調　查　報　告　（公布版）

壹、案　　由：據悉，113及114年間媒體報導外交部文件遭暗網兜售等情案。

貳、調查意見：

民國（下同）113及114年間，媒體報導外交部文件遭置於暗網兜售，案經調閱行政院[1]、外交部[2]、國家安全局[3]（下稱國安局）等機關卷證資料，並於115年4月28日詢問行政院外交國防法務處處長、政風處處長、資訊處副處長，與外交部主任秘書、數位發展部（下稱數發部）資通安全署（下稱資安署）署長及法務部廉政署（下稱廉政署）副署長等機關人員，已調查竣事，茲臚列調查意見如下：

一、外交部及相關機關之公文書於113年至114年間，屢遭不法人士於暗網揭露並公開兜售，案經司法機關立案偵辦，目前尚未偵結。惟查，外交部於113年案發之初，僅憑初步資訊鑑識及行政調查結果，即率爾排除機關公文系統遭駭侵之可能；迨114年再次發生同類事件，該部經比對公文內容雷同，研判損及機密性，仍以「第一級（輕微）資通安全事件」辦理通報。嗣經法務部調查局(下稱調查局)提示兩案具有關聯性，且該部電子公文交換系統有異常登入紀錄，外交部重行清查後，始查得113年間即有駭客入侵跡象，並據以採取防護應變及改善作為。顯見外交部對於資通安全防護及公務機密維護作業洵有疏漏，亟應檢討改進，以杜此類情事再次發生：

---

[1] 行政院115年4月30日院臺外字第1151011279號函參照。

[2] 外交部115年2月12日外政字第1154300073號函參照（密件，本件至125年2月2日解密）及同年4月7日外政字第1150012092號函參照。

[3] 國安局115年3月26日定靜字第1150002252號函參照（密件，本件至125年3月26日解密）。

(一)113年至114年間，外交部及相關機關之公文書屢遭暗網非法揭露及兜售：

1、113年4月17日，暗網論壇「BreachForums」有帳號「Tonya」之不明人士，宣稱持有外交部外流達4GB容量之PDF格式文件，並要求以虛擬貨幣（泰達幣）交易（如圖1），同時公開包含我與邦交國關係評估、駐美代表處電報等計7份公文內容以資佐證。

2、同月19日，復有帳號「tonyb」之不明人士，於同一暗網討論串貼文（如圖2），誣指時任副總統當選人蕭美琴透過外交部走私酒類（英文原文“TAIWAN VICE PRESIDENT HSIAO BI KHIM SMUGGLING ALCOHOL THROUGH THE MOFA”），且張貼2份公文佐證，並宣稱兜售更多文件。

3、114年8月8日，暗網論壇「DarkForums」有帳號「MEM2FOX」，宣稱持有大量外交部公務文件，要求以5萬美金交易（如圖3），並公開5份公文佐證，公文涉及外交部電子公文及財團法人致外交部部長之機密信函等。

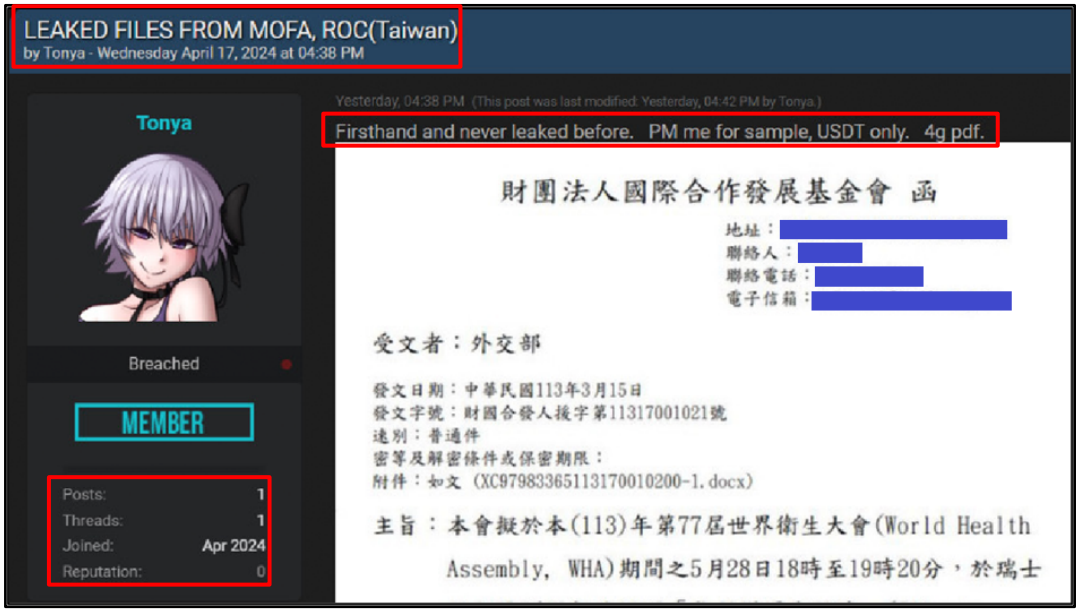


圖1　113年暗網論壇販售宣稱為外交部外流文件之截圖

資料來源：圖片擷取自網路[4]。

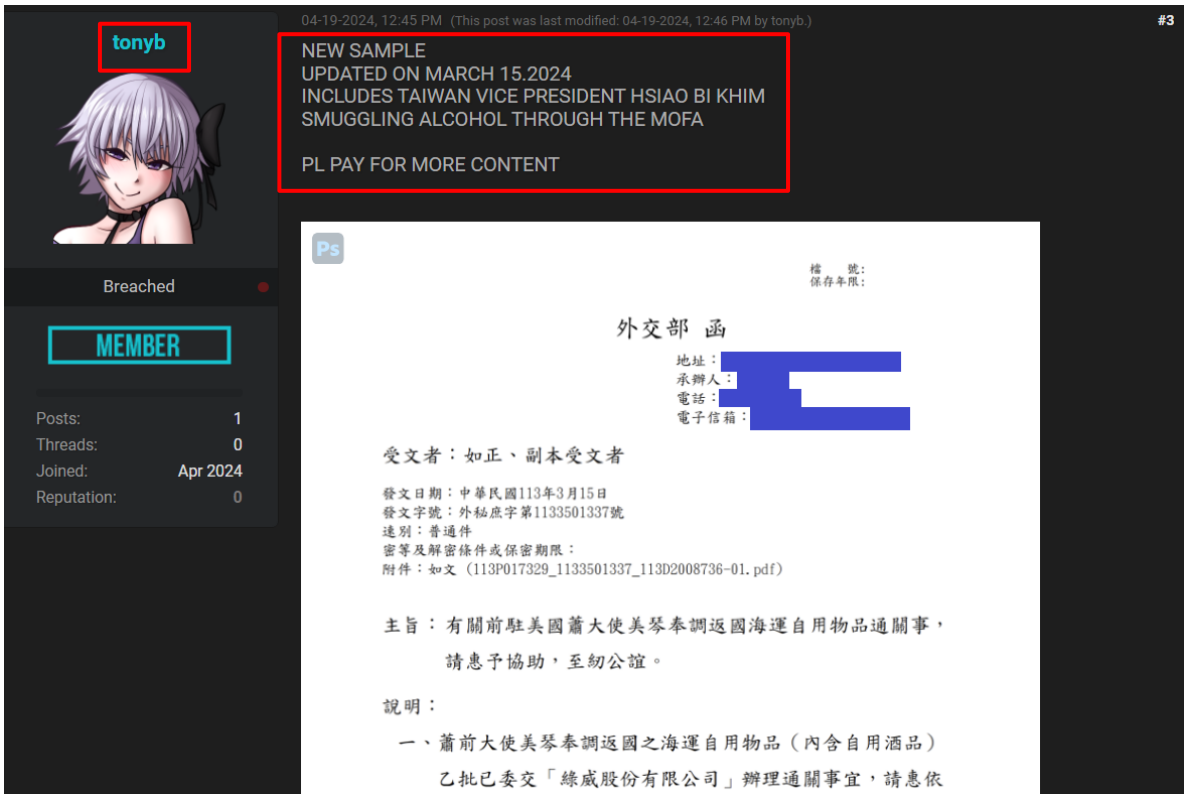


圖2　同暗網討論串帳號「tonyb」貼文截圖

資料來源：圖片擷取自網路[5]。

[4] 第三方網頁快照網站(Archive.ph)暗網討論串備份，標題：「LEAKED FILES FROM MOFA, ROC(Taiwan)」，https://archive.ph/gQc3l，瀏覽日期：115年5月8日。
[5] 第三方網頁快照網站(Archive.ph)，https://archive.ph/gQc3l，瀏覽日期:115年5月8日。

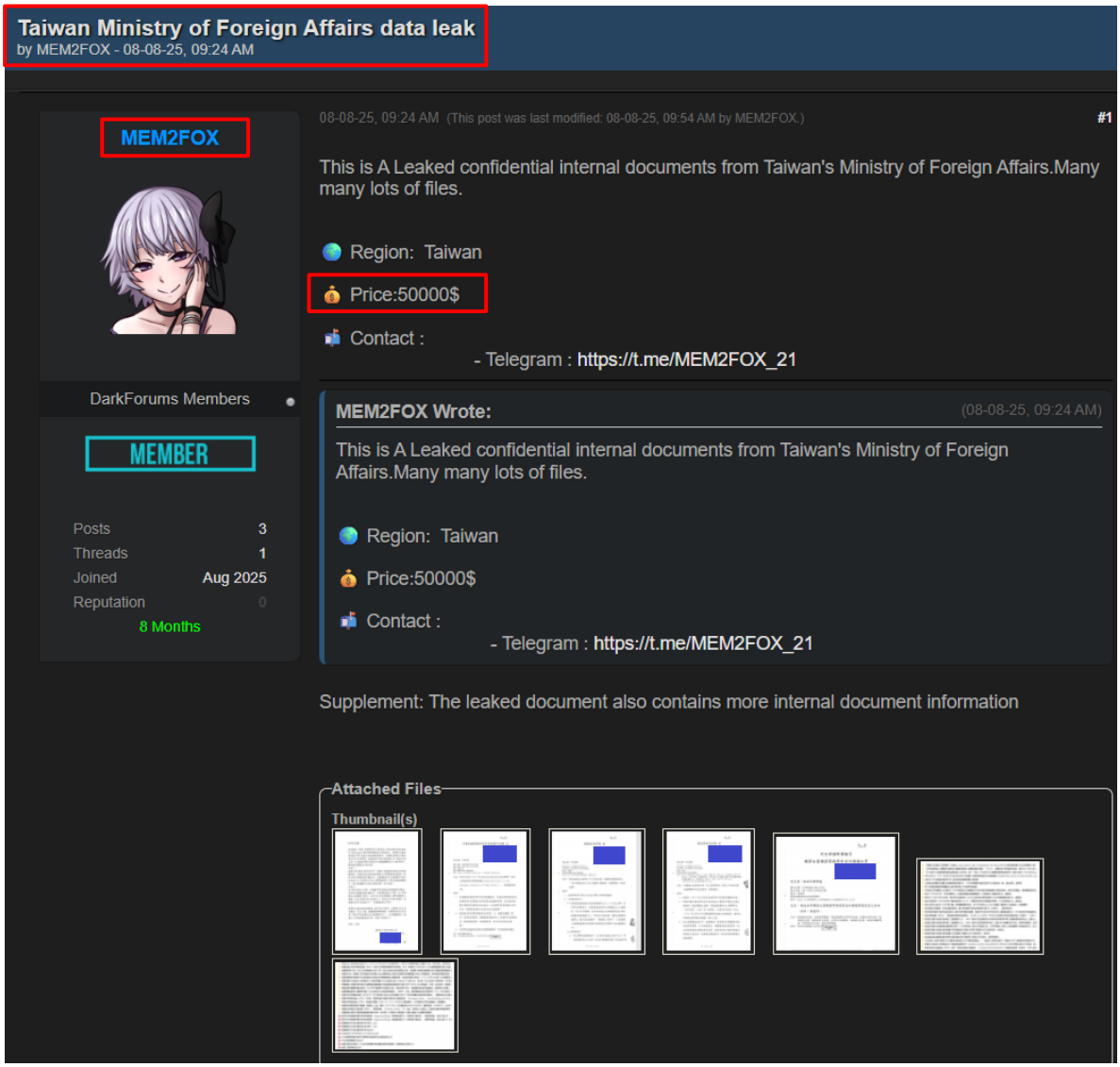


圖3　114年暗網論壇再次出現兜售外交部公文情事

資料來源：圖片擷取自網路[6]。

（二）（略）

（三）有關公文洩漏之常見原因分析如下（如圖4示意）：

1、**外部駭客威脅**：係因機關**資通安全防護未盡周延**，致遭外部駭客入侵攻擊。

2、**員工無意疏失**：係因機關人員資安意識薄弱，或曾將公文複製電子檔案存放於**私人資訊設備或**

[6] 第三方網頁快照網站(Archive.ph)，https://archive.ph/V1NTH，瀏覽日期：115年5月8日。

雲端空間，受駭侵造成公文外流。

3、**人員違法外洩**：係因**機關保密管控機制失靈**，致內部人員蓄意違法外洩公文資訊。

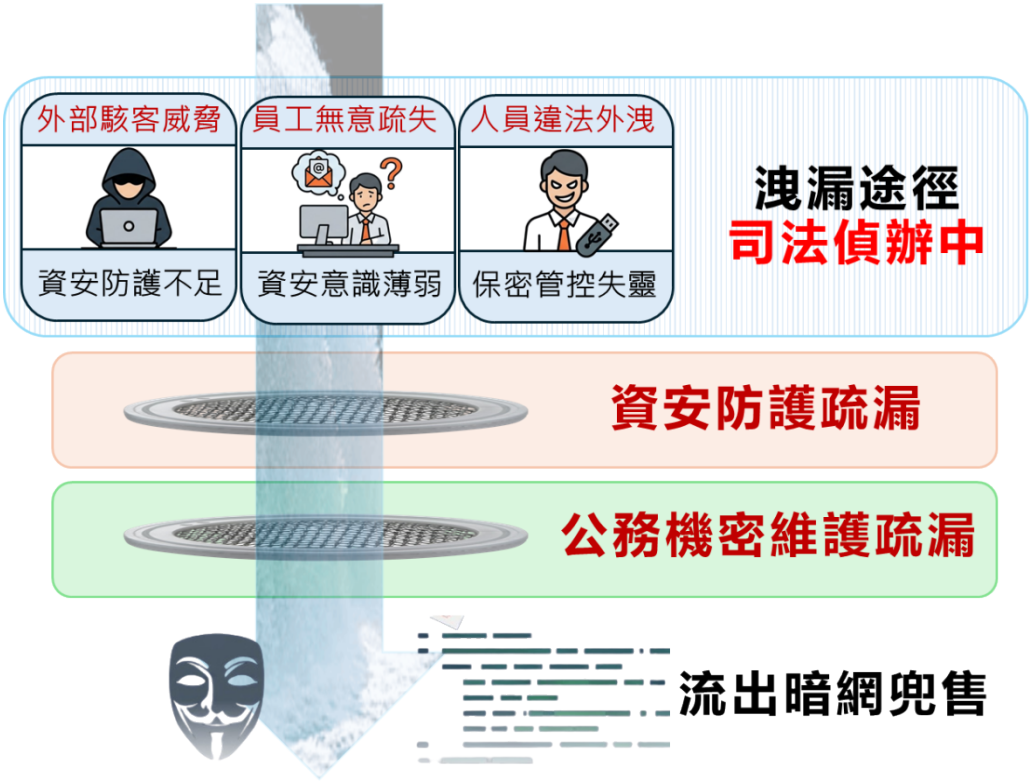


圖4　公文洩漏之常見原因分析

資料來源：本院整理。

（四）（略）

(五)(略)

(六)(略)

(七)(略)

(八)綜上，外交部屬資通安全責任等級A級機關，查其資通安全防護及公務機密維護作業核有疏漏，亟應檢討改進：

1、基礎設備資通安全防護未盡周延：

(1)按外交部業務涉及國家外交機密，依「資通安全責任等級分級辦法」核為資通安全責任等級A級機關，應具備最高等級之防護與應變能力。

(2)(略)

2、公文洩漏損及國家利益與國際威信：

外交部資通安全防護及公務機密維護作業核有疏漏，致公務文件遭非法外流至暗網。該部亟應針對基礎資安防護漏洞澈底檢討，落實各項改善作為並強化資安韌性，以杜絕類案再次發生。

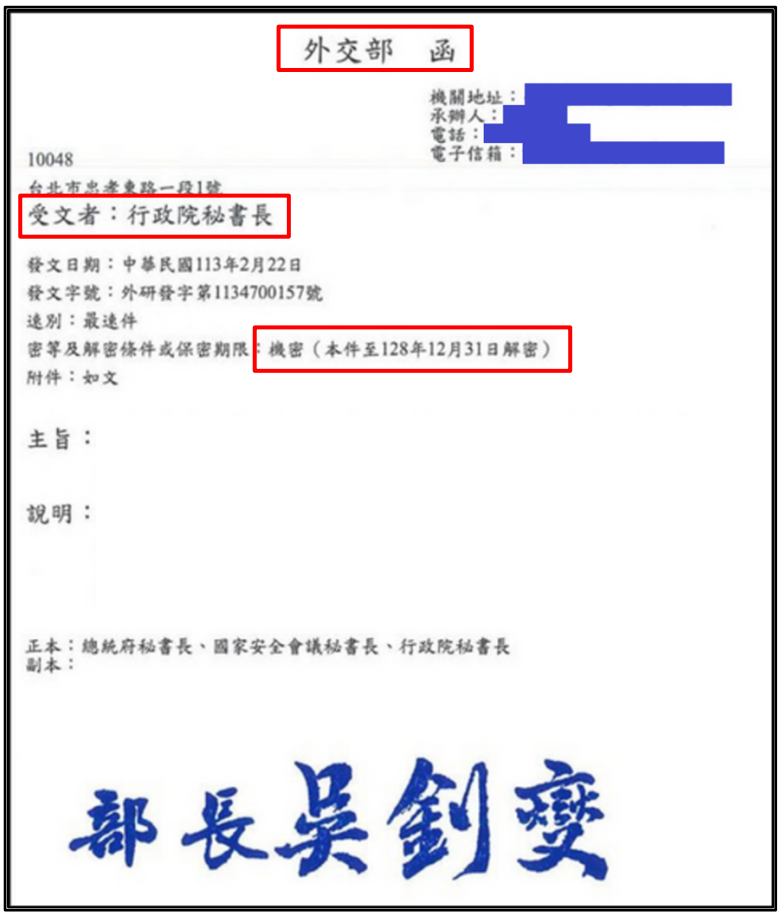
二、113年間外流之「我與邦交國雙邊關係燈號評估」文書，係外交部陳報行政院秘書長之機密文件，業依「國家機密保護法」核定為「機密」等級，按規定應採紙本簽辦及密封傳遞，並禁止非經授權之複製。詎行政院承辦人員於內部作業過程中，違規掃描複製，肇生洩漏風險，顯見該院當時機密文書處理及內部安全維護作業未臻周妥，應予檢討改進。另查114年間外流之「臺灣民主基金會執行長致外交部部長信函」，審其內容涉及政府委託公務事項,具備準公文書性質，且頁面經標註機密，採全程紙本傳遞，理應納入公務機密維護範疇。鑑於該基金會係由外交部督導之政府捐助財團法人，外交部本於監督職權，亟應落實該案

行政調查並檢討機密文書溯源識別管理機制，以杜絕機密外洩漏洞：

(一)113年機密文書外洩經過與機關應處：

1、文件內容與性質：

經查，113年外流機密文書為外交部陳報行政院秘書長（圖5~圖6）及行政院外交國防法務處內部簽陳（圖7）之機密文件，涉及「我與邦交國雙邊關係燈號評估」，該等文書業依「國家機密保護法」核定為「機密」等級。



外交部　函

機關地址：[redacted]
承辦人：[redacted]
電話：[redacted]
電子信箱：[redacted]

10048
台北市忠孝東路一段1號

受文者：行政院秘書長

發文日期：中華民國113年2月22日
發文字號：外研發字第1134700157號
速別：最速件
密等及解密條件或保密期限：機密（本件至128年12月31日解密）
附件：如文

主旨：

說明：

正本：總統府秘書長、國家安全會議秘書長、行政院秘書長
副本：

部長吳釗燮

圖5　暗網論壇流出之公務文件樣張（涉及邦交國關係評估）

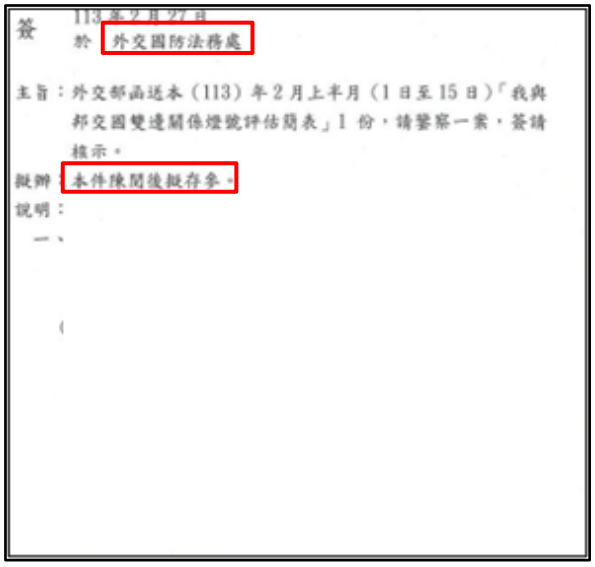
資料來源：圖片擷取自網路[7]。

[7] 第三方網頁快照網站(Archive.ph)，https://archive.ph/gQc3l，瀏覽日期：115年5月8日。

（略）

圖6　暗網論壇流出之「我與邦交國雙邊關係燈號評估簡表」截圖

資料來源：圖片擷取自網路[8]。


簽　113年2月27日
於　外交國防法務處

主旨：外交部函送本（113）年2月上半月（1日至15日）「我與邦交國雙邊關係燈號評估簡表」1份，請鑒察一案，簽請核示。

擬辦：本件陳閱後擬存參。

說明：
一、

圖7　行政院外交國防法務處簽辦公文樣張

資料來源：圖片擷取自網路[9]。

2、標準作業程序：

按「國家機密保護法」相關規定，此類機密文件應採取紙本簽辦、密封傳遞，且應禁止未經授權之複製。

3、違規行為：（略）

4、機密文件洩漏確切原因：

目前檢調偵辦中，機密文件洩漏確切原因尚待釐清。

(二)114年外交部書信外洩經過與機關應處：

[8] 第三方網頁快照網站(Archive.ph)，https://archive.ph/gQc3l，瀏覽日期：115年5月8日。

[9] 第三方網頁快照網站(Archive.ph)，https://archive.ph/gQc3l，瀏覽日期：115年5月8日。

1、文件內容與性質：

（1）係財團法人臺灣民主基金會（下稱臺灣民主基金會）執行長致外交部部長書信（圖8），說明為因應美國國家民主基金會（簡稱NED）經費遭凍結之緊急情況，並審酌該基金會114年度預算情形，研擬有關方案，用以支援與NED長期合作之關鍵國際民主人權非政府組織（NGOs），陳請外交部部長核示之書信。

（2）該文書卷面標列為「機密」，屬逕自列等之書信，外交部並無收文紀錄；惟查，**該文書內容似涉及受託辦理之公務，應認具備「準公文書」性質**。

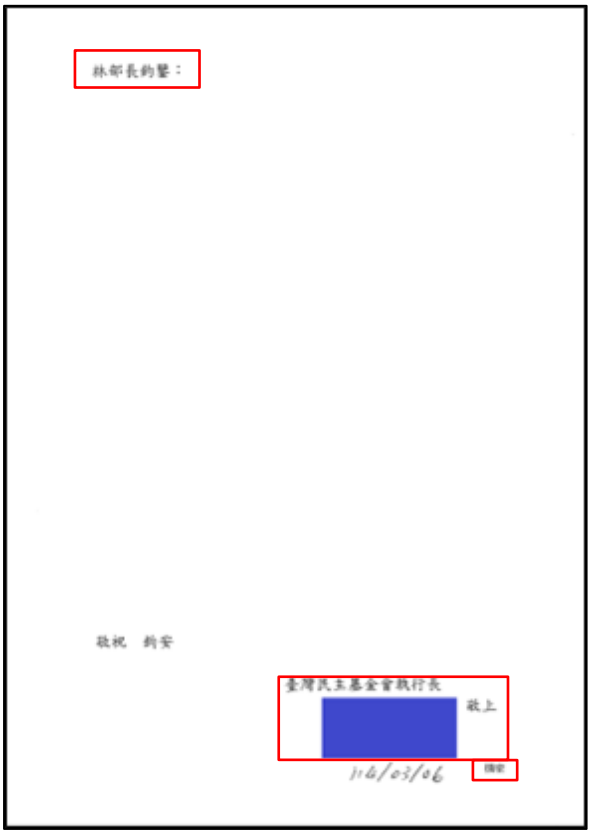


圖8　臺灣民主基金會執行長致外交部部長書信。

資料來源：圖片擷取自網路[10]。

[10] 第三方網頁快照網站(Archive.ph)，https://archive.ph/Lvjo9，瀏覽日期：115年5月8

2、文件洩漏原因：（略）

3、監督責任：

臺灣民主基金會係屬受外交部督導之政府捐助財團法人[11]。

（三）（略）

（四）（略）

（五）（略）

（六）綜上，行政院及外交部於公務機密維護上均有疏漏：

行政院部分，人員法遵及資安風險意識薄弱，逕自掃描複製機密文書成電子檔，致生外洩風險；外交部部分，對於所督導法人產製之準公務機敏資訊流出，未盡溯源釐清及監督管理之責。上開機關應就機密文書於紙本作業與數位轉換間之疏漏，強化人員法紀教育及資訊設備資安管控，以杜絕政府機密文書非法外洩之情事。

三、113年間暗網揭露之4件公文書，屬我國駐美代表處發送之外交電報或密件公文。外交部於清查後，僅以非屬該部部內外流為由，未通知相關外館查處或加強防護措施，核有未當。按我國各駐外館處之資通安全稽核及公務機密維護，均屬外交部（資電處與政風處）之職掌範圍。有關公文外洩事件，該部應即時通報相關館處，針對作業環境進行全面清查並強化安全查核，非謂「排除本部洩密」即可逕予諉責。另查，案涉2件密件公文屬駐美代表處經濟組發送，經濟部依權責負有督導之責，自應積極釐清公文於駐外環境製作及傳遞過程之系統性疏漏。是以，外交部與經濟部對於

日。

[11] 「財團法人臺灣民主基金會捐助暨組織章程」第3條：本會之主管機關為外交部。

所督導駐外館處之公文傳輸資安及公務機密防護工作疏於落實，亟應檢討改善：

(一)113年案件暗網流出公文書，計4件屬我國駐外館處發送：

1、駐美代表處電發外交部之**外交電報**（專號：USA1526，如圖9），涉及「美聯邦眾院歲計委員會通過『美臺21世紀貿易倡議首批協定執行法案』」。


駐 美 國 代 表 處 電 報

專號：USA1526　第1 頁

日期：112.06.13

本電：電文2頁，附件13頁，共15頁

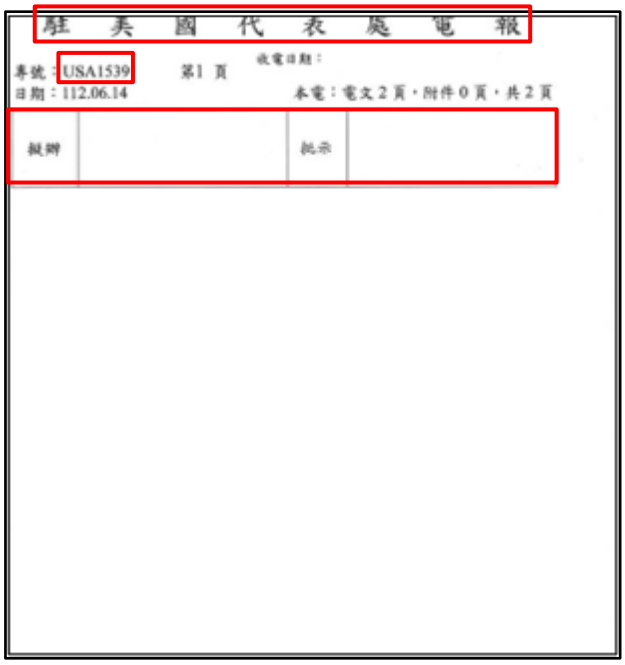
擬辦　　批示

圖9　駐美代表處電報樣張（電報專號：USA1526）

資料來源：圖片擷取自網路[12]。

2、駐美代表處電發外交部之**外交電報**（專號：USA1539，如圖10），內容同樣涉及「美聯邦眾院歲計委員會通過『美臺21世紀貿易倡議首批協定執行法案』」有關情資。

[12] 第三方網頁快照網站(Archive.ph)，https://archive.ph/gQc31，瀏覽日期：115年5月8日。


駐 美 國 代 表 處 電 報

專號：USA1539　第1 頁　收電日期：

日期：112.06.14　本電：電文2頁，附件0頁，共2頁

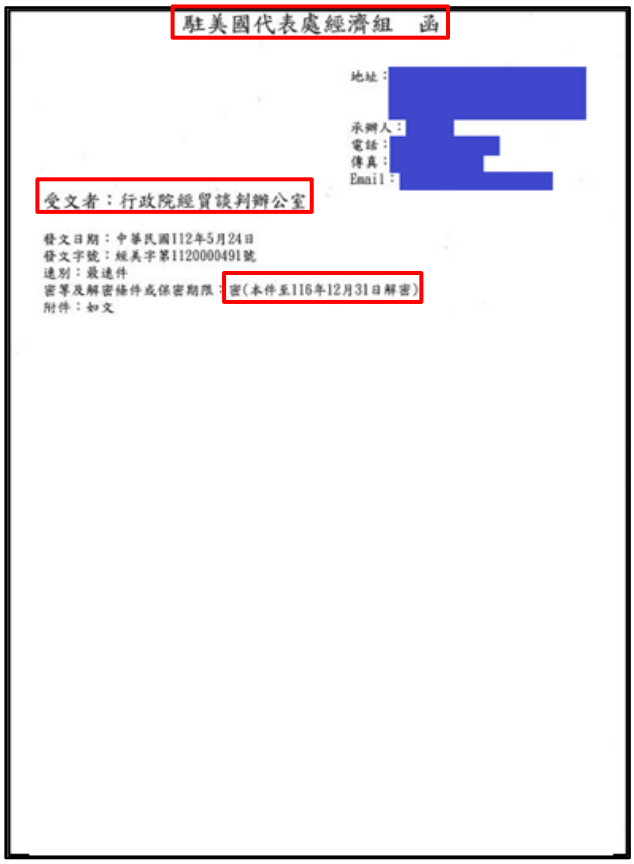
擬辦　批示

圖10　駐美代表處電報樣張（電報專號：USA1539）

資料來源：圖片擷取自網路[13]。

3、駐美代表處經濟組函送行政院經貿談判辦公室之**密件公文**（文號：經美字第11200090491號，如圖11），內容有關「我政府人員出席臺美21世紀貿易倡議簽署儀式之下榻旅館事」。

[13] 第三方網頁快照網站(Archive.ph)，https://archive.ph/gQc3l，瀏覽日期：115年5月8日。


駐美國代表處經濟組　函

地址：[redacted]

承辦人：
電話：
傳真：
Email：[redacted]

受文者：行政院經貿談判辦公室

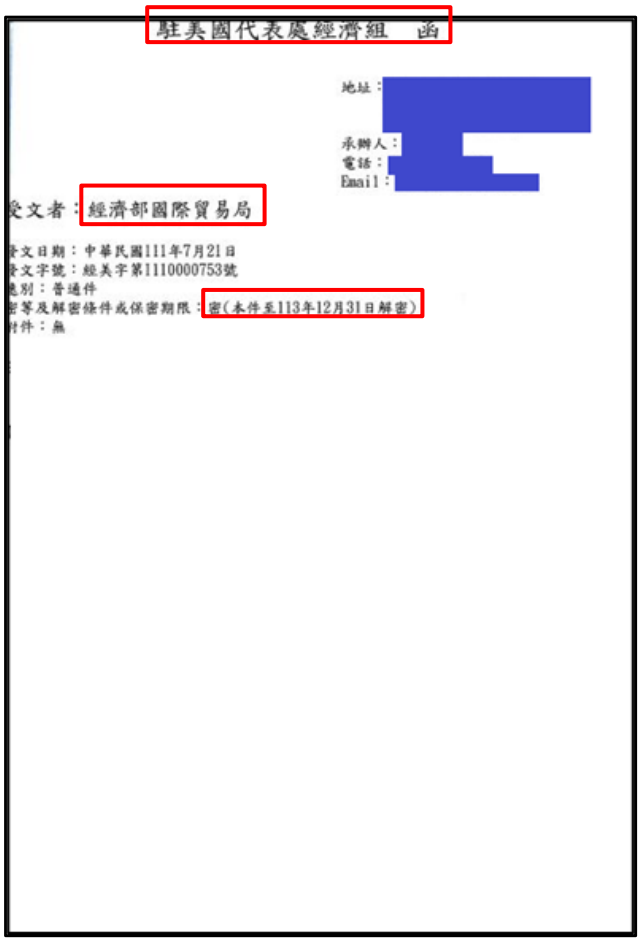
發文日期：中華民國112年5月24日
發文字號：經美字第1120000491號
速別：最速件
密等及解密條件或保密期限：密(本件至116年12月31日解密)
附件：如文

圖11　駐美代表處經濟組函送行政院經貿談判辦公室公文

資料來源：圖片擷取自網路[14]。

4、駐美代表處經濟組函送經濟部國際貿易局(自112年9月26日改制為經濟部國際貿易署，下稱國貿署)之**密件公文**(文號:經美字第1110000753號，如圖12)，內容有關「我方人員與美方重要智庫之晤談重點及情資蒐報」。

[14] 第三方網頁快照網站(Archive.ph)，https://archive.ph/gQc31，瀏覽日期：115年5月8日。


駐美國代表處經濟組　函

地址：[redacted]

承辦人：[redacted]
電話：[redacted]
Email：[redacted]

受文者：經濟部國際貿易局

發文日期：中華民國111年7月21日
發文字號：經美字第1110000753號
速別：普通件
密等及解密條件或保密期限：密(本件至113年12月31日解密)
附件：無

圖12　駐美代表處經濟組函送國貿署公文

資料來源：圖片擷取自網路[15]。

（二）（略）

（三）（略）

（四）次查，外交部負有駐外館處資通安全及公務機密維護之督導職掌，不應非該部部內流出即卸除監督責任：

1、依「外交部處務規程」第21條規定，駐外機構資通安全之規劃、推動及督導，以及該部與駐外機構間往來電報之處理、控管及稽核，均屬資電處之職掌。

[15] 第三方網頁快照網站(Archive.ph)，https://archive.ph/gQc31，瀏覽日期：115年5月8日。

2、駐外館處之機密維護行政監督則為該部政風處權責。

3、本案外洩之4件文書繕發源頭均指向駐美代表處及駐美代表處經濟組，外交部理應即時啟動對駐外環境之全面安全查核，而非於行政調查結論中率爾卸責，導致防護缺口未能及時堵漏。

(五)復查，本案駐美代表處經濟組經美字第1110000753號公文，係由該組發送國貿署，且透過該署電子公文交換系統傳遞，經濟部應詳細調查公文洩漏原因：

1、調查發現，2件駐外單位經濟組密件公文，係透過SMTP協定將公文檔案傳送至國貿署之伺服器，再由該署代辦公文後續。

2、經濟部負有業務指導之責，對於此洩漏文書繕打、存管及電子傳送流程，應落實資安稽核與機密防護督導。

(六)綜上，外交部及經濟部對駐外館處機密維護之督導顯有未周：

外交部於案發初期，未落實對駐外作業環境之行政調查；經濟部對於權管駐外館處經濟組，公文傳輸管道之資安控管未盡督導及落實清查之責。該2部機關亟應就本事件檢討，針對駐外館處之資安防護與公務機密維護，研議強化作為；並衡酌本案缺失，列入重點稽核項目予以管控，以維護國家外交利益與機敏資訊安全。

四、鑑於駭客攻擊手法日趨縝密，本案為例，即具敵對勢力組織化運作特徵，而為維護國家安全，亟應強化機關「資安聯防」及「公務機密維護」之應處。以本案暗網所揭露13件外流公文，經調查分析態樣，顯係由不同疏漏所致。復查，本案凸顯機關之資安鑑識力有

未逮，肇致資安聯防無法啟動，將肇生孤立應處之虞，不利建構有效之整體防禦縱深。爰此，資安署及廉政署作為資通安全與公務機密維護之權責機關，應針對本案深究其因，精進資安鑑識及落實情資共享機制，以維國家利益及公務機密安全：

(一)公文書之本質與重要性：

「公文」係處理政府公務或與公務有關之資料，凡機關與機關、機關與人民往來，或機關內部通行之文書均屬之。**公文如同人體神經系統，為政府溝通之重要工具；雖因應時代發展，部分轉為電子傳輸，然其具備政府公權力**之本質並未改變。

(二)本案遭洩漏文書類型多樣，且具有中國敵對勢力組織化運作特徵，文書型態如下：

1、國家機密公文：包含依「國家機密保護法」核定辦理之外交機密文書。

2、密件公文：包含駐美代表處經濟組發送之密件公文。

3、外交電報：包含駐美代表處電發之外交電報。

4、電子公文：部分非密件普通公文，係經由「電子公文交換系統」繕發傳遞，屬數位通訊傳輸之電子公文。

5、準公文書：臺灣民主基金會致外交部之機密信函，內容涉及委託公務。

6、特定事件公文：遭惡意扭曲內容並配合認知作戰之特定案件相關公文（如外交人員酒類物品通關案）。

(三)美國司法部於114年3月發布新聞稿[16]，揭露起訴涉

[16]新聞稿以及起訴書詳參美國司法部網站，網址：https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global，瀏覽日期：115年6月1日。

嫌駭客行動的12名中國人士，起訴書指出涉案之安洵公司為「中華人民共和國所僱用駭客生態系統的關鍵參與者」，攻擊目標包括我國外交部。鑒於中國駭客組織將外交部等核心機關當作攻擊目標，顯見該等威脅已具備高度組織性與針對性。

(四)本案有關疏漏與違失：

1、內部作業違失：(略)

2、資訊鑑識能力不足與研判失當：(略)

3、資安監控機制存有缺漏：(略)

4、資安事件通報等級未反映實態：(略)

5、督導管理與機密文書溯源識別機制失靈：外交部對其督導之臺灣民主基金會所繕發之具準公文書性質之機密信函，缺乏有效之溯源識別管理及監督機制；且外交部案發後僅以公文非部內流出為由，未對監督法人及駐外館處作業環境進行全面清查與安全查核，應處未能及時補漏。

(五)經查，資安鑑識能力係啟動資安聯防之關鍵，惟資安署強調須俟「事件明確」始能啟動聯防，致**本案於駭侵事實時，未能即時採取聯防應變措施。且於知悉駭侵事實後，亦未將本案暴露之系統弱點納入後續重點稽核範疇**，亟待研析改進：

1、**資安鑑識能力不足影響聯防啟動時機**：(略)

2、**鑑識專業落差造成防護缺口**：(略)

3、**知悉事實後未依規續行通報**：(略)

4、**稽核制度規劃與執行顯有欠妥**：資安署雖稱不會針對特定事件進行稽核[17]，惟依「資通安全管理法」第8條規定，主管機關得定期或不定期稽核

[17] 行政院115年4月30日院臺外字第1151011279號函說明第7頁參照：「三、數位發展部114年資通安全稽核計畫已涵蓋外交部並完成實地稽核作業，稽核內容主要係檢視機關策略面、管理面及技術面等各項法遵事項整體落實情形，**並非針對特定資安事件**」。

公務機關及特定非公務機關之資通安全維護計畫實施情形。關於資安稽核之實施，旨在預警系統運作漏洞並補強，資安署未能針對此次案件暴露之系統弱點納入稽核重點，所稱理由難謂允洽。

(六)復查，本案涉及外洩之公文書，其收發文單位涵蓋國家安全會議、行政院（含經貿談判辦公室）、外交部、經濟部（含國貿署）、財政部國庫署、財政部關務署基隆關、各駐外館處及臺灣民主基金會等。究上揭機關（構）是否知悉公文外洩情事並落實內部行政清查，抑或因未能掌握洩密管道，致皆未依「政風機構維護公務機密作業要點」第17點規定，通報該管政風機構處理，導致相關機關均未能啟動內部清查，此有待廉政署協調釐清。

(七)綜上，本案凸顯國家資安聯防與公務機密維護，因應敵對勢力組織化威脅時仍有未逮。權責機關應汲取本案缺失經驗，分別從技術面（精進鑑識能量、完備機密文書溯源識別機制）及管理面（檢討資安監控範疇、落實情資共享）採行應處措施；資安署與廉政署應就本案暴露之系統性缺漏覈實檢討。

調查委員：**林文程**

賴鼎銘

葉宜津