**2022 年 5 月 16 日**

# 朝鮮民主主義人民共和國(北韓)資訊技術工作人員指南

美國國務院、美國財政部和聯邦調查局 (FBI) 向國際社會、私營部門和公眾發布此公告，以警告朝鮮民主主義人民共和國 (DPRK, 簡稱北韓）資訊技術（IT）工作人員在冒充非北韓國民嘗試獲得就業。對於從事或支持北韓 IT 工作人員相關活動和處理相關金融交易的個人與實體，存在影響聲譽風險和可能需要承擔的法律責任，比如美國和聯合國 (UN) 當局的制裁。

北韓違反美國和聯合國的制裁規定，在世界各地派遣數千名高技能的 IT 工作人員，為其大規模殺傷性武器 (WMD) 和彈道導彈計劃做出經濟上貢獻。這些 IT 員工利用對特定 IT 技能（例如軟體和行動應用程式開發）的現有需求，從包括北美、歐洲和東亞在內等世界各地的客戶那裡獲得自由職業者合同。在許多情況下，北韓 IT 工作人員表明自己為美國和/或非北韓遠程工作人員。工作人員可能通過將工作分包給非北韓人，而進一步混淆他們的身份和/或位置。儘管北韓 IT 工作人員通常從事與惡意網絡活動不同的 IT 工作，但他們利用作為承包商獲得的特權訪問權限，來實現北韓的惡意網絡入侵。 此外， 在此也可能存在員工被強迫勞動的情況。

此公告提供了有關北韓 IT 工作人員如何運作的詳細資訊；僱用自由開發者的公司以及自由職業者和支付平台識別北韓 IT 工作人員時可能存在的危險信號；為公司提供的一般緩解措施，以更好地避免無意中僱用北韓 IT 工作人員或為相關工作運作提供便利。附件提供了來自聯合國 1718 制裁委員會北韓專家小組的報告，其關於北韓 IT 工作人員的更多資訊。FBI 鼓勵美國公司向當地外地辦事處舉報可疑活動，其包括任何可疑的北韓 IT 工作人員活動。

## 北韓 IT 工作人員：背景

北韓 IT 工作人員提供了重要的收入來源，幫助資助北韓政權的最高經濟和安全優先事項，例如相關武器開發計劃。北韓領導人金正恩意識到 IT 工作人員作為外匯與收入的重要來源之重要性，并且可利用其收入扶持他們的運營。

數以千計的北韓 IT 工作人員被派往海外以及一些位於北韓境內都將所獲得的的收入匯回北韓政府。北韓 IT 工作人員主要分佈在中華人民共和國 (PRC) 和俄羅斯，還有少量的人員在非洲和東南亞。這些 IT 員工通常依靠他們的海外聯繫人為他們獲得自由職業，並更直接地與客戶互動。

所有北韓 IT 工作人員所賺的錢都用於扶持北韓領導人金正恩的政權。絕大多數的工作人員都隸屬於直接參與北韓聯合國禁止的大規模殺傷性武器和彈道導彈計劃，以及先進的常規武器開發和貿易部門的實體並為其工作。這導致北韓利用這些北韓 IT 工作人員產生的收入來開發其大規模殺傷性武器和彈道導彈計劃，這違反了美國和聯合國的制裁。其中許多實體單位已被聯合國和美國指定為制裁對象。派遣北韓 IT 人員的北韓實體單位包括：

- **軍需工業部 (MID) 313 總局**負責控制北韓的武器研發和生產——包括核武器和彈道導彈以及其他軍事裝備。MID 隸屬於北韓勞動黨中央委員會，並通過 313 總局將北韓的大部分 IT 勞動力部署到海外。北韓勞動黨的所有財產和財產權益已根據行政命令 (EO) 13722 遭受封鎖。
- **原子能工業部**——北韓核武器發展的關鍵角色，負責北韓核武器計劃的日常運作。原子能工業部根據 EO 13382 指定的。
- 軍事實體單位隸屬於**國防部和北韓人民軍**。北韓人民軍被列入特別指定國民和封鎖財產清單。
- 鮮為人知的實體單位，如**北韓教育委員會對外貿易辦公室**和**中央科教部平壤資訊技術局**。北韓政府的所有財產和財產權益根據 EO13722 遭受封鎖。

一名海外北韓 IT 工作人員的收入至少是在工廠或海外建築項目中從事傳統工作的北韓工人的十倍。在某些情況下，北韓 IT 工作人員個人的年收入可以超過 300,000 美元，而 IT 工作人員團隊的年收入總數可以超過 300 萬美元。他們總收入的很大一部分支持北韓政權的優先事項，包括其大規模殺傷性武器計劃。

北韓 IT 公司及其員工通常從事各種複雜與艱難的 IT 開發工作，例如：

- 行動應用程式和基於網絡的應用程式,
- 建立虛擬貨幣交易平台和數字貨幣,
- 一般 IT 技術支持,
- 圖形動畫,
- 線上賭博程式,
- 手機遊戲,
- 交友應用程式,

- 人工智能相關應用，
- 硬體和韌體開發，
- 虛擬實境和增強實境編程，
- 臉部和生物特徵辨識軟體，以及
- 數據庫開發和管理。

北韓 IT 工作人員開發的應用程式和軟體涵蓋了一系列領域和部門，包括商業、健康和健身、社交網絡、體育、娛樂和生活型態等方面。北韓 IT 工作人員經常參與涉及虛擬貨幣的項目。一些北韓 IT 工作人員為虛擬貨幣交易者設計了虛擬貨幣交易所或創建了分析工具和應用程式，並自行推銷他們的產品。

幾十年來，北韓一直強調數學和科學教育對其公民的重要性。對科學技術進步的重視，歷來是金氏政權的優先事項，這也反映在對相關研究領域的資源和人員投入上。北韓今日的網絡和 IT 教育建立在渴望持續進步的基礎上，並形成了與勞動黨、研究中心和軍隊協調的綜合課程。

- 近年來，在金正恩的領導下，北韓政權越來越重視資訊技術相關學科的教育和培訓，尤其是在北韓的幾所主要教育機構——特別是金日成大學、金策科技大學和平壤科技大學等。僅這些頂尖大學就有大約 30,000 名學生學習資訊和通訊技術相關學科。

- 據報導，截至 2019 年，37 所大學開設了 85 個課程，提供包括資訊安全在內的高級科學、技術、工程和數學 (STEM) 學科的課程。每一個省份至少新建了一所中學，以培養有前途的學生。

- 北韓教育體系競爭激烈，只有名列前茅的學生才能進入精英科技項目。來自金頌書院和金頌一中等中學的學生自小就被招收。

- 北韓 IT 工作人員在海外和他們自己的組織接受額外培訓，通常通過北韓境內的區域 IT 研究中心進一步發展他們的技能。北韓 IT 工作人員歷來在東非、東南亞和南亞接受過培訓，並從海外培訓中獲益良多。

## 北韓 IT 工作人員的運作方式

北韓 IT 工作人員的目標是來自較富裕國家包括北美、歐洲和東亞的雇主的自由職業者合同。在許多情況下，北韓 IT 工作人員表明自己為韓國、中國、日本或東歐和美國的遠程工作人員。

在某些情況下，北韓 IT 工作人員通過第三方分包商的安排，來進一步混淆他們的身份。這些分包商是為北韓 IT 工作人員完成合同的非北韓自由職業 IT 工作人員。北韓 IT 經理還僱傭了自己的非北韓 IT 員工團隊，他們通常不知道北韓雇主的真實身份，也不知道他

們的雇主是北韓公司這一事實。北韓 IT 經理利用他們的外包員工購買軟體，並讓其與客戶互動，以防暴露北韓 IT 工作人員的身分。

儘管北韓 IT 工作人員通常從事非惡意 IT 工作，例如開發虛擬貨幣交易所或網站，但他們都曾利用作為承包商獲得的特權訪問權限來進行北韓的惡意網絡入侵。一些駐在海外的北韓 IT 工作人員為駐在北韓的惡意網絡行為者提供了後勤支持，儘管 IT 工作人員本身不太可能參與惡意網絡活動。北韓 IT 工作人員可以共享對虛擬基礎設施的訪問權限，協助售出被北韓網絡行為者竊取的數據，或協助北韓進行洗錢和虛擬貨幣轉移。

北韓 IT 工作人員還協助北韓官員為北韓的違禁武器計劃採購大規模殺傷性武器和彈道導彈相關物品。

在某些情況下，工人亦會遭受人口販運，包括強迫勞動。 可靠的報告顯示，許多北韓海外員工工作時間過長，受到北韓政府安全人員持續和密切監視，生活條件不安全和不衛生，且幾乎沒有什麼行動自由。 北韓政府扣留了高達 90% 的海外員工工資，這為政府帶來了數億美元的年收入。

### *北韓 IT 工作人員：技術與平台*

北韓海外 IT 團隊最常通過各種線上平台獲得自由職業工作。公司使用這些平台來宣傳 IT 自由開發者可競標的項目合同。極為少見的是，北韓 IT 團隊會尋找當地非北韓國民擔任實際由北韓人控制的公司之名義負責人。在某些情況下，北韓 IT 團隊在帳面上看似為一家合法的當地公司工作，但其實它正從事自己的業務——北韓 IT 團隊會向外國公司支付其費用，來作為隱藏源自北韓背景的回報。北韓 IT 團隊通常包括精通外語的成員，例如精通英語或中文等。

北韓 IT 工作人員使用各種主流和 IT 行業特定的自由職業者合同平台、軟體開發工具與平台、訊息傳遞應用程式、社交媒體與網站為世界各地的公司獲得開發合同，並利用許多數位支付平台與網站收取工作報酬。北韓 IT 工作人員還使用虛擬貨幣交易所和交易平台來管理他們因合同工作收到的數位支付款項，以及用其洗錢和轉移他們收到的資金。

### *北韓 IT 工作人員：隱藏他們的身份*

北韓 IT 工作人員故意在網上混淆他們的身份、位置和國籍，通常使用非韓國名字作為別名。他們還將使用虛擬私人網絡 (VPN)、虛擬私人服務器 (VPS) 或利用第三國 IP 地址，使他們看起來好像從不顯眼的地方連接到網際網路，並減少對其北韓位置或關係被進行審查的可能性.北韓 IT 工作人員通常依賴遠程工作具有的匿名特性，使用代理來建立和維護帳戶，並傾向於通過中介或使用文字聊天而非使用視訊通話交流。

北韓 IT 工作人員使用代理帳戶在自由軟體開發者網站上競標、得標、工作錄取等來獲取報酬。這些代理帳戶屬於第三方個人使用，其中一些人將其身份和帳戶資訊出售給北韓

IT 工作人員。在某些情況下，北韓 IT 工作人員向這些個人支付費用以使用其合法平台帳戶。北韓 IT 工作人員可以使用代理人的真實從屬關係和工作經驗來填寫自由職業者平台中的相關文件。

有時，北韓的 IT 工作人員會在平台上與其他非北韓自由職業者合作，就開發項目提出合作建議。北韓 IT 員工利用這些業務關係獲得新合同和虛擬貨幣帳戶的訪問權限，這些合同和虛擬貨幣帳戶用於在美國或歐洲的虛擬基礎設施上開展 IT 工作，繞過旨在防止欺詐性使用的安全措施。在其他自由職業者的幫助下建立帳戶時，北韓 IT 工作人員可能會自稱是第三國國民，需要美國或其他西方人士的身份證明文件和自由職業者平台帳戶來賺取更多的錢。

隱藏他們的真實位置使北韓 IT 工作人員能夠違反他們用於活動的線上平台與服務之服務協議條款。作為其交易技巧的一部分，北韓 IT 工作人員也可能為每個帳戶設有單一的專用設備，尤其是銀行服務，以規避預防欺詐、制裁合規與反洗錢措施的檢測。

北韓 IT 工作人員經常使用偽造、篡改或造假的文件，包括身份證明文件和偽造簽名——這些文件是他們使用 Photoshop 等軟體製成的，或是他們花錢請文件偽造公司進行修改，將 IT 工作人員自身的或提供照片與真實人物的身分資訊進行結合。北韓 IT 工作人員通常會購買偽造文件，例如：

- 駕駛執照，
- 社會安全卡，
- 護照，
- 國民身份證，
- 外國人永久居留證，
- 高中與大學文憑，
- 工作簽證，以及
- 信用卡、銀行和水電費帳單。

在某些情況下，這些身份是被盜取來的，而在另一些情況下，北韓 IT 工作人員則是唆使非北韓國民用他們自己的個人資訊或他們可以訪問的資訊建立帳戶，然後將帳戶的控制權有償轉讓給北韓 IT 工作人員。這使得北韓 IT 工作人員可以通過遠程桌面訪問使用真實帳戶持有人的基礎設施，線上為客戶競標和完成自由職業者項目時隱藏自身身份。每個 IT 工作人員經常使用多個身份和帳戶，這些身份和帳戶也可以於同一團隊中的 IT 工作人員之間共享。這些帳戶和身份自稱來自於世界各地的國家。

北韓 IT 工作人員可能會竊取美國或國際銀行的客戶帳戶資訊，以便於自由職業者平台、支付供應商和僱用北韓 IT 工作人員的公司驗證他們的身份。至少在一個案例中，北韓 IT 工作人員利用偷來的銀行帳戶資訊進行支票偽造。與北韓 IT 工作人員的代理身份相關的帳戶與簡歷通常包括偽造、但真實且詳細的教育與就業歷史資訊，其包括教育機構和以前雇主的虛假聯繫資訊。

北韓 IT 工作人員還可以在他們線上開發人員資料的就業部分填寫中小型西方公司的名稱，以便北韓 IT 工作人員在項目競標中看起來像是有信譽的美國人或歐洲人。他們可能會使用與西方公司合法域名相似的實際員工姓名和電子郵件地址。

北韓 IT 工作人員還偽造工作協議書、發票、客戶通訊文件和其他用於自由職業者平台等文件，也許是用於滿足平台上的了解相關客戶和反洗錢 (KYC/AML) 措施或類似用於確保用戶活動的合法性程序。這些偽造的文件可能會附上最低限度的聯繫方式資訊以避免驗證。

北韓 IT 工作人員也可能試圖通過將自己偽裝成韓國人或“韓國”公民來掩蓋他們的國籍。

眾所周知，在不知情的公司中獲得自由職業者職位的北韓 IT 工作人員隨後都會向該公司建議雇用其他的北韓 IT 自由職業工作者。

### *北韓 IT 工作人員的簡歷*

北韓 IT 工作人員會宣傳他們在系統與程式開發、數據庫管理系統以及使用各種通用語言、框架、工具和雲端資源方面等的技術。這些通常包括多種編碼和標記式語言的強大技術。 大多數北韓 IT 工作人員的活動項目都與行動與網絡應用程式開發有關。 北韓 IT 工作人員也使用協作共享平台和託管服務進行數據和工作流管理。 這些員工通常聲稱說有使用各種數據庫的經驗，並且熟悉主要提供商的雲端和分析產品與服務。 此外，北韓 IT 工作人員將數位支付和電子商務平台納入其工作中。

北韓 IT 工作人員建立“作品集”網站，通常設計簡單，以提高他們虛構的自由開發者角色的可信度。這些虛構作品集代表了北韓 IT 工作人員的職責工作，並且通常與他們的線上自由開發者帳戶有相關聯。這些網站上的資訊，包括聯繫資訊和地點，以及工作經歷與教育，都可能是虛假的。

## 危險信號

***自由職業者和支付平台公司應注意以下活動，這些活動可能是北韓 IT 工作人員可能使用其平台的跡像或行為。***

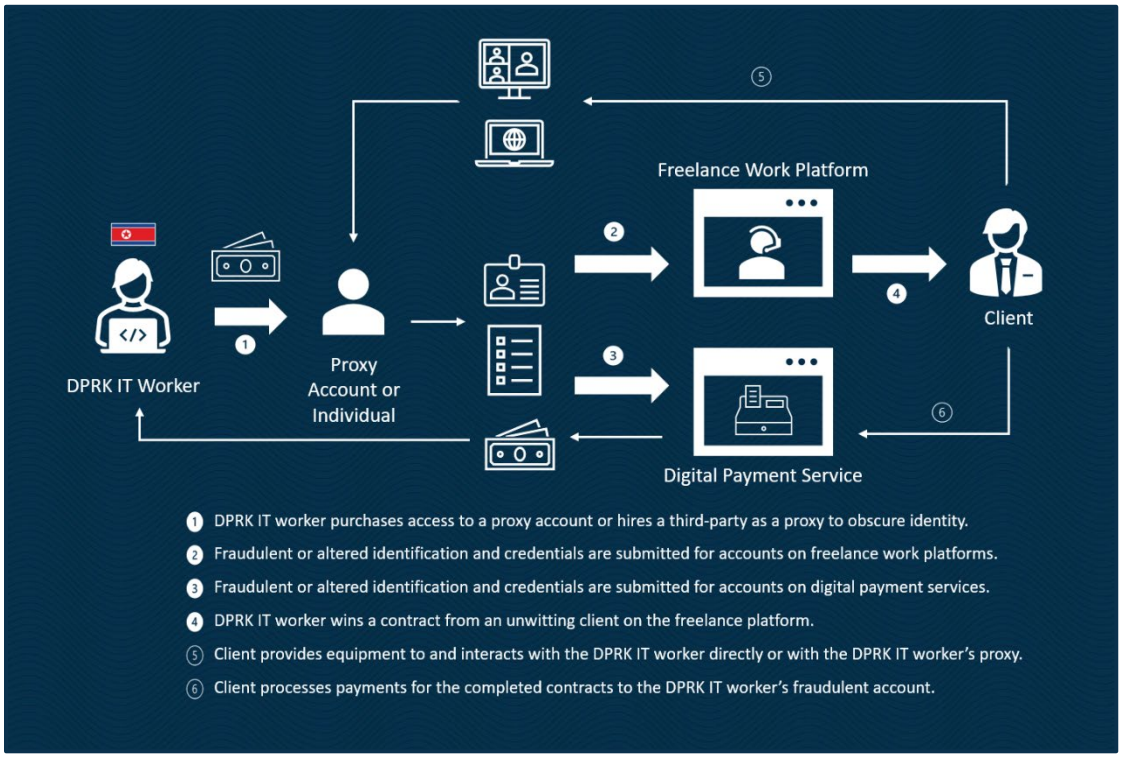
- 在相對較短的時間內從多個 IP 地址多次登錄同一個帳戶，特別是如果這些 IP 地址與不同的國家有關；
- 開發者在同一個平台上通過一個 IP 地址登錄多個帳戶；
- 開發人員連續一天或多天地登錄他們的帳戶；
- 路由器連接埠或與使用遠程桌面共享軟體相關的其他技術設定，例如用於訪問帳戶的路由器中的 3389 連接埠，特別是如果遠程桌面共享軟體的使用非公司的標準作業；
- 開發者帳戶使用欺詐性客戶帳戶來提升開發者帳戶評級，但客戶和開發者帳戶都使用同一個 PayPal 帳戶進行轉帳/取款（用自己的錢支付自己）；
- 招標文件、項目溝通方式等文件模板頻繁使用，尤其是同一個模板在不同開發者帳戶間使用；
- 多個開發者帳戶在短時間內從同一個客戶帳戶獲得高評價，並且用相似或相同文件來建立開發者帳戶和/或客戶帳戶；
- 對活動項目進行廣泛的競標，與開發商競標的項目數量相比，被接受的項目競標數量較少；和
- 經常通過支付平台轉帳，尤其是轉帳給中國的銀行帳戶，有時通過一家或多家公司來掩飾資金的最終目的地。

***僱用自由開發人員的公司應注意以下可能是北韓 IT 工作人員的跡像或行為的活動。***

- 如果自由軟體開發者網站或支付平台帳戶已被關閉，或者員工聯繫雇主要求使用來自不同的帳戶（特別是如果帳戶以不同的名字註冊）；
- 使用數位支付服務，尤其是與中國有關的服務；

- 開發人員的自由職業者平台簡介、社交媒體簡介、外部投資組合網站、支付平台簡介以及猜測估計的地點與時間中的姓名拼寫、國籍、聲稱的工作地點、聯繫資訊、教育經歷、工作經歷和其他詳細資訊不一致；
- 異常簡單的作品集網站、社交媒體簡介或開發人員簡介；
- 來自自稱是軟體開發公司的 C 級主管的個人訊息傳遞或推銷電話，以徵求服務或宣傳專業技能；
- 要求客戶與潛在客戶於另一個獨立平台進行溝通，而非原本客戶使用 IT 自由職業者平台網站；
- 雇主建議將文件或與工作相關的設備（例如筆記本電腦）發送給開發人員，而開發人員要求將物品發送到開發人員身份證明文件中未列出的地址。如果開發人員聲稱他們無法在其身份證明文件上的地址收到物品，請務必慎重；
- 尋求虛擬貨幣支付以逃避 KYC/AML 措施和正規金融系統；
- 在未達到生產基准或簽到會議的情況下要求支付合同款項；
- 無法在規定的營業時間內開展業務；
- 不正確的或不斷變更的聯繫資訊，特別是電話號碼和電子郵件；
- 與申請人不符的簡歷資訊；
- 未按時完成任務或未對任務作出回應；
- 無法及時聯繫到他們（尤其是通過“即時”溝通方式）；和
- 要求同事借用他們的一些個人資訊來獲得其他合同。

## *北韓 IT 工作人員運營概述*




## 可能的緩解措施

### *對於自由職業者和支付平台公司*

- 作為提案審查和進行合同盡職調查程序一部分而提交的文件(如獨立審核的發票與工作協議)，通過使用商業數據庫中的聯繫資訊，而不是所提交文件中提供的聯繫資訊，與所列客戶進行聯繫；

- 仔細審查疑為偽造而上交的身份驗證文件，亦可能向當地執法部門尋求幫助。拒絕低質量圖像作爲身份驗證；

- 驗證是否存在為建立帳戶而提供的任何網站；加強對利用已失效網站建立帳戶的任何帳戶的審查。

- 作為初始盡職調查合同流程和更新政策的一部分，要求提交驗證身份的影片或進行視訊面試以驗證身份；

- 定期使用連接埠檢查功能來確定是否通過桌面共享軟體或 VPN 或 VPS 遠程訪問平台，特別是在使用遠程桌面共享軟體或 VPN 服務訪問帳戶並非標準作業的情況下；

- 自動標記出使用相同或類似文檔建立帳戶或使用相同數位支付服務帳戶的客戶和開發人員帳戶，以便進行額外的審查；

- 在不同開發者帳戶之間使用相同或相似的文檔模板進行投標和項目溝通時，會自動標記為需額外審查；

- 自動標記出在短時間內從單一客戶帳戶獲得高評價的多個開發者帳戶以進行額外審核，尤其是在使用相似或相同的文檔建立帳戶時；

- 自動標記出與項目競標數量相比具有高投標率的開發人員帳戶以及接受項目競標數量較少的帳戶，以便進行額外的審查。此外，標記出項目競標數量相對於帳戶登錄次數較多的帳戶；

- 在全面驗證其帳戶之前，不允許在新建立的帳戶中進行任何活動；

- 對新建立的帳戶進行額外審查；和

*適用於在自由職業者平台上招聘程式設計師和開發人員的公司*

- 進行視訊面試以驗證自由職業者的身份；

- 進行就業前背景調查、藥物測試和指紋/生物辨識登錄，以驗證他們的身份和聲稱的位置。避免使用虛擬貨幣付款，並要求驗證與其他身份證明文件相對應的銀行資訊；

- 通過遠程協作應用程式（例如遠程桌面應用程式）與自由開發者互動時要格外小心謹慎。考慮在提供給自由開發者的任何電腦上禁用遠程協作應用程式；

- 使用通過搜索引擎或其他商業數據庫確定的聯繫資訊，直接與上市公司和教育機構核實就業與高等教育歷史，而不是直接從潛在員工或其個人資料中獲取。

- 檢查僱員的姓名拼寫、國籍、聲稱的位置、聯繫資訊、教育經歷、工作經歷和其他詳細資訊是否在開發人員的自由職業者平台簡介、社交媒體簡介、外部投資組合網站、支付平台帳戶和猜測估計中的地點和時間保持一致性。對簡單的作品集網站、社交媒體簡介或開發人員簡介要格外小心；

- 請謹慎對待對於要求在公司最初找到 IT 員工的原始自由職業者平台網站之外的單獨平台上進行交流的開發人員；

- 如果向開發人員發送文件或與工作相關的設備（例如筆記本電腦），請僅發送到開發人員身份證明文件上列出的地址，如果開發人員要求將筆記本電腦或其他物品發送到陌生地址，則應獲取其他有關文件做佐證。如果開發人員無法在其身份證明文件上的地址收到物品，請保持警惕；和

- 對可能由簽約 IT
  員工以欺詐方式進行的未經授權的小規模交易保持警惕。在一個案例中，受雇於一家美國公司的北韓 IT

  開發人員以欺詐手段向美國公司的支付帳戶收費，並在幾個月內分 30
  次小額分期盜取了超過 50,000
  美元。這家美國公司不知道開發人員是北韓人，也不知道由於金額很小而正在進行的盜竊活動。

## 從事被禁止或應受制裁的行為之後果

從事或支持北韓 IT 工作人員相關活動（包括處理相關金融交易）的個人和實體應了解從事被禁止或可制裁行為的潛在法律後果。

聯合國安理會第 2321、2371 和 2397 號決議強調，來自海外北韓員工的收入有助於北韓的核武器和彈道導彈計劃。聯合國安理會第 2375 號決議禁止聯合國會員國為其管轄範圍內的北韓國民提供與進入其領土有關的新工作許可或更新已過期的許可，除非事先得到聯合國安理會 1718 委員會的批准。聯合國安理會第 2397 號決議要求所有會員國在 2019 年 12 月 22 日之前遣返在其管轄範圍內賺取收入的北韓國民——無論何時或是否已為有關北韓國民簽發工作許可。

外國資產控制辦公室 (OFAC) 有權對任何被認定有以下行為的人實施金融制裁：

- 代表北韓政府或北韓勞動黨從事破壞網絡安全的重大活動；

- 代表北韓在 IT 行業開展業務；

- 參與某些其他惡意網絡活動；

- 從事至少一次從北韓進口或向北韓出口任何商品、服務或技術的重大活動；

- 直接或間接地向北韓或代表北韓政府或北韓勞動黨的任何人出售、供應、轉讓或購買軟體、而所涉及的任何收入或貨物可能有利於北韓政府或北韓勞動黨；或

- 向北韓政府或北韓勞動黨提供物質援助、贊助或提供財政、物質或技術支持，或提供貨物或服務等以支持北韓政府或北韓勞動黨。

例如，2018 年，美國指定制裁中國科技公司延邊銀星網絡科技有限公司。這家公司名義上是一家中國 IT 公司，但實際上它是由北韓人管理與控制的。該公司還建立了一家總部位於俄羅斯的幌子公司 Volasys Silver Star，以規避自由職業者論壇上的身份識別要求。

此外，如果財政部長在與國務卿協商後確定外國金融機構故意與北韓進行或促進了重大貿易，或在知情的情況下代表根據一項指定的人進行或促進了重大交易與北韓有關的行政命令，或根據針對北韓相關活動的第 13382 號行政命令（大規模毀滅性擴散者及其支持者），該機構除其他潛在限制外，可能會失去在美國維持代理或支付過渡帳戶的控制權。

外國資產控制辦公室（OFAC） 調查明顯違反其制裁條例的行為並行使執法權力，如《經濟制裁執法指南》31 C.F.R.第 501 部分附錄 A 所述。違反北韓制裁條例 31 C.F.R.第 510 部分的人可能面臨以下民事罰款最高為適用的法定最高罰款或相關交易價值的兩倍，以較高者為準。

此外，《美國敵對國家制裁法案》（CAATSA；公法 115-44）第 321(b) 節（22 USC § 9241a 等條例）修訂了 2016 年北韓制裁和政策強化法案（22 USC § 9241 等條例），該條款建立了一個可反駁的推定，即全部或部分由北韓國民或北韓公民在世界任何地方開採、生產或製造的重要商品、貨物、物品屬根據 1930 年《關稅法》（如 19 USC § 1307 等條例)禁止進口的強迫性勞動商品。這意味著這些貨物無權進入美國的任何港口，並可能被扣留、扣押和沒收。違規行為可能會導致民事處罰以及刑事起訴。但是，根據 CAATSA 的規定，如果美國海關和邊境保護局 (CBP) 通過明確和令人信服的證據發現，貨物不是由罪犯勞工、勞工強迫或契約勞工生產的，則可批准此類貨物可以進口到美國。根據 1930 年的《關稅法》，禁止進口由囚犯勞工、強迫勞工或契約勞工生產的受刑事制裁（包括強迫或契約童工）的商品，因此此法已實施近 90 年.

司法部負責調查和起訴適用的聯邦法律，包括《國際緊急經濟權力法》（簡稱“IEEPA”），50 USC §§ 1701 et seq. 和《銀行保密法》（BSA），31 USC § § 5318 和 5322。根據 IEEPA，故意違反、企圖違反、共謀違反或導致違反 IEEPA 規定的任何許可、命令、法規或禁令問題，包括任何與北韓相關的行政命令（例如，行政 13722 和 13810 號命令）、13382 號行政命令和《北韓制裁條例》，31 CFR 第 510 部分，皆屬於犯罪。故意違反 IEEPA 的人將面臨最高 20 年的監禁、最高 100 萬美元的罰款或總額為總收益兩倍的罰款，以較高罰金為準，並可能沒收參與此類交易的所有資金。BSA 要求金融機構維持有效的反洗錢計劃，並向 FinCEN 提交相關報告。違反 BSA 的人可能面臨最高 5 年的監禁、最高 250,000 美元的罰款，並可能沒收涉及此類違規行為的財產。違反 IEEPA、BSA 和其他適用聯邦法律的公司和其他實體也可能受到刑事起訴。司法部還與外國合作夥伴合作分享證據，以支持美國和國外的刑事調查和起訴。

根據 31 USC § 5318(k) 的規定，財政部長或司法部長可以傳喚在美國擁有代理銀行帳戶的外國金融機構，以獲取存儲在海外的記錄。如果財政部長或總檢察長書面通知美國金融機構，指出外國金融機構未能遵守此類傳票，美國金融機構必須在十個工作日內終止代理銀行關係。否則，美國金融機構可能會受到日常民事處罰。

### *北韓正義獎賞計畫*

如果您掌握有關北韓在網絡空間中的非法活動的資訊，包括過去或正在進行的行動，通過國務院的“正義獎賞計畫”提供此類資訊，您就有資格獲得最高 500 萬美元的獎勵。如需了解更多詳情，請訪問 https://rewardsforjustice.net/index/?north-korea=north-korea 。

## 附件

### *聯合國專家小組關於北韓 IT 工作人員的報告*

聯合國安理會第 1718 號決議制裁北韓委員會由一個專家小組提供支持，該小組收集、審查和分析來自聯合國會員國、聯合國相關機構和其他各方的關於其執行聯合國安理會針對北韓的決議制裁措施中概述的措施資訊。該小組還向 1718 委員會提供中期和最終報告，就如何改進制裁執行提出建議。這些報告可在以下網址找到：https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

專家小組已調查了多起北韓 IT 工作人員的案件，例如隸屬於聯合國指定軍火工業部 (MID) 的人員，並在專家小組的半年度報告中提供了有關這些調查的資訊，包括以下內容：

專家組在其 2019 年中期報告中首次報導了北韓 IT 工作人員，指出 MID 在北韓核武計劃和彈道導彈計劃發展中的監督作用，它正在利用其下屬貿易公司在國外駐留北韓資訊技術工作人員，例如軟體程式員和開發人員，以賺取外匯。當時，位於歐洲、亞洲、非洲和中東的北韓 IT 工作人員利用外國網站獲取自由職業者工作，並同時偽裝其身份。除了非惡意的資訊技術工作外，北韓 IT 工作人員還進行了涉及盜竊虛擬貨幣等資產的非法工作，以支持北韓網絡行為者規避金融之制裁。

專家組在其 2020 年最終報告中繼續對北韓 IT 工作人員進行調查，發現大多數海外北韓 IT 工作人員受僱於 MID 下屬的公司。截至 2019 年，MID 涉嫌向海外派遣至少 1,000 名 IT 人員以創造收入為目的，通常使用下屬實體或幌子公司。然而，由於他們所使用的混淆技巧，海外和北韓的 IT 工作人員的真實數量尚不清楚。專家組指出，北韓 IT 工作人員使用多種方法在不暴露身份的情況下獲得 IT 自由職業者工作，包括在自由開發者平台上與世界各地不知情的客戶建立帳戶，特別是在中國、俄羅斯、烏克蘭、塞爾維亞、加拿大和美國。專家組進一步調查了中國、尼泊爾和越南的北韓 IT 工作人員團隊和關聯公司的幾個具體案例。

專家小組調查了中國和俄羅斯的一些北韓 IT 工作人員團隊，並在其 2020 年中期報告中詳細說明了他們的調查情況。專家小組注意到，2019 和 2020 年，MID 下屬的數百名北韓 IT 工作人員在中國開展業務，以第三國個人的名義非法訪問自由職業者平台帳戶。專家小組進一步指出，2019 年和 2020 年，北韓 MID 下屬的多組 IT 工作人員在俄羅斯開展業務，利用虛構的外國身份訪問資訊技術自由職業者平台、虛擬貨幣網站和支付網站。

根據專家小組的 2021 年最終報告，北韓 IT 工作人員可以通過使用與北韓訪問國際金融系統類似的混淆方法，包括提供虛構身份證明、使用 VPN 服務來逃避雇主的盡職調查和 KYC/AML 協議，並建立幌子公司。專家小組進一步指出，大多數與北韓有關的帳戶都在

中國境內運營。為避免審查，這些帳戶在與尋求僱用 IT 服務的潛在客戶建立聯繫後會“離場”。與北韓相關的用戶還針對安全級別較低或盡職調查程序不太嚴格的 IT 自由職業者平台。專家小組特別強調了 IT 自由職業者平台在履行合規義務和無意中促進北韓入侵國際支付系統方面面臨的危險，建議聯合國會員國與自由職業者 IT 公司合作，促進和提高制裁合規執行能力。