JENNER & BLOCK

Are You Employing a North Korean IT Worker? What Companies Need to Know to Prepare for and Respond to this Threat

Client Alerts

August 13, 2026
By: Rachel K. Alpert, Aaron R. Cooper, Steven J. Arango, Lauren E. Hackett

On July 31, 2026, the US Department of State and the FBI, joined by counterpart agencies in Australia, Canada, France, Germany, Italy, Japan, the Netherlands, New Zealand, South Korea, and the United Kingdom, issued a joint alert on North Korean IT workers who use false identities to infiltrate companies and fund North Korea's weapons programs. It's the latest in a now-familiar cadence of warnings issued roughly once a year since 2022. Since then, sanctions actions, DOJ indictments, "laptop farm" raids, and FBI warnings underscore the risks associated with these workers, who are engaged in activities from payroll fraud to data theft and extortion; and despite law enforcement's focus, the threat has only become more prominent.

The consequences of mishandling this risk can be significant—government investigations, commercial disputes, reputational harm, theft of confidential information, and in extreme cases, it can involve criminal or civil exposure. Companies can act now to anticipate and guard against the North Korean IT worker threat before they are compromised. Because of the unique threat profile, this preparation should involve updating intrusion detection systems to identify the use of connected devices and remote access tools, ensuring appropriate pre-employment screening for remote workers, assessing sanctions obligations in the event a North Korean IT worker is identified among your employees (or has gained access to your systems through one of your employees), and preparing a new incident response playbook—including appropriate remediation steps and planning for significant law enforcement engagement.

Government Warnings and Typologies

North Korea deploys thousands of skilled IT workers, many based in China, Russia, and elsewhere, using false identification, stolen identities, and proxies to land remote or full-time tech jobs at companies that believe they are hiring ordinary personnel. IT workers' pay flows back to entities tied to North Korea's weapons programs—activity that UN Security Council Resolution 2397 addresses by requiring member states to repatriate North Korean nationals earning income within their jurisdiction. These workers also pose an insider threat: exfiltrating data, planting malware, or extorting their unwitting employer.

The US government and multilateral counterparts have highlighted the threat as it has become more prevalent:

- **2022:** State, Treasury, and the FBI issue the foundational advisory, with the first comprehensive set of red-flag indicators.
- **2023–2024:** Joint updates with South Korea; the United Kingdom's OFSI warns UK firms are targeted too.
- **2025:** The FBI flags a shift to data extortion and AI-driven interview fraud; IC3 warns about United States-based facilitators.
- **2026:** The most broadly multilateral alert to date, spanning 10 allied governments.

The US government is also bringing multiple enforcement tools to bear on countering this threat:

- **2025:** DOJ/FBI coordinated raids on 29 "laptop farms" across 16 states.
- **November 4, 2025:** Treasury sanctions DPRK bankers and institutions involved in laundering cybercrime proceeds and IT worker funds.
- **March 2026:** Office of Foreign Assets Control sanctions six individuals and two entities, citing nearly $800 million generated for the regime in 2024 alone, through cryptocurrency and traditional banking channels.

Thus far, US government efforts have centered on preventative guidance to companies and prosecuting the North Korean perpetrators and the United States-based "mules" supporting them, but victim companies may still face civil or criminal exposure, depending on the nature of the activity, the willfulness of the company's conduct, and the steps the company took to respond.

Beyond penalties, companies can face extortion demands, stolen IP, possible breach-notification duties, and potential reputational or business costs that may follow notifications to any affected third parties.

Building the Right Controls

Developing controls, policies, and procedures before a DPRK IT worker event can help to guard against and mitigate the potential risk.

- **Identity verification:** Require live video interviews pre-employment, and live video attendance post-employment; watch for location mismatches, camera avoidance, or chat-only contact. Verify education and employment history using independently sourced contacts, and cross-check names and locations across resume, platform profile, and payment account.

- **Payment controls:** Avoid or heavily scrutinize crypto payments or third-party accounts. Confirm banking details match ID documents and flag frequent requests to change payment accounts.

- **Ongoing monitoring:** Watch for logins from multiple countries in short succession, or accounts that stay logged in unusually long. Restrict and monitor remote-desktop software, external devices, and VPNs on company devices and apply least-privilege access. Confirm hardware ships only to the address on file.

- **Vendor diligence:** Extend these controls to IT staffing vendors and subcontractors. Recent enforcement has targeted the so-called United States-based "mules" that serve as a local presence for DPRK IT workers, not just the workers themselves.

- **Training and records:** Train HR, hiring managers, and engineering leads on these indicators, and document the training conducted.

- **Incident Planning:** An IT worker incident can trigger a different organizational response than a traditional cyber event. Assess your existing incident response policies to ensure that you have an appropriate plan of action, have identified key decision points, and have thought through any hard decisions in advance.

If You Suspect You've Hired a North Korean IT Worker

If you suspect you have hired a North Korean IT worker, treat it as both a potential sanctions issue and a cybersecurity incident, and be ready for potential law enforcement engagement, in coordination with outside counsel:

- **Sanctions:** Paying a North Korean worker, even unknowingly and unintentionally, can constitute a violation of the North Korea Sanctions Regulations. US sanctions violations are strict liability offenses, although thus far, the Treasury Department's Office of Foreign Assets Control (OFAC) has focused efforts on targeting North Korean operators and facilitators, rather than levying enforcement actions against the companies they duped.

- **Cybersecurity:** Because these workers are often granted authorized network access, treat a suspected case like any intrusion—forensic review of access and data touched, an assessment of notification obligations, and coordination across cybersecurity, legal, and HR. But also keep in mind that the indicators of intrusion may look different, because the worker will be using their own credentials, accessing systems for which they are granted privileges, and (generally) will not be engaged in mass exfiltration of sensitive data.

- **Law Enforcement Engagement:** DOJ and the FBI have signaled through their DPRK RevGen initiative that they want victim companies as partners in these cases, not just sources of evidence. In the first instance, companies should report (although not mandatory) to the FBI (local field

office or IC3). Companies may also consider whether to disclose a potential transaction with North Korean workers to OFAC's enforcement division.

Bottom Line

The multilateral July 31 alert provides a timely reminder to companies that rely on remote tech talent, directly or through staffing vendors, to stress-test hiring, payment, and network-access controls against the now well-established red flags, and to have a response plan that addresses potential sanctions, cybersecurity, and law enforcement coordination considerations. The multidisciplinary nature of these events increases the importance of working with outside counsel to manage the incident and any associated legal obligations.

Related Lawyers

Rachel K. Alpert
Partner
ralpert@jenner.com
+1 202 639 3871

Aaron R. Cooper
Partner
acooper@jenner.com
+1 202 637 6333

Steven J. Arango
Associate
sarango@jenner.com
+1 202 637 6348

Lauren E. Hackett
Associate
lhackett@jenner.com
+1 212 407 1776

Related Capabilities

Data Privacy and Cybersecurity

Investigations, Compliance, and Defense

National Security and Crisis

Stay Informed →