資安事件時，均必須於 1 小時內通報機關，提出緊急應變處置，並配合機關做後續處理；必要時，得由資通安全管理法主管機關於適當時機公告與事件相關之必要內容及因應措施，並提供相關協助。</p> <p>6. 廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合機關對系統品質及資通安全的要求。</p> <p>7. 廠商如違反第 1 目至第 6 目規定，應適用第 15 條之違約責任，並就機關所受損害負賠償之責；如致他人權利受有損害時，廠商亦應負責。</p>	<p>得標廠商及分包廠商限期改善。</p> <p>2、廠商交付之軟硬體應提出安全性檢測證明，涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明；採購金額達新臺幣一千萬元以上，廠商應接受委託機關或其所委託之第三方進行安全性檢測。</p> <p>3、契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還或移交之。</p> <p>4、廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理。</p> <p>5、要求廠商於發生資安事件時有立即通報機關之責任，並允許資通安全管理法主管機關(現為行政院)得適時公開資安事件之處置內容等資訊。</p> <p>6、廠商應確實執行組態管理。</p> <p>7、如違反第 1 目至第 6 目規定，應適用第 15 條之違約責任，並就機關所受損害負賠償之責。</p>

項次	條文內容	說明
10 (第 46 頁)	<p>第十八條 契約終止、解除及暫停執行</p> <p>(一)廠商履約有下列情形之一者，機關得以書面通知廠商終止契約或解除契約之部分或全部，且不補償廠商因此所生之損失：</p> <p>13. 違反本契約第 8 條第 6 款第 12 目、第 20 款第 1 目、第 2 目、第 3 目第 1 子目、第 16 條第 15 款或第 17 款第 1 目至第 6 目之情形且有下列之一者： (1)經機關通知改正而未改正，情節重大。 (2)因而致使機關遭受嚴重損害。</p>	<p>明訂機關如未依契約規定(分包商配合受稽核、履約之資通安全責任)，致機關遭受嚴重損害者，得終止、解除及暫停執行契約。</p>
11 (第 46 頁)	<p>第十八條 契約終止、解除及暫停執行</p> <p>(一)廠商履約有下列情形之一者，機關得以書面通知廠商終止契約或解除契約之部分或全部，且不補償廠商因此所生之損失：</p> <p>15. 本採購如屬經濟部投資審議委員會網站公告之「具敏感性或國安(含資安)疑慮之業務範疇」，廠商於履約期間因股份或資本額變動而成為經濟部投資審議委員會網站公告之陸資資訊服務業者。</p>	<p>廠商於履約期間因股份或資本額變動而成為陸資資訊服務業者，機關得以書面通知廠商終止契約或解除契約之部分或全部，且不補償廠商因此所生之損失。</p>
12 (第 51-52 頁)	<p>第二十條 保密及安全需求 (一)廠商承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務未標示得對外公開之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，廠商不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將</p>	<p>明訂各項保密及安全需求。</p>

項次	條文內容	說明
	<p>之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。</p> <p>(二)廠商知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。廠商同意本條所定公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之廠商團隊成員，並應要求該等人員簽署與本條款內容相同之保密同意書。</p> <p>(三)廠商在下述情況下解除其依本條所應負之保密義務：</p> <ol style="list-style-type: none"> 1. 廠商原負保密義務之資訊，由機關提供以前，已為廠商所合法持有或已知且無保密必要者。 2. 廠商原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所週知之資訊。 3. 廠商原負保密義務之資訊，係廠商自第三人處得知或取得，該第三人就該等資訊並無保密義務。 <p>(四)廠商保證其派至機關提供勞務之派駐勞工於機關工作期間以及本契約終止後，在未取得機關之書面同意前，不得向任何人、單位或團體透露任何業務上需保密之文件及資料。且廠商保證所派駐人員於契約終止(或解除)時，應交還機關所屬財產，及在履約期間所持有之需保密之文件及資料。</p> <p>(五)前款所稱保密之文件及資料，係指：</p> <ol style="list-style-type: none"> 1. 機關在業務上認為不對外公開之一切文件及資料，包括與其業務或研究開發有關之內容。 2. 與廠商派至機關提供勞務之派駐勞工的工作有關，其成果尚不足以對外公布之資料、訊息及文件。 3. 依法令須保密或受保護之文件及資料，例如個人資料保護法所規定 	

項次	條文內容	說明
	<p>者。</p> <p>(六)廠商同意其人員、代理人或使用人如有違反本條或其自行簽署之保密同意書者，視同廠商違反本條之保密義務。</p> <p>(七)其餘涉及資通安全事項，由機關視個案實際需要，依行政院國家資通安全會報技術服務中心(網址：https://nccst.nat.gov.tw/)共通規範辦理，例如「政府資訊作業委外安全參考指引」與資通安全有關事項。</p>	