第2部——"資訊安全"

註釋：

1. *(由2021年第89號法律公告廢除)*

2. 類別5第2部不適用於被用戶攜帶作私人用途的產品。

3. *密碼學註釋：*

項目5A002、5D002(a)(1)、5D002(b)及5D002(c)(1)不適用於以下物品： *(2021年第89號法律公告)*

(a) 符合以下所有描述的物品：

(1) 在零售點，以下列任何方式將存貨普遍而無限制地售予公眾：

(a) 門市交易；

(b) 郵購交易；

(c) 電子交易；

(d) 電話訂購交易；

(2) 密碼功能不能被用户輕易更改；

(3) 該物品的設計可供用户在無需供應商進一步大量支援下自行安裝；

(4) 已刪除；

(5) 在需要時，可應要求讓出口國有關主管當局查閱該物品的詳情並將該等詳情提供予該主管當局，以確定該物品符合上文(a)(1)、(2)及(3)段的描述；

(b) 為本註釋(a)段所描述的現有物品而設計、符合下列所有描述的硬部件或'可執行軟件'： *(2015年第27號法律公告)*

(1) "資訊安全"並非該部件或'可執行軟件'的首要功能或功能組合；

(2) 該部件或'可執行軟件'沒有改變該等現有物品的任何密碼功能，亦沒有為該等現有物品加入新密碼功能；

(3) 該部件或'可執行軟件'的特性設定是固定的，而非按顧客的指示而設計或改裝；

(4) 在出口國有關主管當局決定有需要時，可應要求讓該主管當局查閱該部件或'可執行軟件'和有關最終物品的詳情並提供該等詳情予該主管當局，以確定該部件或'可執行軟件'符合上文(b)(1)、(2)及(3)段的描述。 *(2015年第27號法律公告)*

技術註釋：

就密碼學註釋而言，'可執行軟件'指出自被密碼學註釋豁除於項目5A002之外的現有硬部件的、屬可執行形式的"軟件"。 *(2015年第27號法律公告)*

註釋：

'可執行軟件'不包括在最終物品運行的"軟件"的完整二進制影像。 *(2015年第27號法律公告)*

密碼學註釋的註釋：

1. 為符合註釋3的(a)段，以下各項須適用：

(a) 有多類別個人及行業可能對有關物品有興趣；

(b) 在購買前可獲取有關物品的價錢和主要功能的資料，而無需向售銷者或供應商查詢。簡單的價錢詢問，並不視為查詢。 *(2021年第89號法律公告)*

2. 在斷定註釋3的(a)段時，各國家當局可考慮有關因素，例如數量、價錢、技術要求、現有銷售途徑、典型顧客、典型用途或供應商任何排斥性的做法。 *(2013年第89號法律公告)*

4. *(由2021年第89號法律公告廢除)*

(2010年第45號法律公告)

技術註釋：

(由2015年第27號法律公告廢除)

5A2 系統、裝備及部件

5A002 以下的"資訊安全"系統、裝備及部件：

注意：

至於包含或利用解密技術的"衞星導航系統"接收裝備，參閱項目7A005；而至於相關的解密"軟件"及"技術"，參閱項目7D005及7E001。

(a) 以下經設計或改裝以使用設有'說明的保安演算法'的'資料機密性密碼學'的物品，而有關密碼功能在不使用安全機制的情況下，可藉"啟動密碼"方式使用或啟動，或已藉該方式啟動：

(1) 以"資訊安全"為首要功能的物品；

(2) 並非項目5A002(a)(1)指明的數碼通訊或網絡連結系統、裝備或部件；

(3) 並非項目5A002(a)(1)或5A002(a)(2)指明的電腦、其他以資料儲存或處理為首要功能的物品及該等物品的部件；

注意：

至於作業系統，亦須參閱項目5D002(a)(1)及5D002(c)(1)。

(4) 並非項目5A002(a)(1)、5A002(a)(2)及5A002(a)(3)指明的物品，而其設有'說明的保安演算法'的'資料機密性密碼學'功能符合以下所有說明：

(a) 支援物品的非首要功能；

(b) 由經裝嵌的裝備或"軟件"執行，而該裝備或"軟件"作為獨立物品時，屬類別5第2部指明者；

技術註釋：

1. 就項目5A002(a)而言，'資料機密性密碼學'指利用數碼技術並執行任何密碼功能(以下任何一項除外)的"密碼學"：

(a) "核證"；

(b) 數碼簽署；

(c) 資料完整性；

(d) 不可否認性；

(e) 數碼權管理，包括執行原件受保護的"軟件"；

(f) 支援娛樂、大眾商業廣播或醫療紀錄管理的加密或解密；

(g) 支援本註釋(a)至(f)段所述任何功能的關鍵字管理。

2. 就項目5A002(a)而言，'說明的保安演算法'指以下任何一項：

(a) 使用長度超過56位元(奇偶檢驗位並不包括在內)的密碼匙的"對稱演算法"；

(b) 算法保密性以下列任何一項為基準的"非對稱演算法"：

(1) 超過512位元因子公解法的整數(例如：RSA)；

(2) 在具有大於512位元的乘法群的有限域中將離散對數計算機化(例如：迪菲—赫爾曼技術(Diffie-Hellman)在於Z/pZ)；

(3) 在本註釋(b)(2)段所述者以外超過112位元的乘法群中的離散對數(例如：迪菲—赫爾曼技術(Diffie-Hellman)在於橢圓曲線)；

(c) 算法保密性以下列任何一項為基準的"非對稱演算法"：

(1) 與格(lattices)(例如：NewHope、Frodo、NTRUEncrypt、Kyber、Titanium)相關的最短向量或最近向量問題；

(2) 在超奇異橢圓曲線之間找尋同源(例如：超奇異同源密鑰封裝(Supersingular Isogeny Key Encapsulation))；

(3) 解讀隨機碼(例如：McEliece、Niederreiter)。

技術註釋：

技術註釋2(c)所描述的算法可稱為後量子算法、量子安全算法或抗量子算法。

註釋：

1. 當出口國有關主管當局決定屬有需要時，須應要求讓該主管當局查閱有關物品的詳情，並將該等詳情提供予該主管當局，以確立是否符合以下任何一項：

(a) 有關物品是否符合項目5A002(a)(1)至5A002(a)(4)的準則；

(b) 項目5A002(a)指明的資料機密性密碼功能，是否可於沒有"啟動密碼"的情況下使用。

2. 項目5A002(a)不管制以下任何一項物品或該等物品的特別設計"資訊安全"部件：

(a) 以下的智能卡及智能卡'讀卡器／寫卡器'：

(1) 符合以下任何一項說明的智能卡或可作電子閱讀的個人證件(例如代幣、電子護照)：

(a) 符合以下所有說明的密碼功能：

(1) 限使用於以下任何一項：

(a) 並非項目5A002(a)(1)至5A002(a)(4)所描述的裝備或系統；

(b) 不使用設有'說明的保安演算法'的'資料機密性密碼學'功能的裝備或系統；

(c) 藉本註釋(b)至(f)段豁除於項目5A002(a)之外的裝備或系統；

(2) 該功能的程式不能被重新編排作任何其他用途；

(b) 符合以下所有描述：

(1) 經特別設計並只限保障內存'個人資料'之用；

(2) 已被個人化或只能個人化以作公眾或商業交易或個人識別用途；

(3) 密碼功能並非使用者可取得；

技術註釋：

'個人資料'包括關於某人或某實體的任何特定資料，例如所儲存的金額及進行"核證"所需的資料。

(2) 為本註釋(a)(1)段指明的物品而特別設計或改裝，並只限用於該等物品的'讀卡器／寫卡器'；

技術註釋：

'讀卡器／寫卡器'包括透過網絡跟智能卡或可作電子閱讀的文件連繫的裝備。

(b) 經特別設計並只限用於銀行或'貨幣交易'方面的密碼裝備；

技術註釋：

項目5A002(a)註釋2(b)中的'貨幣交易'包括費用的收取及結算或信貸功能。

(c) 符合以下說明的民用(例如配合商業民用蜂巢式無線電通訊系統一起使用)手提或流動式無線電話：不能直接傳送加密數據至其他無線電話或設備(無線電接入網絡裝備除外)，亦不能經無線電接入網絡裝備(例如無線電網絡控制器(RNC)或基地電台控制器(BSC))轉移加密數據；

(d) 不具備終點至終點加密能力，且製造商指明其沒有功率放大的無線操作的最大有效範圍(即終點與家居據點之間的唯一無中繼距程)少於400米的無線電話裝備；

(e) 民用手提或流動式無線電話和類似的客户無線裝置，而該等電話或裝置只採用已公布或商用密碼標準(可能未經公布的反盜版功能除外)，並符合密碼學註釋(類別5第2部註釋3)(a)(2)至(4)段的條文，且已調整其功能作特定的民間工業用途，而該等功能不影響原本未作調整的裝置的密碼功能；

(f) "資訊安全"功能只限於無線"個人區域網絡"功能兼符合以下所有描述的物品：

(1) 只採用已公布或商用密碼標準；

(2) 按照製造商的說明，密碼功能的標稱操作範圍限於30米或以下；或按照製造商就不能與多於7個裝置互相連結的裝備的說明，密碼功能的標稱操作範圍限於100米或以下；

(g) 設計供民用，並符合密碼學註釋(類別5第2部註釋3)(a)(2)至(4)段的條文的流動通訊無線電接入網絡裝備，而該裝備具有的射頻輸出功率限於0.1瓦(20 dBm)或以下，以及支援16名或以下同步使用者；

(h) 路由器、轉換器或中繼器，而"資訊安全"功能只限採用已公布或商用密碼標準的"操作、管理或維修"任務；

(i) 一般用途電腦裝備或伺服器，但以"資訊安全"功能符合以下所有描述為限：

(1) 只採用已公布或商用密碼標準；

(2) 屬以下任何一項：

(a) 與符合類別5第2部註釋3的條文的中央處理器一體化；

(b) 與並非項目5D002指明的作業系統一體化；

(c) 限於"操作、管理或維修"該裝備；

(j) 為'連接的民間工業用途'而特別設計的，兼符合以下所有描述的物品：

(1) 屬以下任何一項：

(a) 符合以下任何描述、具網絡功能的端點裝置：

(1) "資訊安全"功能限於獲取'非任意資料'或"操作、管理或維修"任務；

(2) 該裝置限於特定的'連接的民間工業用途'；

(b) 符合以下所有描述的網絡連結裝備：

(1) 特別設計供與本註釋(j)(1)(a)段指明的裝置通訊；

(2) "資訊安全"功能限於支援本註釋(j)(1)(a)段指明的裝置的'連接的民間工業用途'，或本網絡連結裝備或本註釋(j)段指明的其他物品的"操作、管理或維修"任務；

(2) "資訊安全"功能只採用已公布或商用密碼標準，而密碼功能不能被用户輕易更改。

技術註釋：

1. '連接的民間工業用途'是連接至網絡的消費者或民間工業用途，而該用途並不包括"資訊安全"、數碼通訊、一般網絡連結或電腦用途。

2. '非任意資料'指直接關乎系統穩定性、性能或物理測量(如溫度、壓力、流速、質量、容量、電壓、物理位置等)的感測器或度量資料，而該等'非任意資料'不能被有關裝置的用户更改。

(b) 作為'啟動密碼權標'；

技術註釋：

'啟動密碼權標'是為以下任何用途而設計或改裝的物品：

(a) 藉"啟動密碼"，將並非類別5第2部指明的物品，轉換成項目5A002(a)或5D002(c)(1)指明而不獲密碼學註釋(類別5第2部註釋3)豁免的物品；

(b) 藉"啟動密碼"，使已在類別5第2部指明的物品，能夠執行項目5A002(a)指明的附加功能。

(c) 經設計或改裝以使用或執行"量子密碼技術"；

技術註釋：

"量子密碼技術"亦稱為量子密碼匙分配(QKD)。

(d) 經設計或改裝以使用密碼技術產生頻道碼、擾碼或網絡辨識碼，供用於使用超寬頻調變技術的系統，並符合以下任何描述：

(1) 頻寬超過500兆赫；

(2) "分頻寬"為20%或以上；

(e) 經設計或改裝以使用密碼技術，產生用於項目5A002(d)所指明者以外的"展頻"系統的延展碼(包括用於"跳頻"系統的跳躍碼)；

(2021年第89號法律公告)

5A003 以下的非編碼"資訊安全"的系統、裝備及部件：

(a) 經設計或改裝以使用機械、電機或電子方法偵測暗中入侵者的通訊纜線系統；

註釋：

項目5A003(a)只管制物理層保安。就項目5A003(a)而言，物理層包括開放式系統互連(OSI)參考模型(ISO/IEC 7498-1)的第1層。

(b) 經特別設計或改裝以減低超出健康、安全或電磁干預標準所需的、帶有資訊的訊號的折衷發送；

(2021年第89號法律公告)

5A004 以下為解除、削弱或繞過"資訊安全"的系統、裝備及部件：

(a) 經設計或改裝以執行'破解密碼功能'；

註釋：

項目5A004(a)包括為以逆向工程方法執行'破解密碼功能'而設計或改裝的系統或裝備。

技術註釋：

'破解密碼功能'是為解除密碼機制而設計的功能，藉以導出機密變數或敏感資料(包括清晰的原文、密碼或密碼關鍵字)。

(2021年第89號法律公告)

5B2 測試、檢驗及生產裝備

5B002 以下的"資訊安全"測試、檢驗及"生產"裝備：

(a) 為"發展"或"生產"項目5A002、5A003、5A004或5B002(b)指明的裝備而特別設計的裝備；

(b) 為評估及驗證項目5A002、5A003或5A004指明的裝備或項目5D002(a)或5D002(c)指明的"軟件"的"資訊安全"功能而特別設計的測量裝備；

(2009年第226號法律公告；2021年第89號法律公告)

5C2 物料

無；

5D2 軟件

5D002 (a) 為"發展"、"生產"或"使用"以下任何一項，而特別設計或改裝的"軟件"：

(1) 項目5A002指明的裝備或項目5D002(c)(1)指明的"軟件"；

(2) 項目5A003指明的裝備或項目5D002(c)(2)指明的"軟件"；

(3) 項目5A004指明的裝備或項目5D002(c)(3)指明的"軟件"； *(2021年第89號法律公告)*

(b) 具有項目5A002(b)指明的'啟動密碼權標'特性的"軟件"； *(2021年第89號法律公告)*

(c) 具有以下任何裝備的特性的"軟件"，或執行或模擬以下任何裝備的功能的"軟件"：

(1) 項目5A002(a)、5A002(c)、5A002(d)或5A002(e)指明的裝備；

註釋：

項目5D002(c)(1)不管制只限採用已公布或商用密碼標準的"操作、管理或維修"任務的"軟件"。

(2) 項目5A003指明的裝備；

(3) 項目5A004指明的裝備； *(2021年第89號法律公告)*

(d) *(由2021年第89號法律公告廢除)*

(2009年第226號法律公告；2013年第89號法律公告)

5E2 技術

5E002 以下的"技術"：

(a) 按照一般技術註釋，供"發展"、"生產"或"使用"項目5A002、5A003、5A004或5B002指明的裝備或項目5D002(a)或5D002(c)指明的"軟件"的"技術"； *(2021年第89號法律公告)*

(b) 具有項目5A002(b)指明的'啟動密碼權標'特性的"技術"； *(2021年第89號法律公告)*

註釋：

項目5E002包括在執行評估或釐定類別5第2部指明的功能、特性或技術的程序中產生的"資訊安全"技術資料。 *(2013年第89號法律公告)*

(2011年第161號法律公告)