出國報告（出國類別：其他）

臺灣銀行支援在美分行資通安全事務報告

服務機關：臺灣銀行股份有限公司
姓名職稱：國際部 王育貞 經理
資通安全處 陳俊甫 領組
派赴國家：美國紐約、美國洛杉磯
出國期間：112 年 12 月 10 日至 112 年 12 月 23 日
報告日期：113 年 2 月 22 日

摘　　要

美國紐約州金融服務署（NYDFS）自 2017 年 3 月 1 日發布金融服務業網路安全要求規範(23 NYCRR 500：Cybersecurity Requirements for Financial Services Companies, 簡稱 Part 500)，要求金融服務機構應以風險基礎建立及維護網路安全計畫，指派首席資安官(Chief Information Security Officer, CISO)確保網路安全計畫的執行情況，每年須向其董事會或同等管理階層提交網路安全年度合規報告書，並於 NYDFS 網站完成線上簽署作業。有鑑於日益嚴峻的資安威脅，資安攻擊工具越來越容易被取得，NYDFS 於 2023 年 11 月 1 日賡續發布金融服務業網路安全要求第二修正版(Second Amendment)，修正原有規定使其更加完整，並新增額外的管控措施，如 Class A 機構每年應針對網路安全計畫實施獨立稽核等，以提升美國紐約州金融服務適法機構整體資安防護。

本行紐約分行 CISO 為向董事會提報紐約分行年度合規報告書，特委託獨立第三方顧問執行 Part 500 合規檢視，確認整體資安作業符合 Part 500 法規要求，另外，NYDFS 發布 Part 500 第二修正版，及紐約分行 CISO 每半年須協助本行洛杉磯分行強化資訊安全管控及行員資訊安全知能，為利前揭各項作業順利執行，及總行對海外分行落實資安的重視，經奉總經理核准，由本行國際部經理及資通安全處同仁，於 112 年 12 月 10 日至 12 月 23 日赴本行紐約分行及洛杉磯分行，協助在美分行完善整體資訊安全防護措施，符合在美分行當地金融資安相關法規要求。

目　　次

壹、目　的

美國紐約州金融服務署（NYDFS）於 2017 年 3 月 1 日發布初版的金融服務業網路安全要求規範(23 NYCRR 500：Cybersecurity Requirements for Financial Services Companies, 簡稱 Part 500)，並於 2023 年 11 月 1 日發布 Part 500 第二修正版，要求金融服務機構應以風險基礎建立及維護網路安全計畫，指派首席資安官(Chief Information Security Officer, CISO)確保網路安全計畫的執行情況，每年須向其董事會或同等管理階層提交年度網路安全合規報告書，並於 NYDFS 網站完成線上簽署作業。適逢本行紐約分行委外辦理 Part 500 查核作業、年度委任協議重新檢視作業、因應 Part 500 第二修正版差異分析及紐約分行 CISO 每半年支援洛杉磯分行強化資安知能等，經奉總經理核准，由本行國際部經理及資通安全處同仁，於 112 年 12 月 10 日至 12 月 23 日赴本行紐約分行及洛杉磯分行進行訪視作業，協助在美分行完善資訊安全防護措施，符合在美分行當地金融資安相關法規要求。

貳、作業過程

本次訪視作業由國際部王經理育貞及資通安全處陳領組俊甫，自 12 月 11 日搭機飛往美國紐約，於 12 月 12 日至 12 月 19 日協助紐約分行辦理 Part 500 等資安相關事務，於 12 月 20 日至 12 月 21 日協助紐約分行 CISO 赴洛杉磯分行辦理資訊安全管控及宣導行員資訊安全知能相關作業，於 12 月 22 日返國。本次訪視重點有協助紐約分行配合獨立委外 Part 500 合規檢查、Part 500 第二修正版差異分析、研擬分行與總行間服務委任協議修正內容、及協助紐約分行 CISO 強化洛杉磯分行資訊安全管控及行員資訊安全知能訓練等作業。本次出國訪視作業依規定作成出國報告陳核，作業過程說明如下：

一、訪視準備

訪視同仁於出訪前先蒐集及檢視紐約分行 Part 500 相關資料，包括分行資訊及資安相關規範、NPI 資訊資產清冊、網路架構圖、資安評估報告改善情形等，由訪視人員先行審閱及問題整理，實地赴分行與當地同仁確認，並因應紐約州金融服務署公布 Part 500 第二修正版，預先瞭解本次 Part 500 修正內容及相關應注意事項，以利本次訪視作業順利進行。

二、訪視重點

本次訪視重點說明如下：

(一) 依紐約金融服務業網路安全要求規範(23 NYCRR Part 500) Section 500.04(b)及 Section 500.17(b)規定，紐約分行 CISO 每年應向董事會或同等管理階層提交書面報告，報告紐約分行網路安全計畫和重大網路安全風險，紐約分行 2023 年度合規報告書將委由總行資通安全處代為提報董事會，由董事會授權同意紐約分行於 NYDFS 數位簽署平台完成合規簽署作業。紐約分行為確認各項資訊作業之安全管控措施符合 Part 500 規範要求，委託獨立第三方顧問於 2023 年 12 月 14 日至 19 日實地執行合規審查作業，為利審查作業順利進行，由總行資通安全處同仁先行協助紐約分行確認各項資訊作業之安全管控措施，及檢視委外合規審查相關準備資料。

(二) 因應 NYDFS 頒布 Part 500 第二修正版(Second Amendment)，法規生效日為 2023 年 11 月 1 日，NYDFS 給予受監管金融機構不同緩衝時間來落實 Part 500 第二修正版條文，其中第二修正版之 Section 500.17(通報機制)，須於生效後 30 日內(2023 年 12 月 1 日前)合規，要求受監管的金融機構須於 4 月 15 日前於 NYDFS 網站簽署前一年度合規聲明，合規聲明須由最高執行階層及紐約分行資安主管(CISO)共同簽署，合規聲明相關文件資料須保留 5 年，其餘修訂項目，Section 500.22 訂有緩衝期，為利紐約分行遵

循及落實 Part 500 第二修正版各項要求，協助紐約分行辦理 Part 500 第二修正版差異分析，並提供相關建議。

(三) 紐約分行與總行資訊處及資通安全處已有簽署資訊服務委任協議，依據協議每年應重新檢視協議內容，已符合最新資訊作業發展，適逢年度委任協議重新檢視期間，及紐約當地頒布 Part 500 第二修正版，為確保海外分行委任資訊作業順利運作，符合海外當地主管機關法規要求，協助紐約分行檢視及修正資訊服務委任協議，並提供相關建議。

(四) 紐約分行資安主管(CISO)應每半年赴洛杉磯分行，協助洛杉磯分行強化資訊安全管控及行員資訊安全知能，包括規範文件修訂檢視、安全檢測、資安事件應變演練、教育訓練等，提供洛杉磯分行資安諮詢及管理，為加強在美分行資訊安全管控，協同紐約分行資安主管(CISO)赴洛杉磯分行執行前揭作業，並視洛杉磯分行需求提供相關協助。

三、訪視經過

(一) 2023/12/10-11：啟程前往美國紐約，本次為臨時訪視配合出國航班，國際部王經理於 12 月 10 日出發，資通安全處同仁於 12 月 11 日出發。

(二) 2023/12/12-19：

1. 依據 Part 500 要求，協助檢視紐約分行網路安全計畫(Cybersecurity Program)、網路安全政策(Cybersecurity Policy)、資訊科技政策及程序(IT Policy and Procedures)、廠商管理政策及程序(Vendor Management Policy and Procedures)、持續營運管理政策(Business Continuity Management Policy)等文件，確認紐約分行資安主管(CISO)是否有落實定期檢視，以符合資訊資安發展現況。
2. 依據 Part 500 要求，協助檢視紐約分行非公開資訊(Nonpublic Information，NPI)清冊、資安風險評估報告、網路架構圖、備份管理作業、營運持續計畫演練紀錄、弱點掃描及滲透測試報告改善情形、資訊系統帳號權限清查紀錄、資訊安全教育訓練等，確認各項資訊作業已遵循 Part 500 及分行所定規範。
3. 紐約分行委託獨立第三方顧問於 12 月 14 日至 19 日執行合規審查作業，查

核顧問已依據 Part 500 各項條文擬定資料調閱清單，並請紐約分行依調閱清單先行準備。訪視同仁協助紐約分行整理相關調閱資料，確認準備資料之完整性，並協助紐約分行配合第三方顧問辦理查核作業。

4. 本行紐約分行已有建立備援中心，採冷備援方式，為確認紐約分行備援機制是否可順利運作，協同分行同仁及本次委外查核顧問實地赴紐約分行備援機房，前往當日適逢紐約州下大雨，從分行出發抵達備援機房車程時間約 30 分鐘左右，抵達後由分行同仁模擬異地備援啟動，實地架設備援機房設備並連線總行資訊系統，測試結果可正常連線，確認分行備援機制正常運作，分行營運持續計畫尚屬妥適。
5. 紐約分行資訊作業部分委任總行管理，與總行資訊處及資通安全處已簽署資訊作業委任總行管理服務協議，依協議每年應重新檢視協議內容，以符合資訊作業發展現況，因應 NYDFS 頒布 Part 500 第二修正版，紐約分行已完成差異分析，部分控制措施須委任總行協助，與紐約分行共同研議委任協議相關修正重點，如分行 NPI 資訊資產清冊之資訊系統及設備日誌集中收容與監控作業等，以利提報 112 年度海外分行資訊作業委任總行管理服務審查會議討論。
6. 紐約分行 CISO 應每半年赴洛杉磯分行，協助洛杉磯分行強化資訊安全管控及行員資訊安全知能，作業項目包括資訊資安相關規範檢視、資安檢測弱點修補情形、資訊系統權限清查作業、資訊安全風險評估、內外部資訊稽核相關改善情形、網路安全事件應變演練等，紐約分行 CISO 已研擬相關作業期程表、安全檢核表、資安事件應變演練計畫(含演練情境)及教育訓練等資料，訪視同仁協助審視並提供相關建議，供紐約分行 CISO 參考調整。
7. 訪視同仁彙整每日訪視進度，及定期與總行召開討論會議，報告委外查核進度、討論紐約分行 Part 500 第二修正版差異分析、委任協議修正重點及紐約分行 CISO 協助強化洛杉磯分行資訊安全管控及行員資訊安全知能相關規劃等，以利總行掌握在美分行資安作業。

(三) 112/12/20-21：隨同紐約分行 CISO 赴洛杉磯分行，協助執行洛杉磯分行資訊安全管控及行員資訊安全知能相關作業，包括檢視洛杉磯分行資訊及資安相關政策、程序及標準作業流程手冊等文件，確認洛杉磯分行安全檢測改善辦理情形，確認洛杉磯分行資訊系統權限控管作業，及確認資訊安全風險評

估等相關事項，另外，協同紐約分行 CISO 與洛杉磯分行同仁共同研擬網路安全事件應變演練計劃，本次演練情境為社交工程演練及勒索軟體，並協同執行應變演練，演練採桌面演練方式進行，分行同仁模擬誤開啟惡意郵件，導致工作站檔案全遭加密，分行立刻拔除網路線，並同步通報分行經副理及紐約分行 CISO，清查受影響範圍，清查結果僅單一工作站受影響，且該工作站為外網工作站，不影響分行業務，故重新安裝工作站作業系統，並再次宣導同仁應防範惡意電子郵件之攻擊，勿開啟與公務非相關之郵件、連結或檔案，演練作業順利執行，演練過程同仁也有相互交流意見，紐約分行 CISO 及訪視同仁也分享國內及紐約分行的作業，供洛杉磯分行同仁參考。

(四) 112/12/22-23：從洛杉磯搭機返國。

叁、訪視結果與建議

本次訪視作業，實地協助紐約分行檢視 Part 500 各項資訊安全作業執行情形，包括網路安全計畫、網路安全政策、紐約分行 CISO 職責、滲透測試、弱點掃描等，並就紐約分行委託獨立第三方顧問辦理 Part 500 查核作業，協助提供總行資安相關作業之說明，以利查核作業順利進行，經委外顧問評估結果，紐約分行有關遵循及落實 Part 500 各項資訊安全作業尚屬合適，無重大發現事項，另有強化建議事項，紐約分行已依查核建議研擬相關強化，並於 2024 年 1 月完成強化作業，經顧問確認無意見。紐約分行 CISO 將依評估結果出具年度合規報告書，並委託總行資安單位代為提報董事會，由董事會授權紐約分行最高執行階層主管及紐約分行 CISO，於 Part 500 所規定時限內(4 月 15 日前)至 NYDFS 網站共同簽署紐約分行合規聲明。

因應 NYDFS 頒布 Part 500 第二修正版(Second Amendment)，法規生效日為 2023 年 11 月 1 日，本次修訂內容，除 Section 500.17 須於生效日起 30 天內（2023 年 12 月 1 日前）符合規範，紐約分行已配合修正網路安全政策及網路安全控管 SOP，並遵循相關規範辦理，其餘修正項目，Section 500.22 提供受監管金融機構不同緩衝時間來落實遵循，紐約分行已就本次第二修正版完成差異分析，經評估部分事項尚屬合規，尚未符合之事項，紐約分行已研擬預計辦理方式及預計完成日期，後續將依規劃逐步落實

各項資訊安全管控，並於法規要求過渡期限前完成，以符合法規要求，紐約分行 Part 500 第二修正版差異分析將併同年度合規報告書提報董事會，以利董事會掌握紐約分行落實 Part 500 最新執行情形。

紐約分行資訊作業部分委任總行管理，與總行資訊處及資通安全處已簽署資訊作業委任總行管理服務協議，依協議每年應重新檢視協議內容，以符合資訊作業發展現況，總行已訂於 2024 年 2 月召開 112 年度海外分行資訊作業委任總行管理服務審查會議，本次訪視亦協助紐約分行重新檢視委任總行管理服務協議，並提供相關建議予分行，紐約分行已依建議修正委任總行管理服務協議，並報送委任協議簽署單位共同檢視，及提報 112 年度海外分行資訊作業委任總行管理服務審查會議審議，經會議討論確認三方皆無意見後，完成年度委任協議檢視作業，後續由三方依委任協議辦理各項作業，並每季提供服務報告予分行。

為落實本行在美分行資訊安全管控，紐約分行 CISO 應每半年赴洛杉磯分行，依「紐約分行 CISO 協助並強化在美分支機構資訊安全管控及強化在美單位資訊安全知能表」，協助並強化洛杉磯分行資訊安全管控及行員資訊安全知能。紐約分行 CISO 排定於 2023 年 12 月 20 日至 12 月 27 日間，赴洛杉磯分行執行前揭作業，本次訪視同仁因出差時程安排，僅協助至 12 月 22 日止，後續由紐約分行 CISO 獨立執行，本次強化作業皆順利完成，包括檢視洛杉磯分行資訊及資安相關政策、程序及標準作業流程手冊等文件，確認洛杉磯分行安全檢測改善辦理情形，確認洛杉磯分行資訊系統權限控管作業，確認資訊安全風險評估結果，辦理網路安全事件應變演練，FedLine Attestation 檢視作業等，紐約分行 CISO 已出具「洛杉磯分行網路安全作業支援情形報告」，提供洛杉磯分行作後續資安強化。

綜上說明，本次訪視所規劃支援在美分行資安作業，皆已順利完成，建議紐約分行針對 Part 500 尚未合規事項持續追蹤，及協助洛杉磯分行持續強化資安管控及行員資安知能，另外，因應紐約聯邦儲備銀行(Federal Reserve Bank of New York)及紐約分

行委託獨立第三方顧問已排定於 2024 年赴分行辦理查核作業與 IT 風險評估作業，建議紐約分行先預作準備，持續與總行保持聯繫與溝通，並洽請總行國際部邀集資訊處、資通安全處等相關部處召開線上會議，以協助分行資安業務順利運行，最後，感謝總行給予這次實地訪視的機會，讓訪視同仁更加瞭解海外分行當地法規的要求，及掌握海外分行資安作業執行情形，對後續總行規劃海外分行資安業務上有很大的助益，本次訪視作業，亦與海外分行當地資訊/資安業務同仁建立良善的互動，彼此交流執行資訊資安業務的經驗與困難，以逐步完善本行整體的資安防護措施。