Introduction

Kaerus Consulting LLC has observed many supplier and vendor issues which affect compliance with National Security Agreements (NSAs). We decided to research the underlying issue thoroughly, examine existing work on the problem by members of the CFIUS Bar, and provide recommendations for practitioners, CFIUS Monitoring Agencies (CMAs), and the Committee itself.

I. The Privity Gap: Vendor Obligations Under the NSA Framework

Section 721 of the Defense Production Act authorizes CFIUS to "negotiate, enter into or impose, and enforce any agreement or condition with any party to the covered transaction" to mitigate national security risks.[1] The statute's operative phrase is precise: *any party to the covered transaction.* Vendors, suppliers, and other third parties in the transaction parties' supply chains are not parties to the covered transaction and therefore cannot be bound directly by an NSA.[2]

This is a limitation rooted in privity, not in the absence of government concern about vendors. The distinction matters for practitioners because it determines where enforcement authority resides and where it does not. Three tiers of government reach over vendor conduct should be distinguished:

(i) Direct binding. A vendor is not an NSA signatory and bears no direct legal obligation under the agreement. CMAs cannot compel a vendor's compliance, impose penalties on a vendor for noncompliance, or subject a vendor to CMA site visits under the NSA's authority. Treasury and DoD descriptions of mitigation authority consistently frame monitoring as directed at "the Transaction

[1] 50 U.S.C. § 4565(l)(3)(A)(ii) (authorizing the President or CFIUS to "negotiate, enter into or impose, and enforce any agreement or condition with any party to the covered transaction" to mitigate national security risks).

[2] An example is the Momentus Inc. National Security Agreement (June 9, 2021), available at https://www.sec.gov/Archives/edgar/data/1781162/000121390021037338/fs42021a5ex10-17_stableroad.htm (defining "Transaction Parties" as the entities to the covered transaction and the U.S. Government signatories, with no reference to downstream vendors or suppliers).

Parties' compliance."[34] The government's enforcement power runs to the transaction parties, not through them to third parties.

(ii) Indirect leverage through procurement controls. CFIUS routinely imposes robust, verifiable obligations on transaction parties that constrain vendor selection and conduct. Published examples include requirements to use "only authorized vendors," tighten procurement and supply chain procedures, and obtain CMA approval before engaging specified categories of suppliers.[56] Transaction parties can be required to incorporate flow-down clauses in vendor contracts, demand software and hardware bills of materials, and retain rights to require vendor substitution upon CMA direction. These measures are enforceable against the transaction party—including through the penalty authority CFIUS has repeatedly demonstrated willingness to use,[7] but their effectiveness depends on the transaction party's commercial leverage over the vendor and its capacity to detect vendor-level risks.

(iii) Parallel authorities that reach vendors directly. The Commerce Department's ICTS rule, implementing Executive Order 13873 and codified at 15 C.F.R. Part 791, authorizes the Secretary of Commerce to prohibit or impose mitigation measures on any ICTS transaction involving persons owned by, controlled by, or subject to the jurisdiction of a foreign adversary.[8] Critically, the ICTS rule's enforcement reach extends to "both direct participants in ICTS transactions and nonparties—such as

[3]U.S. Department of the Treasury, "CFIUS Mitigation," available at https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-mitigation (describing mitigation authority as directed at "transaction parties" and monitoring by designated CMAs).

[4]U.S. Department of Defense, DCSA, "Committee on Foreign Investment in United States (CFIUS)," available at https://www.businessdefense.gov/ibr/gies/cfius/index.html.

[5]Torres Trade Law, "When CFIUS Mitigation Agreements and FOCI Reviews Overlap: A Critical Balancing Act," available at https://www.torrestradelaw.com (listing mitigation measures including "ensuring that only authorized vendors supply certain products or services" and "tightening procurement or supply chain procedures").

[6]Phoenix Strategy Group, "CFIUS Mitigation Agreements: Key Terms Explained" (describing requirements for transaction parties to "assess potential changes required for suppliers, vendors, or customers" and to "compile comprehensive data on customer and vendor relationships").

[7]Morgan Lewis, "CFIUS Annual Report for 2024" (Sept. 2025) (noting the $60 million penalty, the largest in CFIUS history).

[8]Exec. Order 13873, "Securing the Information and Communications Technology and Services Supply Chain" (May 15, 2019); 15 C.F.R. Part 791 (final rule effective Feb. 4, 2025). The ICTS rule authorizes the Secretary of Commerce to prohibit or impose mitigation measures on "any ICTS Transaction subject to United States jurisdiction" involving persons "owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." This authority reaches manufacturers, suppliers, and service providers directly—regardless of whether they are parties to any CFIUS-reviewed investment transaction.

subcontractors or intermediaries—who knowingly assist in violations."[9] Where the NSA stops at the transaction-party boundary, the ICTS rule can reach the vendor directly.

The practical consequence is not that CFIUS lacks tools to address vendor risk, but that the tool it uses most frequently—the NSA—operates through contractual privity with the transaction parties rather than direct regulatory authority over the vendor. The burden of monitoring, enforcing, and bearing penalties for vendor-level failures falls on the transaction parties, regardless of whether the underlying risk originates in the vendor's product design, firmware practices, or component sourcing.

II. Supply Chain Integrity in CFIUS Review

CFIUS increasingly treats supply chain integrity as a central review factor. When assessing vulnerabilities, the Committee evaluates the supply chain of the U.S. business and the identities and relationships of its business partners.[10] Executive Order 14083 further directed CFIUS to weigh the effects of transactions on the resilience of U.S. critical supply chains.[11]

This creates a paradox. CFIUS may require that a transaction party use only "authorized vendors" or "tighten procurement or supply chain procedures."[12] But the vendors themselves remain unbound. The transaction party must enforce compliance through its own contractual relationships—a form of private-sector enforcement that relies on commercial leverage rather than government authority.

The CFIUS enforcement apparatus is substantial. As of year-end 2024, the Committee oversaw 242 active mitigation agreements.[13] Monitoring agencies conducted 79 compliance site visits, nearly double

[9]Morgan Lewis, "Securing the ICTS Supply Chain: Commerce Issues Final Rules Pursuant to EO 13873" (Dec. 11, 2024) (noting the final rule "applies to types of ICTS transactions most affecting US national security" and that "penalties apply to both direct participants in ICTS transactions and nonparties—such as subcontractors or intermediaries—who knowingly assist in violations").

[10]Cooley LLP, "CFIUS Overview," available at https://www.cooley.com/services/practice/cfius/cfius-overview (listing CFIUS factors including supply chain integrity and business partner identities).

[11]Exec. Order 14083, "Ensuring Robust Consideration of Evolving National Security Risks by CFIUS" (Sept. 15, 2022), 87 Fed. Reg. 57369.

[12] Torres Trade Law, *op. cit*.

[13]CFIUS Annual Report to Congress for Calendar Year 2024 (Aug. 2025), available at https://home.treasury.gov/system/files/206/2024-CFIUS-Annual-Report.pdf.

the 43 visits in 2023.[14] The Committee assessed its largest penalty ever, $60 million, along with four additional penalties for material breaches.[15] The percentage of notices cleared with mitigation dropped to approximately 9%, down from 21% in 2023.[16] A November 2024 final rule expanded CFIUS's information-gathering, penalty, and mitigation-negotiation authorities.[17] Yet all of this enforcement activity is directed at transaction parties. The government's ability to audit, sanction, or penalize a vendor under the NSA is mediated entirely through the transaction party's compliance obligations.

Third-party compliance firms describe their work as encompassing risk assessments of "operations, subsidiaries, supply chain, corporate security policies"[18] and audits that include "ensuring supply chain integrity."[19] But these assessments evaluate whether a *transaction party* has discharged its obligations—not whether vendors have independently met national security standards.

III. The Solar Industry: A Case Study in Vendor-Level Risk

A. The Investment Nexus and Critical Infrastructure Function

The solar sector presents a clear causal chain from investment transaction to critical infrastructure risk. When CFIUS reviews an acquisition involving a U.S. solar energy company—whether a developer, independent power producer, or grid-services operator—the critical infrastructure function at issue is the generation and delivery of electricity to the U.S. grid. The investment nexus arises because changes in ownership or control may alter sourcing decisions, vendor relationships, access to operational technology, or governance over equipment deployment.

[14]Latham & Watkins LLP, "6 Key Takeaways From the 2024 CFIUS Annual Report" (Aug. 2025) (noting 242 active mitigation agreements and 79 site visits in 2024, up from 43 in 2023).

[15] Morgan Lewis, *op. cit*.

[16]White & Case LLP, "CFIUS 2024 Annual Report Key Takeaways" (Aug. 2025) (reporting that approximately 9% of notices were cleared with mitigation in 2024, down from 21% in 2023).

[17]Fed. Reg., 89 FR 93179 (Nov. 26, 2024) (CFIUS final rule expanding penalty provisions, information-gathering authority, and mitigation negotiation procedures; amending 31 C.F.R. Parts 800 and 802, effective Dec. 26, 2024).

[18]For example, EisnerAmper, "National Security Advisory & CFIUS Services" (describing supply chain risk assessments as encompassing "operations, subsidiaries, supply chain, corporate security policies").

[19]K2 Integrity, "National Security and CFIUS Services" (describing audits including "ensuring supply chain integrity" as part of third-party monitoring).

Vendor-origin risk manifests as a consequence of the transaction in several ways. A new foreign owner may shift procurement toward affiliated or state-linked suppliers. Even absent affirmative changes, the transaction may bring under CFIUS's purview a U.S. business whose existing vendor relationships already present unmitigated national security concerns—inverters with undisclosed capabilities, firmware under foreign-vendor control, or supply chain concentration that limits substitution options. The NSA is the instrument for addressing these risks, but the risks themselves reside in the vendor's products.

B. Market Concentration: Shipments Data

According to Wood Mackenzie's market-share tracking, global solar photovoltaic (PV) inverter shipments reached 536 Gigawatts of Alternating Current (GW(AC)) in 2023 and 589 GW(AC) in 2024.[2021] In both years, Chinese manufacturers Huawei and Sungrow ranked first and second by shipment volume. In 2023, the two firms combined for more than 50% of the global market—measured by GW(AC) shipped, not installed base—driven largely by their utility-scale offerings. By 2024, their combined share rose to approximately 55%, with Huawei shipping 176 GW(AC) and Sungrow 148 GW(AC). Nine of the top ten global inverter suppliers by shipment volume were headquartered in China.

Chinese firms' dominance extends beyond inverters. The Coalition for a Prosperous America reported in May 2025 that Chinese companies control over 80% of the *broader* global solar supply chain—encompassing polysilicon, wafers, cells, and modules—and dominate U.S.-based production and deployment.[22] These figures should be understood in context: shipment data reflects annual flows, not the cumulative installed base, which includes equipment deployed over many prior years from diverse sources. Nevertheless, the trend lines indicate deepening concentration in Chinese-headquartered firms.

---

[20]Wood Mackenzie, "Global Solar Inverter and Module-Level Power Electronics Market Share 2024" (Aug. 2024) (reporting that Huawei and Sungrow "captured more than 50% of the global market" by shipment volume in GW(AC) in 2023, "largely through the popularity of their utility-scale inverters"). Nine of the top ten inverter suppliers by shipments were headquartered in China.

[21]Wood Mackenzie, "Global PV Inverter Shipments Grew by 10% in 2024 to 589 GWac" (July 2025) (reporting that Huawei and Sungrow combined for 55% of the global inverter market by shipment volume in 2024, with Huawei shipping 176 GW(AC) and Sungrow 148 GW(AC)). These figures measure annual shipments, not installed base; the installed base reflects cumulative deployments over many years.

[22]Coalition for a Prosperous America, "Distrust Grows" (May 22, 2025) (stating that "subsidized Chinese firms control over 80% of the global solar supply chain and dominate U.S.-based production as well as deployment"). The 80% figure refers to the broader supply chain including polysilicon, wafers, cells, and modules—not inverters specifically.

C. Reported Undocumented Communication Devices

In May 2025, Reuters reported—citing two anonymous U.S. energy officials—that undocumented communication devices, including cellular radios, had been discovered in Chinese-manufactured solar inverters and batteries deployed in the United States.[23] Reuters stated that U.S. experts who "strip down equipment hooked up to grids to check for security issues" found these components, but that Reuters was "unable to determine how many solar power inverters and batteries they have looked at.".[24] The identities of the affected manufacturers were not disclosed.

The U.S. Department of Energy acknowledged the concern: "While this functionality may not have malicious intent, it is critical for those procuring to have a full understanding of the capabilities of the products received."[25] Security experts told Reuters that the devices "provide additional, undocumented communication channels that could allow firewalls to be circumvented remotely," and warned of the potential to destabilize grids. A SolarPower Europe cybersecurity report modeled that compromising only 3 GW of inverter-linked generation capacity could significantly impact Europe's grid stability.[26]

Separately, a Forescout Research study in March 2025 identified nearly 50 software vulnerabilities across inverters from vendors Sungrow, SMA, and Growatt, with 80% classified as high or critical severity.[27] While software vulnerabilities are distinct from undocumented hardware components, both categories illustrate the breadth of vendor-originated risk in networked energy infrastructure.

D. The November 2024 Deye Remote-Disabling Incident

[23]Reuters, "Ghost in the Machine: Rogue Communication Devices Found in Chinese Inverters" (May 14, 2025) (citing two anonymous U.S. energy officials; Reuters reported it was "unable to determine how many solar power inverters and batteries they have looked at"; the identities of affected manufacturers were not disclosed).

[24]PV Magazine, "Hidden Devices Found in Chinese-Made Inverters in the US, Reports Reuters" (May 14, 2025) (noting that "Reuters cites two unnamed sources, who would only provide a few details" and that "the number of devices investigated was also not disclosed").

[25]Utility Dive, "'Rogue' Communication Devices Found on Chinese-Made Solar Power Inverters" (May 15, 2025) (reporting that the undisclosed devices "could allow firewalls to be circumvented remotely" according to anonymous sources; confirmed that the DOE acknowledged the discovery).

[26]SolarPower Europe & DNV, Cybersecurity Report (Apr. 2025) (modeling that compromise of approximately 3 GW of inverter-linked generation capacity could significantly impact Europe's grid stability).

[27]Forescout Research, Vedere Labs, "SUN:DOWN" (Mar. 2025) (identifying nearly 50 vulnerabilities across Sungrow, SMA, and Growatt inverters, with 80% classified as high or critical severity on the CVSS scale).

On November 15, 2024, Chinese inverter manufacturer Zhejiang Deye Technology remotely deactivated a significant number of its branded inverters in the United States.[28] The incident arose from a commercial dispute: Deye's U.S. distribution partner, Sol-Ark, held exclusive distribution rights, and Deye-branded units had been sold through unauthorized channels. Deye's cloud infrastructure enabled it to push a deactivation command to inverters connected to its platform, rendering them inoperable.

The affected systems were residential, behind-the-meter installations acquired through gray-market channels; no grid-scale disruption was reported. Deye later characterized the lockout as an automated authorization-verification mechanism rather than a deliberate remote-control action, though affected users reported total loss of system functionality. Whether commercial or strategic in origin, the incident demonstrated a concrete capability: a foreign vendor's cloud infrastructure can remotely disable energy equipment deployed in the United States without the knowledge or consent of the equipment operator.

E. Legislative and Policy Responses

In November 2025, more than fifty members of the Republican Study Committee demanded that the Commerce Department restrict future imports of Chinese inverter equipment used in critical infrastructure.[29] Lithuania enacted legislation restricting remote control of energy installations by states classified as unfriendly, and the United Kingdom initiated a review of Chinese technology in its energy sector.[30]

CFIUS has acted in the energy sector directly. In one case, the Committee ordered a technology company with Chinese R&D ties to divest its stake in a Hawaiian solar energy storage supplier.[31] In the Nippon Steel–U.S. Steel transaction, mitigation included a "Golden Share" granting the U.S. Government consent rights over strategic decisions.[32] These actions demonstrate willingness to address ownership-

[28]Solarboi.com, "Sol-Ark Manufacturer Reportedly Disables All Deye Inverters in the US" (Nov. 17, 2024); FYIVT, "The November 2024 Inverter Shutdown Was Real—and It Came from China" (May 20, 2025) (confirming that Chinese manufacturer Deye remotely deactivated its inverters in the U.S. on November 15, 2024, in connection with an exclusive distribution dispute with Sol-Ark; the event affected residential behind-the-meter systems acquired through unauthorized channels and did not cause grid-scale disruption).

[29]Republican Study Committee, "RSC Calls Out Chinese Solar Inverters as Security Risk" (Nov. 2025) (letter signed by more than fifty members requesting Commerce Department action).

[30]American Security Project, "China's Unseen Cyber Threat to Energy Security" (June 2025).

[31]Global Competition Review, "CFIUS Orders Business with China Ties to Divest Control Over US Energy Company."

[32]O'Melveny & Myers LLP, "A New Paradigm for CFIUS" (2025) (describing the Nippon Steel–U.S. Steel "Golden Share" provision granting U.S. Government consent rights over strategic decisions).

level risk. The America First Investment Policy signaled a preference for more concrete, time-limited mitigation conditions.[33] However, neither divestiture orders nor Golden Share provisions reach the vendor level. A U.S. solar company operating under an NSA may still purchase inverters from vendors whose equipment contains undisclosed capabilities, because the NSA governs the transaction party's conduct, not the vendor's product design.

IV. Why the Gap Exists and Why It Matters

The CFIUS framework was designed to regulate cross-border investment flows, not to serve as a comprehensive supply chain security regime. It addresses national security risks arising from changes in ownership or control of a U.S. business, the *investment nexus*, not risks arising from vendor relationships that predate or are independent of the covered transaction.

CFIUS addresses supply chain risk by requiring transaction parties to manage their vendors—demanding authorized-vendor lists, security audits, and software bills of materials. This indirect approach has three critical limitations:

Leverage asymmetry. When a vendor controls a dominant market position, the transaction party's ability to demand transparency into firmware architecture, enforce audit rights, or credibly threaten vendor substitution is constrained by commercial reality. Flow-down clauses are only as effective as the buyer's ability to walk away from a supplier that refuses to comply.

Information asymmetry. The transaction party may not know what it does not know about its vendors' products. As reported by Reuters, the undocumented communication devices discovered in 2025 were found not by purchasers or their third-party monitors but by government experts who physically disassembled equipment. A transaction party conducting a contractually negotiated firmware review would be unlikely to discover undisclosed radios embedded in circuit-board hardware.

Misallocated risk. The entire compliance burden falls on the transaction parties, even when the underlying national security risk originates entirely at the vendor level. A penalty may punish a party that diligently performed its contractual monitoring obligations but lacked the technical capacity or commercial leverage to detect or prevent vendor malfeasance.

[33] America First Investment Policy, National Security Presidential Memorandum (Feb. 2025).

Analysts have identified at least four dimensions of national security risk from Chinese clean technology supply chain dominance: dual-use technology concerns, coercion risk by a dominant supplier, espionage and sabotage through embedded technology, and relative economic gains that finance adversary military expenditures.[34] Each dimension manifests at the vendor level, in the manufacturer's design choices, the firmware update architecture, or the component sourcing, rather than at the investment transaction level that CFIUS reviews.

V. Recommendations

The following recommendations could address the gap between NSAs' transaction-party focus and the vendor-level risks that define much of the national security landscape.

1. Expand Vendor Disclosure Requirements Within NSAs

NSAs could require transaction parties to maintain continuously updated registries of all vendors supplying components to critical-infrastructure installations, including hardware bills of materials (HBOMs), software bills of materials (SBOMs), firmware-update protocols and signing-key custodians, remote-management capability disclosures (including all communication modules and their documented purposes), and ownership and corporate-control disclosures for each vendor. CMAs should receive notifications upon any change in vendor identity, ownership, or technical architecture. This gives monitoring agencies a basis for demanding vendor substitution when threat intelligence warrants it.

2. Establish a Critical-Infrastructure Component Certification Program

The government could create a certification regime for components, structured as follows:

Certification requirements: (a) verified HBOM and SBOM disclosing all hardware components and software modules; (b) independent penetration testing and vulnerability assessment by an accredited laboratory; (c) confirmation that all remote-management and communication capabilities are documented and that any remote-disable capability ("kill switch") can be disabled or placed under operator control; (d) firmware update-signing using keys escrowed with a U.S.-based or allied-nation

[34]War on the Rocks, "China, Clean Technologies, and National Security" (Oct. 2024) (identifying four dimensions of national security risk from Chinese supply chain dominance: dual-use technology concerns, coercion risk, espionage and sabotage, and relative economic gains).

custodian; (e) vulnerability-disclosure program meeting ISO/IEC 29147 standards; and (f) periodic recertification on a cycle not exceeding 24 months.

NSA integration: NSAs would reference the program by requiring that all critical-infrastructure components deployed by the transaction party hold current CMA-approved certification as a condition precedent to deployment. Failure to maintain certified equipment would constitute a material breach, triggering the substitution and transition-plan obligations described in the Model Clauses below.

3. Systematize CFIUS–Commerce ICTS Coordination

The ICTS rule under Executive Order 13873 can reach vendors directly—prohibiting or imposing conditions on any ICTS transaction involving foreign-adversary-linked persons. CFIUS could establish a formal referral protocol under which vendor-level risks identified during NSA monitoring are systematically transmitted to Commerce's Office of Information and Communications Technology and Services (OICTS) for potential investigation under 15 C.F.R. Part 791. The referral protocol should include:

(a) standardized threat-intelligence formats for CMA-to-OICTS transmission; (b) defined timelines for OICTS acknowledgment and preliminary assessment; (c) feedback loops permitting CMAs to receive OICTS determination outcomes for NSA compliance purposes; and (d) provisions permitting CMAs to treat an OICTS prohibition or adverse determination against a vendor as an independent trigger for the transaction party's vendor-substitution obligation under the NSA.

4. Require Vendor Flow-Down Clauses with Specified Minimum Terms

Current NSA practice permits CFIUS to require that transaction parties "tighten procurement or supply chain procedures," but the specific contractual terms that must be obtained from vendors are not standardized. NSAs could mandate that transaction parties incorporate the following minimum provisions in all vendor contracts for critical-infrastructure components:

(a) audit rights permitting the transaction parties and its CMA-approved monitors to inspect vendor facilities, firmware source code, and component inventories; (b) SBOM/HBOM delivery and continuous-update obligations; (c) firmware-key escrow with a U.S.-based custodian; (d) incident-reporting obligations requiring vendor notification to the transaction party within 24 hours of discovery of any security vulnerability, unauthorized access, or undisclosed component; (e) a prohibition on remote

disabling or modification of deployed equipment without prior written authorization from the operator; and (f) a right of the transaction party to terminate the vendor relationship and transition to an alternative supplier upon CMA direction, with the vendor's contractual cooperation in the transition.

Where a vendor refuses to accept these terms, the transaction party should be required to report the refusal to its CMAs within a specified period and, absent CMA approval of an alternative arrangement, to identify and transition to an alternative vendor within a defined timeline.

5. Enhance Government-to-Industry Intelligence Sharing

Transaction parties under NSAs could receive timely, actionable intelligence regarding vendor-level threats. The 2025 rogue-device reports illustrated a dangerous information gap: government experts could detect undisclosed capabilities that neither the transaction party nor its third-party monitors would have discovered through contractual vendor audits alone. *T*hreat briefings, sanitized intelligence products, and rapid notification protocols should become standard features of the CMA–transaction party relationship.

Toward a Layered Approach

No single recommendation solves the vendor gap. The NSA framework's strength lies in its specificity—it addresses identified risks arising from a particular transaction. Vendor-level risks are structural and industry-wide. They are not unique to any single covered transaction, and they cannot be resolved by any single mitigation agreement.

What is needed is a layered approach in which the NSA framework is complemented by sector-specific tools—the ICTS rule for direct vendor regulation, certification programs for component security, import restrictions where warranted, and investment incentives for domestic alternatives—that collectively create a security perimeter around critical energy infrastructure. The NSA governs the investment transaction. But it should not be asked to do the work of a comprehensive supply chain security regime. Recognizing this distinction is the first step toward closing the gap.

The GAO has noted that mitigation agreements have become "increasingly complex," with more detailed measures that make monitoring more challenging.[35] Adding vendor-level obligations to NSAs

[35]GAO Report GAO-24-107358, "Foreign Investment in the U.S.: Efforts to Mitigate National Security" (noting that mitigation agreements have become "increasingly complex" with "more detailed and specific measures").

without corresponding enforcement mechanisms would compound this complexity without meaningfully reducing risk. The more effective path is to ensure that different instruments—NSAs, ICTS rules, procurement standards, and industrial policy—operate in coordination rather than in isolation.

VI. Conclusion

National Security Agreements are a powerful tool for managing risks from foreign investment, and CFIUS's enforcement apparatus is more active and better resourced than at any prior point. Committee's indirect tools, authorized-vendor requirements, procurement controls, flow-down clauses, and vendor-substitution demands, give it meaningful influence over supply chain conduct through the transaction party.

Yet these tools operate within a structural constraint: the NSA binds only the parties to a covered transaction. Vendors whose products may constitute the very source of national security risk stand outside the enforcement perimeter. They are not signatories. They bear no direct obligations. They cannot be penalized for noncompliance with an agreement they never executed. The transaction party is left to manage, through commercial contractual mechanisms, risks that may exceed its leverage, its technical capacity, and its access to information.

The solar industry brings this into sharp relief. When undocumented communication devices are reportedly found in Chinese-manufactured inverters connected to the U.S. grid, and when a foreign vendor demonstrates the capability to remotely disable deployed equipment, the risk is immediate. But the NSA governing the company operating that installation cannot reach the manufacturer who designed the capability into the product. Addressing this gap requires augmenting the NSA framework through enhanced vendor disclosure, component certification, ICTS coordination, standardized flow-down clauses, domestic manufacturing investment, and better intelligence sharing. Only through a multi-layered approach can the United States ensure that the promise of national security mitigation is not undermined by an unregulated vendor ecosystem.

Appendix: Illustrative NSA Model Clauses

The following model clauses are provided for illustrative purposes to assist in drafting NSA provisions that address vendor-level supply chain risks. They are intended as starting points and should be adapted to the specific transaction, industry, and risk profile.

(a) Vendor Registry and Continuous Update

Section —. *The Transaction Parties shall establish and maintain a Critical-Infrastructure Vendor Registry ("Registry") identifying each vendor that supplies hardware, software, firmware, or networked communication components to any installation that constitutes or supports Critical Infrastructure as defined in this Agreement. The Registry shall include, for each listed vendor: (i) legal name, jurisdiction of incorporation, and ultimate beneficial ownership; (ii) a description of the component(s) or service(s) supplied; and (iii) the Hardware Bill of Materials ("HBOM") and Software Bill of Materials ("SBOM") for each component. The Transaction Party shall update the Registry within ten (10) business days of any change in vendor identity, ownership, component specification, or firmware architecture, and shall provide the updated Registry to the CMAs within five (5) business days of such update.*

(b) Remote-Access Controls and Kill-Switch Governance

Section —. *No component deployed at a Critical Infrastructure installation may include a remote-disable, remote-modification, or remote-access capability ("Remote-Access Capability") unless such capability is (i) fully disclosed in the HBOM/SBOM; (ii) subject to operator-controlled activation (i.e., the capability must be disabled by default and activatable only upon affirmative action by the Transaction Parties' authorized personnel); and (iii) incapable of being exercised by the vendor, manufacturer, or any third party without the Transaction Party's prior written authorization. Any component discovered to contain an undisclosed Remote-Access Capability shall be removed from service within thirty (30) days of discovery, or such shorter period as the CMAs may direct, and the Transaction Parties shall immediately notify the CMAs and initiate the Substitution Protocol under Section [ref].*

(c) SBOM/HBOM and Firmware-Key Escrow

Section —. *For each component listed in the Registry, the Transaction Parties shall obtain from the vendor and deliver to the CMAs (i) a complete SBOM conforming to NTIA Minimum Elements for a Software Bill of Materials or successor standard; (ii) a complete HBOM identifying all physical components including communication modules, processors, and memory devices; and (iii) escrow of all firmware-signing keys with a U.S.-based or allied-nation escrow agent approved by the CMAs. The escrow agreement shall permit the CMAs or their designee to access escrowed keys upon determination that the vendor has become unresponsive, noncompliant, or subject to adverse action under any U.S. national security authority. Firmware updates shall be signed with escrowed keys and verified by the Transaction Parties prior to deployment.*

(d) Right to Demand Vendor Substitution

Section —. *Upon written direction from the CMAs, the Transaction Parties shall cease procurement from any designated vendor and implement a transition to a CMA-approved alternative vendor within ninety (90) days, or such other period as the CMAs may specify. The Transaction Parties shall maintain at all times a documented Vendor Substitution Plan identifying at least one pre-qualified alternative vendor for each critical component category. The Substitution Plan shall be updated annually and submitted to the CMAs for review. The Transaction Parties' obligation to complete the transition shall not be excused by increased cost, supply delay, or performance difference, except where the Transaction Parties demonstrate to the CMAs' reasonable satisfaction that no commercially available alternative exists, in which case the CMAs and the Transaction Parties shall negotiate a remediation plan.*

(e) Incident Reporting Timelines

Section —. *The Transaction Parties shall report to the CMAs: (i) within twenty-four (24) hours of discovery, any cybersecurity incident, unauthorized access, or anomalous behavior affecting a component deployed at a Critical Infrastructure installation; (ii) within forty-eight (48) hours of discovery, any identification of an undisclosed hardware or software component, undocumented communication capability, or firmware modification not authorized by the Transaction Parties; and (iii) within five (5) business days, any vendor notification of a security vulnerability affecting a deployed component, whether or not a patch or mitigation is available. Reports shall include: the nature and scope of the incident; the affected component(s) and installation(s); remedial steps taken or planned; and an assessment of potential national security impact.*

(f) Audit Rights Obtained From Vendors

Section —. *The Transaction Parties shall obtain from each vendor listed in the Registry a contractual commitment granting the Transaction Parties, their CMA-approved third-party monitors, and (upon reasonable notice) representatives of the CMAs, the right to: (i) conduct on-site inspections of vendor manufacturing, testing, and software-development facilities; (ii) review firmware source code, hardware design specifications, and quality-control records; (iii) commission independent penetration testing of components prior to deployment; and (iv) receive copies of all third-party security certifications, audit reports, and vulnerability assessments conducted within the preceding twenty-four (24) months. The Transaction Parties shall exercise these audit rights at least annually for each critical-infrastructure vendor and shall provide audit results to the CMAs within thirty (30) days of completion.*

(g) Consequences for Inability to Obtain Vendor Cooperation

Section —. *If the Transaction Parties are unable, after commercially reasonable efforts documented in writing, to obtain from a vendor the contractual commitments required by Sections [ref(a)–ref(f)] within sixty (60) days of notification to the CMAs, the Transaction Parties shall: (i) immediately notify the CMAs of the vendor's refusal or non-response; (ii) submit a Forced Transition Plan to the CMAs within thirty (30) days of such notification, identifying alternative vendors, transition timelines, and interim risk-mitigation measures; (iii) upon CMA approval of the Forced Transition Plan, implement the transition within the timeline specified therein; and (iv) pending completion of the transition, implement all commercially available interim mitigations, including but not limited to network segmentation, enhanced monitoring, and restriction of remote-access capabilities. Continued use of a noncompliant vendor's components beyond the approved transition timeline shall constitute a material breach of this Agreement.*