ANDREW R. GARBARINO, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

January 23, 2026

Mr. Ryan Roslansky
Chief Executive Officer
LinkedIn Corporation
1000 W Maude Avenue
Sunnyvale, CA 94085

Dear Mr. Roslansky:

The Subcommittee on Cybersecurity and Infrastructure Protection of the House Committee on Homeland Security is examining a growing national security threat driven by the Democratic People's Republic of Korea's (commonly known as North Korea, hereafter "DPRK") exploitation of modern remote work and digital hiring practices to embed operatives within U.S. companies under false identities.[1] Although this activity is not a recent development and is frequently encountered at the company level as hiring fraud or identity theft, its scale, sophistication, and potential impact have increased significantly. The Kim Jong Un regime has adapted this model into a state-directed strategy to evade sanctions, generate illicit revenue, and obtain unauthorized access to U.S. corporate and technological environments. As a result, this activity now poses serious and direct risks to the security of the homeland.

Public reports,[2] federal law enforcement actions,[3] and private sector investigations[4] have demonstrated that DPRK operatives are using stolen or fabricated identities and artificial intelligence-enabled impersonation tools, including synthetic imagery and voice manipulation technologies, to defeat traditional safeguards and obtain remote employment at American companies.[5] These operatives often deliberately apply for and secure positions in technical, cloud, and security relevant roles, thereby enabling the DPRK government to penetrate internal systems, proprietary data, and operational environments never intended to be exposed to a hostile foreign adversary.[6] These activities have been the subject of sustained investigative attention across the federal government, including by the Department of Justice, the Department of Treasury, and the Intelligence Community.

---

[1] Elmira Aliieva, *North Korean Agents Are Trying to Infiltrate Amazon, Chief Security Officer Says*, NBC NEWS (Dec. 23, 2025).
[2] Robert McMillan & Dustin Volz, *North Korea Infiltrates U.S. Remote Jobs—With the Help of Everyday Americans*, WALL ST. J. (May 27, 2025).
[3] U.S. Dep't of Justice, *Justice Department Announces Nationwide Actions to Combat Illicit North Korean Government Revenue Generation* (Nov. 14, 2025).
[4] Maggie Miller & Dana Nickel, *Tech Companies Have a Big Remote Worker Problem: North Korean Operatives*, POLITICO (May 12, 2025).
[5] Isaac Yee, et al., *Inside North Korea's Effort to Infiltrate U.S. Companies*, CNN (Aug. 5, 2025).
[6] *Id*.

Public U.S. Government advisories and allied assessments make clear that the DPRK's use of remote information technology (IT) workers is a coordinated, state-directed program overseen by senior elements of the Kim Jong Un regime, rather than the actions of independent or criminal actors.[7] These operations are managed through government and Workers' Party of Korea entities responsible for weapons development, military procurement, and illicit revenue generation, including the Party's Munitions Industry Department and its subordinate 313 General Bureau.[8]

These entities deploy and manage overseas IT workers through front companies, foreign intermediaries, and support networks operating primarily from third countries, including within the People's Republic of China and the Russian Federation.[9] DPRK workers are directed to secure remote employment abroad and remit a substantial portion of their earnings back to the regime.[10] U.S. and allied assessments further indicate that this workforce operates alongside, and in certain cases in coordination with, the DPRK's broader intelligence and cyber apparatus, including the Reconnaissance General Bureau, which is responsible for foreign intelligence collection and offensive cyber operations.[11]

The funds generated through these schemes are a known source of hard currency for the DPRK government and support prohibited weapons programs, including ballistic missile and other strategic capabilities.[12] This threat has grown as U.S. companies have increasingly relied on remote work and digital hiring practices. The widespread use of online professional identities, cloud-based business systems, and AI-enabled tools for recruiting, onboarding, and collaboration has created new opportunities for foreign hostile actors to gain access to U.S. companies in ways that were not previously possible.

Your company sits at the center of this threat landscape as one of the world's leading professional networking and digital hiring platforms. Public reports indicate that DPRK operatives have exploited professional networking services, including LinkedIn, to construct and validate false professional identities, establish credibility within U.S. industry networks, and identify and pursue remote employment opportunities under fraudulent pretenses.[13] LinkedIn plays a critical role in the modern hiring lifecycle, from identity representation and professional verification to recruiter outreach and candidate screening. Accordingly, your platform has emerged as a primary vector through which foreign adversaries can scale access to U.S. companies, normalize fabricated personas, and embed operatives into sensitive corporate environments. LinkedIn therefore brings a uniquely consequential perspective on how these DPRK remote IT operations originate, how they propagate across digital labor markets, and how they can be detected and disrupted at the earliest stages.

---

[7] U.S. Dep't of State, Office of the Spokesperson, Multilateral Sanctions Monitoring Team Report on DPRK Violations and Evasions of UN Sanctions Through Cyber and Information Technology Worker Activities (Jan. 12, 2026).
[8] *Id*.
[9] U.S. Dep't of State, U.S. Dep't of the Treasury, & Fed. Bureau of Investigation, *Guidance on the Democratic People's Republic of Korea Information Technology Workers* (May 16, 2022).
[10] *Supra* note 7.
[11] *Supra* note 7.
[12] *Supra* note 7.
[13] *Supra* note 4.

For these reasons, I respectfully request that you designate a senior executive or comparably senior subject matter expert to testify before the Subcommittee at a hearing titled, "*AI, Deepfakes, and Digital Deception: An Examination of North Korea's Use of Remote IT Workers to Infiltrate U.S. Companies, Fund Its Weapons Program, and Threaten the Homeland*." The hearing will take place on Tuesday, February 10, 2026, at 10:00 a.m. in 310 Cannon House Office Building and will examine how these schemes function in practice, how AI has accelerated their scale and effectiveness, and what steps U.S. companies and the federal government, including the Cybersecurity and Infrastructure Security Agency, can take to reduce risk. Please confirm your witness by February 2, 2026.

Per Rule X and XI of the U.S. House of Representatives, the Committee is the principal committee of jurisdiction for overall homeland security policy and has broad authority to oversee "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security." If you have any questions regarding this request, please contact the Committee on Homeland Security Majority staff at (202) 226-8417. Thank you for your prompt attention to this matter.

Sincerely,

_____

ANDY OGLES
Chairman
Subcommittee on Cybersecurity
and Infrastructure Protection

cc: The Honorable Eric Swalwell, Ranking Member
Subcommittee on Cybersecurity and Infrastructure Protection