本所採購　　　　　　　　　　　　　　　(以下簡稱本案)之資安要求事項及驗收文件如下：

本案資通系統防護需求分級為：[ ] 高 [ ] 中 [ ] 普

本案為：[ ] 資通系統開發 [ ] 資通系統增修或維護(第三項免辦理) 廠商或代理人章：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 項次 | 要求事項 | 依分級結果執行措施 | 驗收條件(辦理情況說明) | 是否符合 |
| 高 | 中 | 普 |
| 一 | 依本所要求進行資通系統安全性檢測，安全性檢測應使用取得授權的商用軟體，並將弱點資料庫更新至最新版本。 | 商用安全性檢測軟體弱點資料庫最新版本證明。 |  |
| 二 | 於系統開發階段依分級執行「源碼掃描」安全檢測，及依據本所｢資通安全責任等級分級辦法｣執行｢附表十所定資通系統防護基準｣ | 移除「源碼掃描」所有風險，並具備系統嚴重錯誤通知機制，及等級｢普｣之所有控制措施。 | 應依據本所｢資通安全責任等級分級辦法｣執行｢附表十所定資通系統防護基準｣。 | [高]，完成所有普中高措施。[中、普]，知悉資通系統防護需求查檢表\*註相關要求事項。 |  |
| 三 | 於系統開發交付測試時完成「滲透測試」之安全檢測，並依本所要求修正。 | 移除「滲透測試報告」之所有風險。 | 免辦理 | 免辦理 | [高]，移除滲透測試所有風險。 |  |
| 四 | 於系統測試或系統維護階段執行「弱點掃描」之安全檢測，並依本所要求修正。 | 移除「弱點掃描報告」之所有風險。 | 移除「弱點掃描報告」之最高風險。 | [高]，移除弱掃報告所有風險。[中、普]，移除弱掃報告最高風險。 |  |
| 五 | 跡證保存，於開發設計或維護階段，依本所「資訊安全事件管理程序書」之6.5規定事項辦理。 | Log紀錄保存項目：1. 作業系統日誌(OS event log)、2. 網站日誌(Web log)、3. 應用程式日誌(AP log)、4. 登入日誌(Logon log)。 | log紀錄保存設計。 |  |
| 六 | 若本所自行或另行委託第三方進行安全性檢測，應依檢測結果修正風險。 | 委託金額一千萬以上：移除「弱點掃描報告」所有風險。委託金額未達一千萬：移除「弱點掃描報告」最高風險。 | [ ]  另辦理安全性檢測：[一千萬以上]移除所有風險。[一千萬以下]移除最高風險。 |  |

確認應辦事項是否符合，並於結案時繳回資訊管理單元

 註：資通系統防護需求查檢表，請參考下列網址擇一下載：

1. 資通安全責任等級分級辦法附表十資通系統防護基準
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304>
2. 所內公告 > 資訊管理 > 資安政策及規範 > 資通訊系統作業流程 > 資通安全相關表單(限所內同仁)
<https://www.firdi.org.tw/Bulletins_List.aspx?BulletinTypeID=213>

請購人/專案負責人簽名：

(已知悉廠商應辦事項)

日期：

流程：立案填寫 > 結案繳回資訊管理單元