朝鮮網路威脅通告

發佈時間：　2020 年 4 月 15 日

標題：　朝鮮網路威脅指南

美國國務院，財政部和國土安全部以及聯邦調查局發佈此通報，作為針對國際社會，網路維護者和公眾的朝鮮網路威脅的綜合資源。本通報重點介紹北韓（正式稱為朝鮮民主主義人民共和國，簡稱朝鮮）所構成的網路威脅，並提出了減輕威脅的建議措施。特別是，附件一列出了與朝鮮網路威脅有關的美國政府資源，附件二包含了指向聯合國1718制裁委員會（朝鮮）專家小組報告的鏈接。

朝鮮的惡意網路活動威脅著美國和更廣泛的國際社會，特別是對國際金融體系的完整性和穩定性構成了重大威脅。在美國和聯合國強大制裁的壓力下，朝鮮越來越依靠非法活動（包括網路犯罪）創造收入，以便實施其大規模殺傷性武器和彈道飛彈計劃。美國特別對朝鮮的惡意網路活動深表關切，美國政府將其稱為『隱身眼鏡蛇（HIDDEN COBRA）』。朝鮮有能力進行影響美國關鍵基礎設施的擾亂性或破壞性網路活動。朝鮮還利用網路能力從金融機構竊取資金，並顯示出擾亂性和有害網路活動的模式，這與國際上日益增強的對網路空間中負責任的國家行為的共識背道而馳。

美國與志同道合的國家密切合作，以關注並譴責朝鮮在網路空間中的擾亂性、破壞性或其他破壞穩定的行為。例如，在2017年12月，澳洲，加拿大，紐西蘭，美國和英國將WannaCry 2.0勒索軟體攻擊歸因於朝鮮，並譴責朝鮮的有害和不負責任的網路活動。丹麥和日本發表了支持性聲明，共同譴責破壞性的WannaCry 2.0勒索軟體攻擊，該攻擊於2017年5月影響了全球數十萬台電腦。

國際社會、網路維護者和公眾保持警惕，共同努力，這對于減輕北韓構成的網路威脅至關重要。

朝鮮針對金融部門的惡意網路活動

朝鮮的許多在網路上行動者都隸屬於聯合國和美國指認的實體，例如偵察總局。朝鮮政府主使的網路行動者主要包括駭客、密碼學家和軟體開發人員，他們進行間諜活動、針對金

融機構和數字貨幣交易所的網路盜竊，以及針對外國媒體公司的出於政治動機的行動。他們開發了各種惡意軟體工具在全球範圍內部署以支持這些活動，並且越來越嫻熟老練。朝鮮政府主使的網路行動者非法獲取收入的常見策略包括但不限於：

網路金融盜竊和洗錢 聯合國安理會1718委員會專家小組的2019年中期報告（2019 專家小組中期報告）指出，儘管受到聯合國安理會制裁，朝鮮仍然愈發有能力通過惡意網路活動使用越來越複雜的工具和策略手段從金融機構竊取資金來創收。2019專家小組中期報告指出，在某些情況下，這些惡意網路活動也已擴展到通過多個司法管轄區洗錢。 2019專家小組中期報告提到，該機構正在調查數十起涉嫌由朝鮮進行網路攻擊的搶劫案，截至2019年底，朝鮮試圖通過這些非法網路活動竊取多達20億美元。美國司法部在2020年3月提出的一項沒收訴訟與專家小組的調查結果中的部分內容一致。具體來說，沒收訴訟指控北韓網路行動者如何利用北韓基礎設施，以助其陰謀駭入數字貨幣交易所，竊取數億美元的數字貨幣並洗錢。

大規模勒索行動 朝鮮網路行動者還對第三國實體進行大規模勒索行動，其手段是侵入某個實體的網路，脅迫實體支付贖金，否則就將其網路關閉。在某些情況下，朝鮮網路行動者以長期有償諮詢服務的名義要求受害者付款，以確保今後不會發生此類惡意網路活動。朝鮮網路行動者也收費為第三方客戶攻擊其目標網站和敲詐。

加密劫持 2019年專家小組中期報告指出，專家小組還在調查朝鮮使用的『加密劫持』的陰謀方案，該陰謀方案旨在入侵受害機器並竊取其計算資源來開採數字貨幣。專家小組發現了幾起事件，其中感染了加密劫持惡意軟體的電腦將挖出的資產（其中大部分是匿名性增強的數字貨幣，有時也稱為『隱私硬幣』）發送到位於朝鮮的服務器，包括平壤的金日成大學。

這些活動凸顯了朝鮮使用網路手段創造收入，同時減輕制裁的影響，並且顯示任何國家都可能暴露在朝鮮的攻擊之下，為其利用。根據2019年專家小組中期報告，專家小組還在調查這種企圖違反聯合國安理會對朝鮮制裁的活動。

美國政府公開歸罪於朝鮮的網路攻擊行動

朝鮮一再針對美國及其他政府和軍事網路，以及與私人實體和關鍵基礎設施有關的網路，以竊取數據並進行擾亂性和破壞性的網路活動。迄今為止，美國政府已將以下網路事件公開歸因於朝鮮政府主使的網路行動者和同謀：

- ***索尼影業*** 2014年11月，朝鮮政府主使的網路行動者涉嫌對索尼影視娛樂（Sony Pictures Entertainment—SPE）發起網路攻擊，以報復2014年的電影《訪談》。朝鮮網路行動者侵入索尼影視娛樂網路以竊取機密數據，威脅索尼影視娛樂高管和員工，並損壞了數千台電腦。
    - 美國聯邦調查局關於索尼調查的最新報告（2014年12月19日）https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

- 美國司法部對朝鮮政權支持的程序員的刑事訴訟（2018年9月6日）https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***孟加拉國銀行搶劫案*** 2016年2月，朝鮮政府主使的網路行動者試圖通過環球銀行金融電信協會（SWIFT）網路上的未經授權交易從全球金融機構竊取至少10億美元，並據稱從孟加拉國銀行偷走了8100萬美元。根據投訴，朝鮮網路行動者在通過針對銀行員工的魚叉式網路釣魚電子郵件破壞了該銀行的電腦網路之後，進入孟加拉銀行與SWIFT網路連接的電腦終端。朝鮮網路行動者隨後發送偽造的SWIFT認證資訊，指示紐約聯邦儲備銀行將資金從孟加拉國銀行的聯邦儲備帳戶轉到陰謀者控制的帳戶。

  - 美國司法部對朝鮮政權支持的程序員的刑事訴訟（2018年9月6日）https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***WannaCry 2.0*** 朝鮮政府主使的網路行動者開發了被稱為WannaCry 2.0的勒索軟體，以及這種勒索軟體的前兩個版本。2017年5月，WannaCry 2.0勒索軟體感染了150多個國家/地區的醫院、學校、企業和家庭中的數十萬台電腦。 WannaCry 2.0勒索軟體對受感染電腦的數據進行加密，並允許網路行動者要求以比特幣數字貨幣支付贖金。美國財政部指認一名朝鮮電腦程序員參與了WannaCry 2.0的陰謀活動，並參與了對索尼影業的網路攻擊和對孟加拉銀行的搶劫案，此外，還指認了他工作的機構。

  - 網路和基礎設施安全局（CISA）的技術警報：與WannaCry勒索軟體相關的指標（2017年5月12日）https://www.us-cert.gov/ncas/alerts/TA17-132A
  - 白宮新聞發布會介紹WannaCry勒索軟體的來源歸屬（2017年12月19日）https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
  - 美國司法部對朝鮮政權支持的程序員的刑事訴訟（2018年9月6日）https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
  - 美國財政部認定朝鮮發動了多次網路襲擊（2018 年 9 月 6 日）https://home.treasury.gov/news/press-releases/sm473

- ***快錢行動（FASTCash）*** 自2016年底以來，朝鮮政府主使的網路行動者採用了一種稱為『快錢』的自動櫃員機（ATM）現金提取欺詐陰謀，從亞洲和非洲的自動櫃員機（ATM）竊取數千萬美元。快錢陰謀遠程破壞銀行中的支付開關應用服務器，以協助欺詐性提款。在2017年的一起事件中，朝鮮網路行動者允許同時從30多個國家/地區的自動櫃員機（ATM）提取現金。在2018年的另一起事件中，朝鮮網路行動者允許同時從23個不同國家的自動櫃員機（ATM）中提取現金。自2016年底以來，朝鮮政府主使的網路行動者採用了一種稱為『 快錢』的欺詐性自動櫃員機（ATM）現金提取計劃，從亞洲和非洲的自動櫃員機

（ATM）竊取數千萬美元。 快錢陰謀可遠程破壞銀行中的支付開關應用服務器，以促進欺詐性交易。在2017年的一起事件中，朝鮮網路行動者能夠同時從30多個國家的自動櫃員機（ATM）提取現金。在2018年的另一起事件中，朝鮮網路行動者讓人能夠同時從23個不同國家的自動櫃員機（ATM）中提取現金。

  - 網路安全和基礎設施安全局（CISA）關於快錢行動的警告（2018年10月2日）https://www.us-cert.gov/ncas/alerts/TA18-275A
  - 網路安全和基礎設施安全局（CISA）的惡意軟體分析：與快錢有關的惡意軟體的分析報告（2018年10月2日）https://www.us-cert.gov/ncas/analysis-reports/AR18-275A

- ***數字貨幣交易所駭客*** 正如美國司法部在一個沒收物權的訴訟中所陳述的那樣，2018年4月，朝鮮政府主使的網路行動者駭入一個數字貨幣交易所，並偷走了價值近2.5億美元的數字貨幣。訴訟進一步描述了如何通過數百次自動數字貨幣交易對被盜資產進行洗錢，以掩蓋資金的來源，防止執法機構追踪資產。據稱，有兩名中國公民隨後代表朝鮮集團給這些資產洗錢，從朝鮮控制的賬戶中收到了約9100萬美元，並從另一家交易所的駭客入侵中獲得了950萬美元。 2020年3月，美國財政部指認這兩個人受到網路制裁和對朝鮮的制裁，同時司法部宣布兩人先前已被起訴洗錢和無執照的轉賬，113個有關的數字貨幣帳戶將面臨沒收。

  - 美國財政部針對為拉撒路集團（Lazarus Group）的加密貨幣洗錢的個人制裁（2020年3月2日）https://home.treasury.gov/news/press-releases/sm924
  - 美國司法部對兩名中國國民給來自交易所駭客的加密貨幣洗錢的指控，以及民事沒收訴訟（2020年3月2日）https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

應對朝鮮網路威脅的措施

北韓針對全球使用網路的基礎設施，為其政權的優先事項（包括大規模毀滅性武器計劃）創收。我們強烈敦促各國政府、產業、民間團體和個人採取以下所有相關措施，以保護自己，抵禦朝鮮的網路威脅：

- **提高對朝鮮網路威脅的認識**。著重指出朝鮮進行的惡意網路活動的嚴重性、範圍和種類，將提高公共和私營部門對該威脅的普遍認識，並促進採用和實施適當的預防和減輕風險措施。

- **分享關於朝鮮網路威脅的技術資訊。**同時在國內和國際共享資訊，發現和防禦朝鮮的網路威脅將增強網路和系統的安全性。應與各國政府和私營部門共享行爲規範。根據 2015 年《網路安全資訊共享法》（美國法典 6 U.S.C. §§ 1501–1510）的規定，非聯邦實體可以與聯邦和非聯邦實體共享與隱身眼鏡蛇（HIDDEN COBRA）相關的網路威脅指標和防禦措施。

- **實施和推廣網路安全行爲規範。**採取措施（包括技術措施和行為措施）以增強網路安全性，將使美國和全球網路基礎設施更安全，更具生命力。金融機構，包括貨幣服務公司，應採取獨立的步驟來防禦惡意的朝鮮網路活動。這些步驟可能包括但不限於通過政府和/或行業管道共享威脅資訊；分割網路以最大程度地降低風險；定期保存數據的備份副本；進行有關通常社會工程策略的意識培訓；實施對資訊共享和網路進入進行管理的政策；以及製定網路事件應對計劃。美國能源部的網路安全能力成熟度模型和美國國家標準技術研究院的網路安全框架為開發和實施可靠的網路安全實踐提供了指導。如附件一所示，網路安全和基礎設施安全局（CISA）提供了廣泛的資源，包括技術警報和惡意軟體分析報告，以使網路防御者能夠識別並減少遭受惡意網路活動的威脅。

- **通知執法機關。**如果某個機構懷疑自己是朝鮮或其他國家發動的惡意網路活動的受害者，至關重要的是及時通知執法部門。這不僅可以加快調查的速度，而且在發生金融犯罪時，還可以增加追回任何被盜資產的機會。

  美國執法部門截獲了北韓網路行動者盜竊的價值數百萬美元的數字貨幣。鼓勵包括金融服務公司在內的所有類型的金融機構通過回復美國執法部門對有關這些網路威脅的資訊的請求在前端進行合作，而在後端則通過在收到美國執法部門的請求或美國法院的命令後，識別可沒收資產來進行合作，并且通過與美國執法部門合作以支持沒收此類資產。

- **加強反洗錢 （AML） / 打擊恐怖主義融資 （CFT)）/ 反武器擴散融資（CPF）。** 各國應迅速有效地執行反洗錢/打擊恐怖融資/反武器擴散融資方面的金融行動特別工作組（FATF）標準。這包括確保金融機構和其他有關實體按照金融行動特別工作組標準以及金融行動特別工作組公開聲明和指南採取降低風險的措施。特別是，金融行動特別工作組呼籲所有國家採取對策，以保護國際金融體系避免朝鮮正在發生的洗錢、恐怖主義融資和武器擴散融資活動的風險[1]。這包括建議所有金融機構和其他有關實體特別注意與朝鮮的業務關係和交易，包括朝鮮公司、金融機構及代表其行事的機構。根據聯合國安全理事會第 2270 號決議執行部分第 33 段，會員國應關閉其領土內朝鮮銀行的現有分支機構、子公司和代表處，並終止與朝鮮銀行的往來關係。

  此外，2019 年 6 月，金融行動特別工作組修改了標準，要求所有國家對包括數字貨幣交易所在內的數字資產服務提供商進行監管和監督，並降低從事數字貨幣交易時的風險。數字資產服務提供商應該對客戶活動的變化保持警覺，因為他們的業務可能被用於促進洗錢、恐怖分子融資和武器擴散融資。美國尤其關注提供匿名支付和帳戶服務功能而又沒有交易監控、可疑活動報告以及客戶盡職調查等義務的平台。

[1] *FATF 關於朝鮮的呼籲全文見如下鏈接：* https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html

美國金融機構，包括在美國全部或大部分地區開展業務的位於國外的數字資產服務提供商、以及其他有關企業和個人，應確保按照《銀行保密法》遵守其監管義務（據聯邦法規 31 CFR 第 10 章由美國財政部金融犯罪執法網路 FinCEN 實施）。對於金融機構，這些義務包括制定和維護有效的反洗錢計劃，這些計劃合理地設計來防止貨幣服務業務被用於促進洗錢和資助恐怖主義活動，以及識別和報告可疑交易，在向 FinCEN 報告的可疑活動中包括通過涉及數字資產的網路事件或非法融資進行的、影響的或促成的交易。

國際合作 為了應對朝鮮的惡意網路活動，美國定期與世界各國合作，通過外交、軍事、執法和司法、網路防禦等管道共享資訊和證據，以提高對朝鮮網路威脅的認識。為了阻止朝鮮通過網路手段竊取資金的努力並防禦朝鮮的惡意網路活動，美國強烈敦促各國加強網路防禦；關閉在第三國的朝鮮合資企業；並以符合適用國際法的方式驅逐位於外國的朝鮮資訊技術工作者。聯合國安理會2017年的一項決議要求所有成員國在2019年12月22日之前遣返在國外賺取收入的朝鮮國民，包括資訊技術工作者。美國還爭取增強外國政府和私營部門了解、識別、防禦、調查、起訴和應對朝鮮的網路威脅，並參與國際努力以幫助確保網路空間的穩定。

從事違禁或可制裁行為的後果

從事或支持朝鮮網路相關活動，包括處理相關金融交易的個人和實體，應意識到從事違禁或可制裁行為的潛在後果。

美國財政部外國資產控制辦公室（OFAC）有權對任何確定具有以下和其他行為的人施加制裁：

- 代表北韓政府或朝鮮勞動黨開展了破壞網路安全的重大活動；
- 在北韓的資訊技術（IT）行業工作；
- 從事某些其他惡意的基於網路的活動；或者
- 從事至少一項重大的從北韓進口或向北韓出口的任何商品、服務或技術。

此外，如果美國財政部長經與美國國務卿協商，確定某一外國金融機構在知情的情況下進行了或協助了對北韓的重大貿易，或在知情的情況下進行了或協助了與代表根據與北韓有關的行政命令或根據與北韓有關的活動的第 13382 號行政命令（大規模毀滅武器擴散者及其支持者）所指認的人的重大交易，或違反了其他可能的限制，該機構可能失去在美國維持往來帳戶或付款賬戶的能力。

美國財政部外國資產控制辦公室對明顯違反其制裁規定的行為進行調查，並按照《經濟制裁執行指南》（聯邦法規 C.F.R. 31 501 部分，附錄 A）所述行使執法權。違反《北韓制裁法規》（聯邦法規 C.F.R. 31 501 部分）的人可能面臨民事罰款，數額可達適用的法定最高罰款額度或相關交易價值的兩倍。

2019 年專家小組中期報告指出，朝鮮使用和企圖使用網路手段從銀行和數字貨幣交易所竊取資金可能會違反聯合國安理會多項決議，即聯合國安理會 1718 號決議執行部分第 8（d）段；聯合國安理會 2094 號決議執行部分第 8 和第 11 段；以及聯合國安理會 2270 號決議執行部分第 32 段。與朝鮮有關的聯合國安理會決議還提供了各種機制，以鼓勵遵守聯合國實施的有關朝鮮的制裁。例如，聯合國安理會 1718 委員會可對與聯合國指認實體進行業務交易或逃避制裁的任何個人或實體實施有針對性的制裁（即資產凍結，禁止個人旅行）。

美國司法部對故意違反適用制裁法的行為提起刑事訴訟，例如《美國國際緊急經濟權力法》（美國法典 50 U.S.C. §§ 1701 及以下）。故意違反此類法律的人將面臨最高 20 年的徒刑，最高 100 萬美元或相當于總收入兩倍的罰款（以較高者為準），並沒收參與此類交易的所有資金。司法部還刑事起訴蓄意違反《銀行保密法》（BSA）（美國法典 31 U.S.C. §§ 5318 和 5322）的行為。其中要求金融機構保持有效的反洗錢計劃並向 FinCEN 提交某些報告，以及其他要求。違反《銀行保密法》的人將面臨最高 5 年的徒刑，最高 25 萬美元的罰款，並可能沒收與違規行為有關的財產。在適當的情況下，司法部還將對違反這些法規的公司和其他實體進行刑事起訴。司法部還與外國夥伴合作，分享證據，以支持彼此的刑事調查和起訴。

根據美國法典 31 U.S.C. § 5318(k)的規定，美國財政部長或司法部長可以傳喚在美國設有代理銀行帳戶的外國金融機構，以獲取該機構儲存在海外的記錄。如果美國財政部長或司法部長向美國金融機構發出書面通知，而外國金融機構未遵守該傳票，則該美國金融機構必須在 10 個工作日內終止其代理銀行業務關係。否則，美國金融機構可能會受到每日民事處罰。

關於朝鮮的司法獎賞

如果您掌握有關朝鮮在網路空間進行非法活動的資訊，包括過去或正在進行的行動，通過美國國務院司法獎賞計劃提供此類資訊，可能使您有資格獲得最高 500 萬美元的獎賞。有關更多詳細資訊，請訪問 www.rewardsforjustice.net。

附件一：美國政府應對朝鮮網路威脅的公共資訊和資源

美國國家情報局主任辦公室的美國情報界年度全球威脅評估。2019年，美國情報界評估朝鮮對金融機構構成了重大的網路威脅，仍然是網路間諜活動威脅，並保留了進行破壞性網路攻擊的能力。朝鮮繼續利用網路能力從金融機構竊取收入。平壤的網路犯罪活動包括試圖從全球金融機構竊取超過11億美元的資金，包括成功地從孟加拉國銀行竊取大約8100萬美元。可以在以下網址找到該報告 https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf。

網路安全和基礎設施安全局（CISA）技術報告。美國政府將朝鮮的惡意網路活動稱為『隱身眼鏡蛇』。『隱身眼鏡蛇』報告提供了有關朝鮮網路行動者所使用的工具和基礎設施的技術細節。這些報告使網路防御者能夠識別並減少朝鮮惡意網路活動的影響。網路安全和基礎設施安全局的網站包含有關這些持續威脅的最新消息：https://www.us-cert.gov/northkorea。

此外，網路安全和基礎設施安全局為利益相關者提供了廣泛的網路安全和基礎設施安全知識和實踐，分享了這些知識以實現更好的風險管理，並將其付諸實踐以保護國家的關鍵職能。以下是網路安全和基礎設施安全局資源的鏈接：

- 保護保護關鍵基礎設施：https://www.cisa.gov/protecting-critical-infrastructure
- 網路安全：https://www.cisa.gov/cyber-safety
- 發現和預防：https://www.cisa.gov/detection-and-prevention
- 資訊分享：https://www.cisa.gov/information-sharing-and-awareness
- 網路安全和基礎設施安全局深度見解：https://www.cisa.gov/insights
- 打擊網路犯罪：https://www.cisa.gov/combating-cyber-crime
- 網路安全必讀：https://www.cisa.gov/cyber-essentials
- 安全建議：https://www.us-cert.gov/ncas/tips
- 國家網路意識系統：https://www.us-cert.gov/ncas
- 工業控制系統通告：https://www.us-cert.gov/ics
- 報告事件、網路釣魚、惡意軟體和漏洞：https://www.us-cert.gov/report

美國聯邦調查局的私人行業通知和警報報告。美國聯邦調查局的私營行業通知（PIN）提供最新資訊，可增強私營部門對潛在網路威脅的認識。美國聯邦調查局的聯絡警報系統（FLASH）報告包含聯邦調查局收集的重要資訊，供特定的私營部門合作夥伴使用。它們旨在為受眾提供可以用於行動的情報，以幫助網路安全專業人員和系統管理員防範網路罪犯的持續惡意行為。如果您發現企業內有任何可疑活動或掌握相關資訊，請立即聯繫聯邦調查局的CYWATCH。欲獲得與朝鮮有關的網路威脅私營行業通知或聯絡警報系統報告，請聯繫cywatch@fbi.gov。

- 聯邦調查局網路處：https://www.fbi.gov/investigate/cyber
- 聯邦調查局法律專員計劃：聯邦調查局法律專員的核心任務是在指定的外國建立並保持與主要執法機構和安全服務部門的聯繫。https://www.fbi.gov/contact-us/legal-attache-offices

美國網路司令部惡意軟體資訊發布。美國國防部的網路部隊積極尋找朝鮮的惡意網路活動，包括用於詐騙金融機構惡意軟體，進行間諜活動的惡意軟體，以及進行針對美國及其合作夥伴的惡意網路活動的惡意軟體。美國網路司令部會定期發布惡意軟體資訊，為行業和政府識別漏洞，以保護其基礎設施和網路免受朝鮮非法活動之害。可以在以下推特（Twitter）帳戶中找到支持網路安全的惡意軟體資訊：@US_CYBERCOM 和 @CNMF_VirusAlert。

美國財政部制裁資訊和非法融資警報

外國資產控制辦公室 (OFAC) 的網上資源中心提供了大量有關朝鮮制裁和針對惡意網路活動的制裁的資訊，包括制裁通告、相關法規、行政命令和與朝鮮及網路相關制裁的規章。外國資產控制辦公室還發布了一些有關朝鮮制裁、與網路相關的制裁和數字貨幣的常見問題解答。如果對外國資產控制辦公室制裁法規和規定有任何問題或疑慮，請致電1-800-540-6322與外國資產控制辦公室的合規熱線聯繫，或發電子郵件至 OFAC_Feedback@treasury.gov

- 朝鮮制裁
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx
  - 常見問題解答 - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk
- 惡意網路活動制裁
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx
  - 常見問題解答 - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber
  - 關於虛擬貨幣的常見問題解答 - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

金融犯罪執法網（FinCEN）已發布有關朝鮮使用國際金融體系的通告（https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008）。FinCEN還向承擔可疑活動報告義務的金融機構發布了具體的通告，為何時以及如何報告網路犯罪和/或與數字貨幣相關的犯罪活動提供了指導：

- 網路犯罪
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005
- 非法數字貨幣活動
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003
- 企業電子郵件洩露
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

聯邦金融機構檢查委員會（FFIEC）開發了網路安全評估工具，以幫助金融機構識別其風險並確定其網路安全準備情況。評估工具可以在以下鏈接找到 https://www.ffiec.gov/cyberassessmenttool.htm。

附件二：聯合國專家小組關於朝鮮網路威脅的報告

聯合國1718制裁委員會（朝鮮）專家小組報告。聯合國安理會1718朝鮮制裁委員會得到一個專家小組的支持，該專家小組『收集、審查和分析』聯合國會員國、聯合國有關機構和其他各方執行聯合國安理會針對朝鮮的決議中概述的措施的資訊。該小組還通過向1718委員會提供中期報告和最終報告，就如何改善制裁的執行提出建議。這些報告可以在以下的鏈接找到https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports。