情況說明書：

朝鮮民主主義人民共和國(北韓)資訊技術工作人員指南

資訊技術工作人員

2022 年 5 月 16 日

美國政府發布此公告作為國際社會、私營部門和公眾的綜合資源，以更好地了解和防備朝鮮民主主義人民共和國（DPRK，又名北韓）資訊技術（IT）工作人員。 該公告提供了有關北韓 IT 工作人員如何運作的詳細資訊，並鑒定了危險信號指標和盡職調查措施，以幫助公司避免僱用北韓自由開發人員，並幫助自由職業者和數位支付平台識別濫用其服務的北韓 IT 工作人員。 僱用或支持北韓 IT 員工的活動會帶來許多風險，從知識產權、數據和資金盜竊到聲譽損害以及法律後果，當中也包括美國和聯合國 (UN) 當局的制裁措施。

北韓已向世界各地派遣了數千名高技能 IT 人員，為北韓違反美國和聯合國制裁的武器計劃提供收入。 這些工作人員：

- 濫用自由職業者平台的整體生態系統，從世界各地的客戶公司偷偷獲取 IT 開發合同——以及濫用許多社交媒體平台，與客戶和支付平台進行溝通，以收取他們的工作報酬；
- 開發涵蓋多個領域的應用程序和軟體，包括但不限於商業、加密貨幣、健康與健身、社交網絡、體育、娛樂與生活型態等方面；
- 在許多情況下，謊稱自身為外國（非北韓）或美國遠程工作人員，包括使用虛擬私人網絡 (VPN)、虛擬私人服務器 (VPS)、購買的第三國 IP 地址、代理帳戶以及偽造或使用被盜取來的身份證明文件；和
- 將作為承包商獲得的特權訪問用於非法目的，包括允許其他北韓行為者進行惡意網絡入侵。

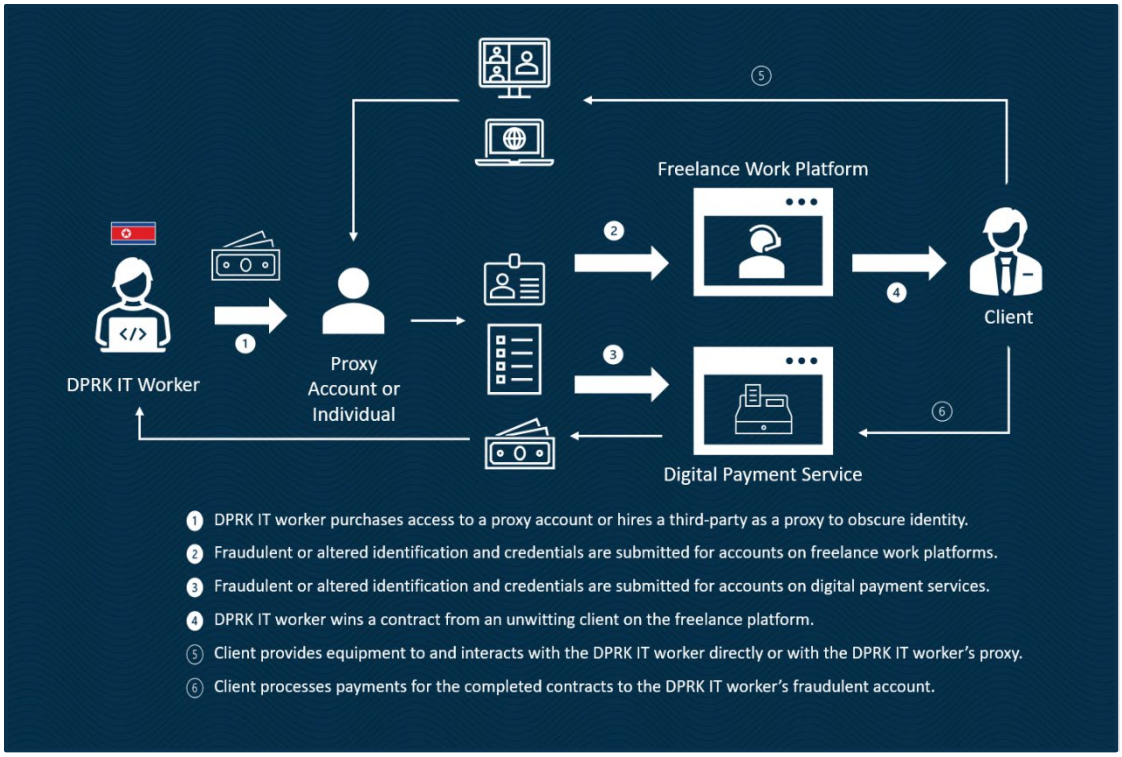
北韓 IT 工作人員潛在活動的一些危險信號包括：

- 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；
- 通過支付平台頻繁轉帳，特別是向中華人民共和國（PRC）銀行帳戶轉帳，或要求以加密貨幣支付；
- 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和時間中的姓名拼寫、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；
- 無法在規定的營業時間內開展業務和無法及時聯繫到他們（尤其是通過“即時”溝通方式）；

私營部門可以考慮採取盡職調查措施，以防止無意或不知情地僱用北韓 IT 員工，包括：

- 直接與所列出的公司和教育機構核實工作申請的一部分提交的文件作為提案審查（不使用提交文件中提供的聯繫資訊）；
- 對偽造的身份證明文件進行嚴格審查；
- 進行視訊面試以驗證潛在自由職業者的身份；
- 進行就業前背景調查和/或指紋/生物識別登錄，以驗證身份和聲稱的位置；
- 避免使用加密貨幣付款，並要求驗證與其他身份證明文件相對應的銀行資訊；
- 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；和
- 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。

北韓 IT 工作人員運營概述



如需獲得更多資訊，請參閱北韓網絡諮詢，瀏覽財政部資源中心，和/或聯繫您的當地聯邦調查局辦公室。如果您有關於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活動，請通過國務院的正義獎賞計畫提供此類資訊，您可能有資格獲得高達 500 萬美元的獎勵。