Your Subcontractor's Engineer Does Not Exist

What a North Korean placement inside a defense contractor costs a company that did nothing wrong — and what converts it from a victim into a respondent.

PUBLISHED	STATUS	REVISED
9 AUGUST 2026	PUBLISHED	9 AUGUST 2026
VERSION	**AUTHOR**	**LICENSE**
1.6	COLLIN B. GEORGE, CISSP	CC BY 4.0

UNCLASSIFIED // OPEN SOURCE

Analytic record

TYPE	Analysis — a structural account of why remote-hiring identity verification fails against a state adversary, and where legal exposure actually attaches. Stable except where the enforcement posture toward host companies changes.
GOVERNING JUDGMENT	Identity verification in remote hiring concentrates on attributes an adversary can falsify at no cost, and is performed once, at onboarding. Where the host holds CUI or export-controlled technical data, a successful placement creates exposure under three regimes at once. But no enforcement action has been brought against an employer arising from an inadvertent placement of this kind; hosts have been treated as victims. For the enforcement posture examined here, the meaningful change in a host company's position occurs after discovery, or after circumstances sufficient to establish knowledge or disregard — not from the fact of having been deceived. Detection capability, not hiring outcome, determines where a company stands.
PROBABILITY	That identity verification weighted toward low-cost-to-falsify attributes fails against a purchased genuine identity is assessed as certain; it follows from the structure of the fraud. That host companies will continue to be characterized as victims absent aggravating conduct is assessed as likely, and rests on an enforcement practice that could change without rulemaking.
ANALYTIC CONFIDENCE	High for the factual record, which rests on Department of Justice charging documents and sentencing announcements and on Treasury designation notices. High for the statement of the applicable legal standards, which rest on published regulatory text. Moderate for the application of those standards to the reported facts, because the public record does not disclose every element. Moderate for the forward-looking assessment of employer exposure, which is an inference from the absence of enforcement rather than from a stated agency position. These are separate axes and are not combined.
REGISTERS	This assessment operates on three levels and marks the transitions between them: what the public record establishes, what the applicable law provides, and what is inferred about enforcement. Inferences are identified as inferences.
SUPERSESSION	Reassess on any enforcement action against a host company, on any OFAC enforcement action against an employer in a services-procurement fact pattern with a DPRK nexus, on any False Claims Act resolution predicated on a fraudulent-placement fact pattern, on new OFAC designations altering the facilitation architecture, or on revision of the NIST SP 800-171 personnel security family.
RESEARCH CUTOFF	Public record surveyed through 9 August 2026. Enforcement in this area is active and the record moves.

REVISION HISTORY	1.6, 9 August 2026 — Mondo TV settlement identified and the adjacent-precedent distinction sourced; secondary corroboration cited. 1.5, 9 August 2026 — § 126.18 scope narrowed to paragraph (a) with (d) and (e) addressed; retention obligation marked as a structural reading; diversion presumption stated as rebuttable; § 126.1(a) carve-outs noted; stale source cross-reference corrected. 1.4, 9 August 2026 — § 126.18(c) corrected to a two-route safe harbour under § 126.18(b); screening scope corrected to all of § 126.1 with the Table 1 presumption distinguished. 1.3, 9 August 2026 — § 126.1(e)(1) scoping clause adopted; § 120.63 causal claim replaced with a descriptive statement; § 126.18(c) audit-right overstatement corrected; strict-liability scope resolved; designation series and Kim Se Un chain added; cutting pass. 1.2, 9 August 2026 — export analysis corrected to § 126.1(e)(2) and the § 120.63 definitional route, with § 126.18 re-scoped to foreign consignees; adjacent enforcement precedent distinguished; secondary-source corroboration disclosed; N.D. Ga. attribution corrected. 1.1, 9 August 2026 — ITAR authority expanded with pinpoint citations; sanctions section rebuilt on three registers; E.O. 13382 proliferation chain added; N.D. Ga. attribution and restitution figures corrected. 1.0, 9 August 2026 — first draft.

Executive summary

— North Korean IT workers obtained employment at more than 100 US companies, including many Fortune 500 firms, using the compromised identities of more than 80 US persons. The scheme ran from approximately 2021 until October 2024 and generated more than $5 million.

— The identity checks did not fail because the adversary was sophisticated. They failed because the adversary bought a real American. The identity on the application was genuine, the address was a facilitator’s residence in the United States, and the company-issued laptop sat at that residence connected to a keyboard-video-mouse switch, so the connection originated from a US residential network because it did.

— One of those placements reached information marked as controlled under the International Traffic in Arms Regulations, at a California defense contractor.

— Victim companies incurred legal fees, network remediation costs, and other damages and losses of at least $3 million while being characterized throughout as victims — money spent by organizations that lost nothing to the fraud itself.

— That characterization is the finding. Neither the Department of Justice nor the Office of Foreign Assets Control has filed an enforcement action against a company that inadvertently hired one of these workers. The hire is not where exposure attaches. Exposure attaches to what a company does once it could have known, which means detection capability rather than hiring outcome determines its position.

IF YOU READ NOTHING ELSE

What to do	Ask whether your organization could detect a placement that has already passed onboarding. Not whether your background checks are adequate — whether anything in your environment would surface a credentialed employee whose device is in one place and whose operator is in another. If nothing would, the control that matters is absent, and the absence is invisible because every check you run returns clean.
Who this affects	Any organization that hires remote technical staff, directly or through a staffing intermediary, and holds CUI, export-controlled technical data, source code, or virtual currency. Cleared facilities and prime contractors with subcontracted development are the acute case.
What being wrong costs	At least $3 million in legal and remediation costs across the victim companies in a single charged scheme, most of which lost nothing to the fraud. Where controlled technical data was reachable, a legal question arises about whether an export occurred and whether it was authorized. And where personnel security controls were attested to under a federal contract, the attestation describes a control that did not do what was represented.

The Record

What follows in this section is what Department of Justice charging documents and announcements state.

From approximately 2021 until October 2024, defendants and co-conspirators compromised the identities of more than 80 US persons to obtain remote jobs at more than 100 US companies, including many Fortune 500 companies, and caused US victim companies to incur legal fees, computer network remediation costs, and other damages and losses of at least $3 million.

Six US-based facilitators, including Kejia Wang and Zhenxing Wang of New Jersey, received at least $696,000 for their services. To deceive US companies into believing the workers were located in the United States, they hosted company-issued laptops at their residences and connected them to keyboard-video-mouse switches enabling remote access from overseas. They created shell companies with corresponding websites and financial accounts — Hopana Tech LLC, Tony WKJ LLC, Independent Lab LLC — to make the workers appear affiliated with legitimate US businesses, and opened accounts to receive payments from victimized companies, much of which was transferred to overseas co-conspirators.

Kejia Wang and Zhenxing Wang were sentenced on 15 April 2026 to 108 months and 92 months respectively, with a combined forfeiture of $600,000, restitution of $29,236.03 ordered against Kejia Wang, and restitution of $200,000 ordered against Zhenxing Wang. Eight co-defendants charged in the

same indictment — Chinese and Taiwanese nationals — remain at large. Those charges are allegations and the defendants are presumed innocent until proven guilty.

The scale extends well past this scheme. The coordinated actions announced on 30 June 2025 included searches of 29 known or suspected laptop farms across 16 states and the seizure of 29 financial accounts used to launder illicit funds. The same release separately reports searches of 21 premises across 14 states between 10 and 17 June 2025, recovering approximately 137 laptops; it does not state the relationship between the two counts. In early June 2025 the Department filed a civil forfeiture complaint for over $7.74 million tied to an illegal employment scheme.

A May 2022 advisory reported that individual North Korean IT workers have been known to earn up to $300,000 annually, generating hundreds of millions of dollars collectively each year on behalf of designated entities including the North Korean Ministry of Defense. Treasury has stated that the DPRK withholds up to 90 percent of overseas workers' wages. (DOJ attributes the advisory to the FBI and the Departments of the Treasury and State; Treasury attributes it to the Departments of State, Treasury, and Justice.)

The Technical Data

Record. IT workers employed under this scheme gained access to sensitive employer data and source code, including ITAR data from a California-based defense contractor that develops artificial-intelligence-powered equipment and technologies. Between approximately 19 January 2024 and 2 April 2024, an overseas co-conspirator remotely accessed without authorization the company's laptop and computer files containing technical data and other information. The stolen data included information marked as being controlled under the ITAR.

The government does not name the contractor and neither does this assessment.

Legal consequence. Under 22 CFR § 120.50(a)(2), an export includes releasing or otherwise transferring technical data to a foreign person in the United States — a deemed export. Under § 120.50(b), such a release is deemed an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency. Release is defined at § 120.56, foreign person at § 120.63, and technical data at § 120.33.

Two provisions in the release definition bear directly on a placement fact pattern and are more on point than the access event itself. Section 120.56(a)(3) provides that release occurs through the use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data. Section 120.56(b) provides that authorization is required to provide access information to a foreign person where that access information can cause or enable access to unencrypted technical data — and § 120.55 defines access information to include decryption keys, network access codes, and passwords.

The consequence is that the regulated act is upstream of the file access. Issuing credentials to a foreign person is itself the conduct the provision addresses. In a placement, that occurs at onboarding.

So: if the accessed information was ITAR technical data and the person accessing it was a foreign person, both the provision of access information and the subsequent release would fall within § 120.50 unless an applicable authorization or exemption applied. The public record establishes that information marked as ITAR-controlled was accessed by an overseas co-conspirator without authorization from the company. It does not establish the classification of every accessed file, the accessing individual's nationality as a matter of proof, or whether any licence or exemption covered the release. Those elements are not resolved here.

Two features of the proscribed-country regime narrow the analysis considerably. North Korea appears in Table 1 to § 126.1(d)(1) under a policy of denial, so on a DPRK nexus the licensing route is close to formally unavailable; § 126.1(a) separately provides that the exemptions in the subchapter do not apply to defense articles for export to proscribed countries or persons, subject to narrow carve-outs at §§ 123.17, 126.6, and 126.18(e). There is also no bona fide employee exemption available for a release to a foreign person inside the United States. That release requires authorization. (Table 1 is also the list § 126.18 keys to for its diversion presumption, a point the subcontract discussion below turns on.)

The domestic dividing line is definitional and binary. Under § 120.63 a foreign person is one who is not a US citizen or national, excluding lawful permanent residents and protected individuals under 8 U.S.C. 1324b(a)(3). A release to anyone on the near side of that line is not an export at all, and no employee-status exemption bridges the two sides — the exemptions turning on employment status, § 126.18 among them, operate on foreign entities abroad.

Which means the operative question in a placement is never whether an exemption was available. It is whether the US-person determination was correct. The same structure governs foreign-national access to controlled nuclear technology: 10 CFR § 810.3 draws the line in nearly identical terms, and a transfer to a foreign national is deemed an export to the country of citizenship or lawful permanent residence whether it occurs in the United States or abroad — the direct analogue of § 120.50(b).

Two regimes, one dividing line, one failure point.

The scoping provision reaches this fact pattern directly. Section 126.1(e)(1) prohibits any sale, export, or transfer of defense articles or services to a proscribed country "or to any person acting on its behalf, whether in the United States or abroad," absent a licence or written approval. A placed DPRK worker is a person acting on North Korea's behalf, in the United States. The prohibition does not require the country-attribution route through § 120.50(b) — though that route reaches the same place, and the two are mutually reinforcing.

Section 126.1(e)(2), titled *Duty to notify*, then provides that any person who knows or has reason to know of a proposed, final, or actual sale, export, transfer, reexport, or retransfer of articles, services, or data as

described in (e)(1) must immediately inform the Directorate of Defense Trade Controls, with notifications submitted to the Office of Defense Trade Controls Compliance.

That is an affirmative duty triggered by knowledge or reason to know. It arises on discovery, not on conclusion of an investigation. It runs to any person with the requisite knowledge, not only to the contracting party.

The consequence is worth stating plainly, because it is the analytic centre of this assessment. The export reporting duty, the sanctions knowledge question, and the False Claims Act scienter standard all key to the same threshold.

> **A company's position under all three regimes changes at the same moment: when it knows, or has reason to know. Not when it hired.**

The encryption provision at § 120.54(c) does not assist here. It provides that the ability to access technical data in encrypted form does not constitute a release, and § 120.54(b)(1)(ii) conditions the end-to-end encryption definition on the means of decryption not being provided to any third party. Here the access was by a credentialed user on a company-issued machine and the data was decrypted for that user by design. Section 120.50(a)(6) separately makes the release of previously encrypted technical data an export in its own right. The provision addresses data secured against the person holding it; it does nothing about a person who has been given the key.

Assessment. The significant point is not that a violation has been adjudicated. It is that the exposure exists in a form no security control reports on. Nothing was breached. Access controls restricting controlled technical data to authorized employees performed exactly as designed. What failed was a determination made once, at hiring — that this person is a US person — which was false from the day it was recorded and which no event in the world would ever correct.

> **WHY THIS MATTERS**
>
> Every compliance determination is true as of a date and against a state of the world that moves without notifying the holder. A US-person determination stored as a static attribute at onboarding is the purest case: nothing will ever tell the system it was wrong.

Why the Identity Checks Passed

The instinct on reading this is that the verification must have been weak. It generally was not. It was ordinary, and ordinary is the problem.

Treasury's own account confirms the mechanism directly. In designating Song Kum Hyok in July 2025, OFAC stated that he used US persons' names, Social Security numbers, and addresses to create aliases for foreign workers seeking employment with US companies. The identity is not fabricated. It is a real American's, used by someone else.

The attributes on which hiring verification concentrates are those a determined counterparty can obtain or falsify at low cost:

- **A legal identity.** Purchased. Real name, real Social Security number, real credit and employment history. The background check passes because the identity is authentic; only the association between the identity and the applicant is false.
- **A US address.** A facilitator's residence. Genuine, verifiable, and in the right country.
- **A device location.** The company-issued laptop physically sits at that address. Network telemetry and IP geolocation report a US residential connection because there is one.
- **A face and a voice.** A US person available for the video interview and onboarding call.

Against those sit attributes expensive to fake and largely unchecked: an operating history independently corroborable through named references reached by channels the applicant did not supply, banking tenure in the applicant's own name, device provenance and behavioral consistency over time, and physical presence verified by means other than an address the applicant provided.

The general principle is that an attribute's value to a screen is not its predictive power but its predictive power discounted by the counterparty's cost of falsifying it. Every attribute in the first list predicts well against the general applicant population, which is why hiring systems rely on them, and every one is available for purchase to a state programme with facilitators willing to take a fee. The result is a verification stack that produces documentation of a check having occurred while providing no evidence against the population it most needs to exclude.

> **An attribute that predicts well and is free to change is a liability rather than an asset.**

It produces accuracy against unsophisticated actors, who never bother to change it, and close to none against those who will — while generating a complete audit trail that the process was followed.

> **WHY THIS MATTERS**
>
> A hiring process built on cheap-to-falsify attributes is not weakly protective against a state adversary. It is non-protective, and it documents its own diligence while being so.

Three Regimes, One Failure

Where the host is a defense contractor, one placement raises questions under three separate bodies of law at once.

Export control. Addressed above, and the exposure most likely to be missed: it does not present as a security incident. A credentialed user opened a file.

Sanctions. Treated below; the analysis is more complicated than it first appears.

Attestation. Where the host operates under a federal contract carrying DFARS 252.204-7012, the NIST SP 800-171 Revision 2 personnel security family was represented as implemented, and an affirmation of continuous compliance was made under 32 CFR 170.22, which runs annually. The exposure is datable: DFARS 252.204-7021 began phasing into solicitations on 10 November 2025, and Phase 2 — under which Level 2 C3PAO certification becomes mandatory for CUI-handling contracts — begins 10 November 2026. A successful placement means the represented control did not do what the representation described. Whether that gap is material, and whether any representation was false when made, are separate questions turning on facts specific to the contractor. No published enforcement matter has yet linked a fraudulent placement to a False Claims Act theory, and nothing here should be read as predicting one.

> **WHY THIS MATTERS**
>
> These are three regimes with three regulators, three limitation periods, and three sets of counsel. A company that treats a discovered placement as an HR and IT incident will address none of them.

The Sanctions Question, Carefully

Record. The facilitation architecture is being mapped rather than sampled. At least six designation actions in fourteen months: 16 January, 8 July, 24 July, and 27 August 2025; 4 November 2025; and 12 March 2026. Three are surveyed here.

On 12 March 2026, OFAC designated six individuals and two entities involved in DPRK IT worker networks, including Amnokgang Technology Development Company and Quangvietdnbg International Services Company Limited under E.O. 13810. Two of the six individuals — Do Phi Khanh and Hoang Van Nguyen — were designated under E.O. 13382, the proliferation authority, for supporting Kim Se Un, whom OFAC identifies as a DPRK nuclear procurement facilitator; OFAC states that Do acts as Kim's proxy in opening bank accounts and laundering proceeds from DPRK IT workers. Kim Se Un was himself designated on 24 July 2025 alongside Korea Sobaeksu Trading Company. The chain is therefore traceable end to end in Treasury's own record: IT-worker proceeds, a laundering proxy, and a designated nuclear procurement facilitator.

On 8 July 2025, OFAC designated Song Kum Hyok under E.O. 13694 as amended by E.O. 14306; Gayk Asatryan and two Russian companies, Asatryan LLC and Fortuna LLC, under E.O. 13722; and Korea Songkwang Trading General Corporation and Korea Saenal Trading Corporation under E.O. 13810.

On 16 January 2025, OFAC designated Department 53 of the Ministry of the People's Armed Forces and Liaoning China Trade Industry Co., Ltd. under E.O. 13687, and Korea Osong Shipping Co., Chonsurim Trading Corporation, Jong In Chol, and Son Kyong Sik under E.O. 13722. Liaoning China Trade supplied notebook and desktop computers, graphics cards, HDMI cables, and network equipment enabling Department 53's overseas IT worker activities.

The July 2025 and March 2026 releases both state expressly that OFAC may impose civil penalties for sanctions violations on a strict-liability basis, and that the prohibitions reach the provision of funds, goods, or services by, to, or for the benefit of a blocked person.

Legal consequence. Strict liability is a statement about the mental element once a violation is established. It is not a statement about what constitutes a violation. The threshold question remains whether a prohibited transaction occurred.

In the typical fact pattern that question is genuinely complicated. The payment of record goes to a US bank account held under a stolen US identity, and the recipient of record is a US person who exists. A violation theory therefore has to be constructed around the ultimate interest of a blocked person or the DPRK government in the funds, and around the onward remittance abroad. It does not follow from the worker's nationality, and it does not follow from the existence of designations elsewhere in the network.

The March 2026 release contains a provision that points the other way on employer exposure and deserves attention. It states that non-US persons are also prohibited from causing or conspiring to cause US persons to wittingly or unwittingly violate US sanctions, as well as from engaging in conduct that evades US sanctions. That is the government describing the US company as the party caused to violate — not as the violator.

Assessment. The operative question for an employer is therefore not whether it unknowingly employed a North Korean. It is: what transaction occurred, who was legally the recipient and who the beneficiary, what property or interest was blocked, and what did the company know or have reason to know at the time. Each of those is answerable with facts a company holds, and none of them is answered by the designation record alone.

> **WHY THIS MATTERS**
>
> A company that reads the designations and concludes it is strictly liable will over-disclose and mismanage its position. A company that reads the absence of employer enforcement and concludes it is safe will under-prepare. Both errors come from skipping the transaction analysis.

What Has Not Happened

Now the part that reframes everything above.

Record. Neither the Department of Justice nor OFAC has filed an enforcement action against a company that inadvertently hired one of these workers. Host companies have been consistently characterized as victims, systematically targeted by a state programme. The public record contains prosecutions of facilitators, indictments of overseas workers, designations of front companies and their financiers, seizures of accounts and domains, and a civil forfeiture action against laundered proceeds. It contains no penalty against an employer.

The adjacent line that has to be addressed. The slate is clean for this fact pattern, and only for this fact pattern. OFAC has settled DPRK-sanctions matters against companies that procured services ultimately performed by North Korean workers. The nearest is Mondo TV S.p.a., an Italian animation company that paid $538,000 in June 2024 to settle 18 apparent violations of the North Korea Sanctions Regulations, having remitted approximately $537,939 between May 2019 and November 2021 to Scientific Educational Korea Studio, a Government of North Korea-owned firm. A reader will raise it.

It does not transfer, and the reason is the transaction analysis this assessment has already insisted on. In Mondo the contracting counterparty was itself a Government of North Korea-owned entity; the relationship dated to the 1990s and senior management communicated with its representatives directly. The prohibited transaction was identifiable from the commercial relationship because the counterparty's DPRK character was a fact about the contract rather than a fact concealed from it. OFAC's theory was that Mondo caused US financial institutions to process wire transfers containing blocked property interests and to export financial services to North Korea.

In a placement, the counterparty of record is a US person who exists, whose identity was stolen, and whose payment lands in a US account. Those are different transactions, and the elements are established differently.

One feature of Mondo does carry across, and it cuts toward the reading advanced here: OFAC reached a non-US person for causing US financial institutions to violate. That is the same structural move as the March 2026 language about non-US persons causing US persons to violate wittingly or unwittingly — the party characterized as caused, in both instances, is the one downstream of the concealment.

The distinction is real but it is narrow, and it is the boundary of the clean slate. A company that contracts with an offshore development shop and never establishes who is behind it is closer to the settled matters than to the placement cases, whatever it believes about its exposure.

Assessment. This is an inference from published enforcement, not a stated agency policy, and it is stated as such. But the consistency is notable: it holds across every action in the DPRK RevGen sequence and across two administrations. Read together with the March 2026 language about non-US persons causing US persons to unwittingly violate sanctions, the posture appears deliberate rather than incidental. It is also, as noted, a conclusion reached independently by practitioners with visibility into non-public matters this assessment does not have.

> **What follows is not that employers are safe. It is that the hire is not where exposure lives.**

Which raises the question this assessment exists to answer.

What Converts a Victim Into a Respondent

Three transitions are visible in the record and in the agencies' stated expectations.

Detection followed by continued payment. A company that identifies a suspect placement and keeps paying has made a decision with knowledge. Everything protective in the victim characterization depends on the absence of that knowledge, and it is available exactly once.

A programme the government declines to credit. Both agencies have signalled that they expect vigilance against workers attempting to circumvent US law. Where controls are deficient enough that a placement was not merely undetected but undetectable, and where the company can produce no evidence of having looked, the victim characterization becomes a question rather than an assumption.

Third-party reporting that arrives first. Financial institutions file. When a bank's screening surfaces the payment pattern, the resulting inquiry opens with the government already informed and the company reactive. Whether the company had found the placement first is the first fact established. Bank filings are not the only channel: the March 2026 Treasury release flags the FinCEN whistleblower programme, under which awards are available where information leads to penalties exceeding $1,000,000. That creates a monetary incentive for insiders and counterparties to report, and it is likely to be faster than institutional screening.

The underlying logic generalizes. Where liability turns on a standard reaching deliberate ignorance and reckless disregard, declining to look is not protective. Measuring and acting converts the measurement into evidence of diligence. Measuring and doing nothing creates the adverse record. Not measuring leaves the exposure intact while forfeiting the diligence position entirely. Non-measurement is the dominated option, and the calculation does not change because the subject is a hiring process rather than a control set.

> **WHY THIS MATTERS**
>
> The company that finds a placement in its own environment, acts, and discloses is in a materially different position from the one that learns of it from a subpoena. The difference is not the placement. It is the sequence.

What the Verification Stack Has to Do

Four changes, all using information the organization already holds or can obtain without new tooling.

Weight verification by cost to falsify. Retain the identity and background checks; they exclude the unsophisticated. Add at least one attribute the counterparty cannot purchase — independently sourced employment references reached through channels the applicant did not supply, banking tenure in the applicant's own name, or verified physical presence established by means other than a submitted address.

Re-verify. A verification performed once at onboarding is a determination stored as a static attribute, and it will become false without notifying anyone. Re-verification on a schedule and on behavioral triggers — device relocation, access-pattern change, hours inconsistent with a stated timezone, requests to redirect equipment or payment — converts a one-time check into a control.

Detect the topology, not the person. The distinguishing physical fact in every one of these placements is that the operator and the device are in different places. A KVM switch between a company laptop and a remote operator is detectable. So is a residential address hosting laptops issued by multiple unrelated companies, a device that never moves, and a session pattern inconsistent with a human at the keyboard in the stated location. This is the one control that addresses the failure directly, because it tests a fact the adversary cannot purchase away.

Flow it into the subcontract as a term. Where technical staff arrive through a staffing intermediary, the verification requirement belongs in the agreement as an obligation with an audit right and a remedy, not as a representation collected once at onboarding. A representation transfers no risk and produces no evidence.

Where the intermediary is a foreign entity — an authorized end-user, consignee, or sub-licensee operating abroad under a licence or agreement — this is not merely prudent contracting. The binding condition at § 126.18(b) is that the entity maintain effective procedures to prevent diversion. Section 126.18(c) supplies two routes to satisfying it: host-nation security clearances for the employees, or a technology security and clearance plan that includes screening employees for substantive contacts with restricted or prohibited countries listed in § 126.1, together with an executed non-disclosure agreement. The five-year record retention and the duty to produce screening records to DDTC are stated in unqualified terms, but on the structure of the paragraph those obligations sit within the second route; a conservative reading, and DDTC practice, may treat the plan as expected of anyone relying on the exemption. Separately, an employee with substantive contacts with persons from a Table 1 to § 126.1(d)(1) country is presumed to raise a risk of diversion unless DDTC determines otherwise.

Two consequences follow. The counterparty's diversion-prevention obligation is regulatory rather than contractual, so it is not something a US prime has to negotiate into existence. But which route the counterparty uses determines what records exist at all — and that is itself the diligence question, because a counterparty relying on host-nation clearances will have no screening file to produce. Note the limit in either case: § 126.18(c) requires production to DDTC, not to a US prime. An audit right against the counterparty comes from the contract you negotiate, not from the ITAR. Section 120.64 defines the regular employee whose status the exemption turns on, including the conditions under which a staffing-agency secondee qualifies.

The scope matters and is narrow. Section 126.18(a) governs transfers to or within a foreign end-user or consignee, taking place within the territory where that entity is located, and only within the scope of an approved licence, other export authorization, or licence exemption. It has no application to a US company using a US staffing agency, which is the fact pattern in the charged conduct above.

Two other paragraphs do reach individuals physically in the United States, and both are closed here on their own terms. Paragraph (d) covers reexports to dual- and third-country-national employees of a foreign authorized end-user or consignee who may be in the United States during the reexport, but requires exclusive nationality of NATO, the EU, Australia, Japan, New Zealand, or Switzerland — so it cannot reach a DPRK nexus. Paragraph (e) likewise covers Australian and UK citizens and is AUKUS-

specific. It is also the only § 126.18 route § 126.1(a) preserves for proscribed destinations, which is why the door closes twice rather than once.

> **WHY THIS MATTERS**
>
> Every one of these is implementable with data the organization already generates. What is missing is not capability. It is the decision to check for a failure mode no existing control reports on.

Three Questions That Settle It for Your Organization

None requires counsel to answer, though the answers may send you to counsel.

One. Could we detect a placement that has already passed onboarding? Not whether our screening is adequate — whether anything in the environment would surface a credentialed employee whose operator is not where the device is. If the honest answer is no, the exposure is undetectable rather than absent, and every check will continue to return clean.

Two. What would we do in the first forty-eight hours? Who decides. Who is notified. Whether access is cut before or after evidence is preserved. Whether export counsel and sanctions counsel are called, or only employment counsel. And the item most organizations have not considered: § 126.1(e)(2) imposes a duty to inform DDTC immediately on knowing or having reason to know, with notification to the Office of Defense Trade Controls Compliance. That clock starts on reason to know, not on the conclusion of the internal investigation, and a company that sequences its response around finishing the investigation first may have run it. The duty runs to any person with the knowledge, which is worth establishing before the event rather than during it. Deciding this during the event means making the choices that determine your posture under time pressure and without advice.

Three. If controlled technical data was reachable by that account, what is the disclosure question? Whether a release occurred, whether it was authorized, and whether disclosure is required are legal determinations that belong with export counsel immediately — not after the internal investigation concludes.

If those answers are clear and consistent, the organization can defend its posture. If any is unresolved, that is the finding, and it is better identified now than in the forty-eight hours after a placement surfaces.

When This Stops Being a Design Question

Whether a particular access constituted an unauthorized export, whether a particular payment involved blocked property or a blocked person’s interest, whether a representation made in a federal contract was accurate when made, and whether any of it must be disclosed are legal determinations. The last belongs with counsel immediately.

What is a design question, and what this assessment addresses, is whether an organization can detect a placement that has already defeated its hiring controls, and what its position is if it cannot. That question has an answer, and the answer is not more thorough background checks.

This assessment is not legal advice and is not a substitute for counsel.

LIMITATIONS

What this assessment does not establish

This assessment describes a structural failure in remote-hiring verification and the legal questions that follow from it. It does not determine whether any particular organization is deficient, whether any particular access constituted a violation, whether any particular payment was prohibited, or how any specific matter would be resolved.

The export analysis states what the regulation provides and identifies the elements on which the conclusion depends. The public record does not establish every element, and this assessment does not resolve them by inference.

The sanctions analysis identifies where the legal uncertainty lies rather than resolving it. The strict-liability standard stated in OFAC's releases addresses the mental element once a violation is established; it does not establish that an unknowing employer has committed one.

The finding that no enforcement action has been brought against an inadvertent host company rests on the published record. Non-public inquiries, declinations, and matters resolved without announcement cannot be excluded, and the absence of published enforcement is evidence rather than proof.

The assessment that host companies will continue to be treated as victims is an inference from enforcement practice, not from a stated agency policy. It could change without notice and without rulemaking.

No published enforcement matter has yet linked a fraudulent placement to a False Claims Act theory. The argument is that the elements are present in a fact pattern of this shape, not that such a case has been brought.

Charges described as indictments are allegations, and those defendants are presumed innocent until proven guilty. Sentences, forfeitures, and restitution described are as reported in Department of Justice announcements.

An assessment that cannot state what would change it should not be published. This one would change on any enforcement action against a host company, on an agency statement that the hire itself creates exposure, on a False Claims Act resolution predicated on this fact pattern, or on a demonstrated verification method that defeats a purchased genuine identity at onboarding.

RELATED ACTIONS

A parallel matter in the Northern District of Georgia

A separate indictment unsealed in the Northern District of Georgia on 30 June 2025 charges four North Korean nationals who travelled to the United Arab Emirates on North Korean travel documents and worked as a co-located team. Kim Kwang Jin and Jong Pong Ju obtained employment — at a blockchain research and development company headquartered in Atlanta and a virtual token company based in Serbia respectively — by providing false identification documents containing a mix of stolen and fraudulent identity information. Once trusted, they were assigned projects giving them access to virtual currency assets, and stole virtual currency valued at over $900,000: approximately $175,000 in February 2022, and approximately $740,000 in March 2022, the latter obtained by modifying the source code of two of the employer's smart contracts. Chang Nam Il was subsequently hired by the Serbian company under the alias "Peter Xiao" on Jong Pong Ju's recommendation. Kang Tae Bok is alleged to have held laundering accounts opened with fraudulent Malaysian identification. The indictment states that neither company would have hired Kim Kwang Jin and Jong Pong Ju had it known they were North Korean citizens. Those charges are allegations; the defendants remain at large.

The matter is included for two reasons. That last statement is the clearest articulation in the record of what the deception was for: not access to a job, but access to assets, obtained by concealing the single fact that would have prevented the hire. And the source-code modification is the sharper illustration of what a placement actually buys — not an insider who steals, but an insider with commit access who alters production contracts.

SOURCES

Primary sources

Assertions about the charged conduct trace to Department of Justice charging documents and announcements and to Treasury designation notices; legal statements trace to published regulatory text and to the executive orders named. One finding — the absence of enforcement against inadvertent host companies — is a negative finding and rests in part on secondary practitioner commentary, identified at source 15 and explained in the method note. Where the public record does not settle a question, the text says so rather than resolving it by inference.

1. U.S. Department of Justice, *Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes* (30 June 2025), Press Release 25-680; five-count indictment in *United States v. Zhenxing Wang et al.* (D. Mass.); information in *United States v. Kejia Wang* (D. Mass.).

2. U.S. Department of Justice, *Two U.S. Nationals Sentenced for Facilitating Fraudulent Remote Information Technology Worker Scheme that Generated $5M in Revenue for the Democratic People's Republic of Korea* (15 April 2026).

3. Indictment, *United States v. Kim Kwang Jin, Kang Tae Bok, Jong Pong Ju, and Chang Nam Il* (N.D. Ga.), unsealed 30 June 2025.

4. U.S. Department of the Treasury, *Treasury Sanctions Facilitators of DPRK IT Worker Fraud Targeting U.S. Businesses* (12 March 2026), and corresponding SDN List entries. Designations under E.O. 13810 and E.O. 13382.

5. U.S. Department of the Treasury, *Sanctions Imposed on DPRK IT Workers Generating Revenue for the Kim Regime* (8 July 2025), and corresponding SDN List entries. Designations under E.O. 13694 as amended by E.O. 14306, E.O. 13722, and E.O. 13810.

6. U.S. Department of the Treasury, *Treasury Targets IT Worker Network Generating Revenue for DPRK Weapons Programs* (16 January 2025), and corresponding SDN List entries. Designations under E.O. 13687 and E.O. 13722.

7. Federal Bureau of Investigation, Internet Crime Complaint Center, Public Service Announcements of May 2024 and January 2025 concerning DPRK remote IT worker schemes.

8. FBI, Department of the Treasury, and Department of State, joint advisory of May 2022 concerning DPRK IT workers.

9. 22 CFR part 120 definitions: § 120.50(a)(2) (deemed export by release to a foreign person in the United States); § 120.50(a)(6) (release of previously encrypted technical data); § 120.50(b) (country attribution); § 120.33 (technical data); § 120.54(b)(1)(ii) and § 120.54(c) (end-to-end encryption; ability to access encrypted technical data not a release); § 120.55 (access information); § 120.56(a)(3) and § 120.56(b) (release through use of access information; authorization required to provide access information); § 120.63 (foreign person); § 120.64 (regular employee).

10. 22 CFR § 126.1: § 126.1(a) (exemptions unavailable for proscribed destinations); Table 1 to § 126.1(d)(1) (North Korea, policy of denial); § 126.1(e)(1) (prohibition reaching persons acting on behalf of a proscribed country, whether in the United States or abroad); § 126.1(e)(2) (duty to notify DDTC).

11. 22 CFR § 126.18: § 126.18(a) (transfers to or within a foreign end-user or consignee, within territory and within the scope of an authorization); § 126.18(b) (effective procedures to prevent diversion); § 126.18(c)(1)–(2) (host-nation clearance route; screening and NDA route, with five-year retention and production to DDTC, and the rebuttable Table 1 diversion presumption); § 126.18(d) (reexports to dual- and third-country nationals of specified nationalities); § 126.18(e) (Australian and UK citizens). Provision amended 30 December 2025; cite the current text.

12. 10 CFR § 810.3 (foreign national), cross-referenced for the parallel definitional structure.

13. NIST SP 800-171 Revision 2, personnel security family; DFARS 252.204-7012; DFARS 252.204-7021 (Federal Register final rule, 10 September 2025, for the phase dates); 32 CFR 170.22.

14. George, Collin B., *The Export Rule Controls Your Data. It Never Tells You How to Protect It.* Assessment SB-2026-02, Sanctir LLC, 30 July 2026.

15. Secondary. Skadden, Arps, Slate, Meagher & Flom LLP, *North Korean Remote IT Worker Fraud: Managing Insider Threat, Sanctions and Employment Risk* (8 June 2026), `https://www.skadden.com/insights/publications/2026/06/north-korean-remote-it`. See also Crowell & Moring LLP, *From Deepfakes to Sanctions Violations: The Rise of North Korean Remote IT Worker Schemes* (22 September 2025). Cited for corroboration of the negative finding at "What Has Not Happened," as described in the method note.

16. U.S. Department of the Treasury, Office of Foreign Assets Control, Enforcement Release, *Mondo TV, S.p.a. Settles with OFAC for $538,000 for Apparent Violations of the North Korea Sanctions Regulations* (26 June 2024).

17. U.S. Department of the Treasury, designation of Kim Se Un and Korea Sobaeksu Trading Company (24 July 2025).

SUGGESTED CITATION

George, Collin B. *Your Subcontractor's Engineer Does Not Exist: What a North Korean Placement Costs a Company That Did Nothing Wrong.* Assessment SB-2026-04, version 1.6. Sanctir LLC, 9 August 2026.

METHOD

Method note

This assessment is independent open-source analysis. It operates on three registers, marked in the text: what the public record establishes, what the applicable law provides, and what is inferred about enforcement practice.

Factual findings about the charged conduct trace to Department of Justice charging documents and announcements and to Treasury designation notices. Legal statements trace to the ITAR provisions cited, the NIST and DFARS provisions cited, and the executive orders named.

The observation that no enforcement action has been brought against an inadvertent host company is a negative finding, and negative findings cannot be established from primary sources alone. It was identified through secondary practitioner commentary and then checked against the published enforcement record. Practitioner analyses published in 2026 reach the same conclusion in similar terms, including the characterization of host companies as victims systematically targeted and the observation that both agencies expect vigilance. That convergence is noted as corroboration rather than as independent derivation, and it is part of why the forward-looking confidence in this assessment is rated moderate rather than high.

Where the public record does not settle a question — including whether non-public inquiries into host companies exist, and whether the victim characterization reflects policy or circumstance — that is stated rather than resolved by inference.

Sanctir is a solo practice; this work was subjected to adversarial self-review, not external peer review.

AUTHOR

About the author

Collin B. George, CISSP, is the principal of Sanctir LLC, an independent research and advisory practice working on CMMC and NIST SP 800-171, export controls, sanctions, and defense industrial base risk.

Sanctir is a solo practice. This assessment was subjected to adversarial self-review rather than external peer review, and is not affiliated with any government agency, academic institution, or defense contractor.

ORCID 0009-0007-8162-6839 · Full background · Contact