CENTER FOR COMPETITIVE STATECRAFT AND STRATEGIC POLICY

WORKING PAPER | WP-2026-PERSIST-01

PERSIST:

A Litigation-Resilient Architecture for U.S. Competitive Statecraft

Against the People's Republic of China

Independent Policy Research | March 2026

ABSTRACT

This paper presents a competitive statecraft architecture designed to reduce the People's Republic of China's (PRC's) capacity to coerce neighbors, acquire military-relevant technology through illicit means, conduct transnational repression, and undermine allied cohesion. The architecture is built on five independent, severable pillars grounded in existing U.S. statutory authority, multilateral mechanisms, and documented PRC enabling conduct. This revision adds four hardening elements: (1) a six-rail authority framework mapping what each legal instrument can and cannot reach; (2) a tiered escalation ladder converting pressure into procedure—evidence-gated, reversible, and coalition-conditioned; (3) a standards-of-proof framework distinguishing credible signal, confirmed attribution, material enabling behavior, and systemic-risk threshold; and (4) a neutral designation-selection rule with objective triggers, a prohibited-factor list, and a selection log as the primary defense exhibit against selective-enforcement challenge.

Keywords: competitive statecraft, export controls, ECRA/BIS, IEEPA/OFAC, CFIUS, deterrence-by-denial, financial integrity enforcement, evidence gating, coalition durability, stability architecture, tiered escalation, designation-selection log, severability, PRC coercive capacity

Disclaimer: This working paper represents independent policy research and analysis. It does not constitute legal advice and does not represent the position of any government agency, academic institution, or political organization. All citations are drawn from publicly available U.S. federal law, regulations, executive authorities, and open-source analytical material. Nothing in this paper directs any agency action or compels any enforcement decision.

INTERPRETIVE RULE: SEVERABILITY

Each section, pillar, prong, appendix, and definition in this framework is intended to be independently operative and severable from every other. Judicial invalidation, enjoinment, or limitation of any provision does not affect the validity or enforceability of any remaining provision. Each mechanism is grounded in its own independent legal or policy authority and is designed to function in the absence of any other. This interpretive rule applies to all policy instruments, interagency coordination documents, and implementing guidance that incorporates this framework by reference.

SECTION 1: DESIGN PRINCIPLES FOR A LITIGATION-RESILIENT COMPETITIVE POSTURE

1.1 The Core Design Problem

A competitive statecraft posture that overpromises collapses twice: first in legal and political challenge, where enjoined or discredited mechanisms generate adverse precedent and coalition fracture, and second in practice, where disabled mechanisms create operational gaps that the PRC can exploit. The goal of this framework is a posture that applies maximum lawful pressure and does not hand opponents — foreign or domestic — an easy procedural win.

The design rules that govern this architecture:

- Target conduct and documented enabling behavior — not ethnicity, viewpoint, national origin, or political affiliation. Every enforcement or denial mechanism must be tied to an act, a verified pattern, or a documented element — not to identity or political position.
- Never treat unverified suspicion as a confirmed finding. The standards-of-proof framework in Section 4 maps the evidence threshold required before each category of action.
- Avoid automatic penalties. Every consequence must flow from documented findings, notice, and an administrative or policy record. 'Automatic' reads as arbitrary — exactly what legal and political challengers exploit.
- Tie every action to a documented authority rail. Measures without clear statutory or executive authority are vulnerable to challenge and create adverse precedent that constrains future legitimate action.
- Build each pillar to stand independently. If one mechanism is challenged, enjoined, or politically constrained, the others continue operating. No single point of failure.
- Gate coalition-sensitive measures on allied coherence. Tier 2 and above measures that carry significant market, diplomatic, or systemic risk require prior coalition-risk review. Unilateral action at higher tiers undermines the coalition durability that makes the framework effective.
- Build reversibility into every pressure line. Each pressure measure specifies what verified behavior change by the PRC triggers suspension or reversal. Reversibility is not weakness — it is what makes the pressure credible and distinguishes deterrence from punishment.
- Apply controls prospectively where feasible. New licensing definitions, entity additions, and secondary exposure criteria should include effective-date clarity and compliance runway where national security permits. Ambiguity about when a control applies produces compliance failures that become litigation and coalition fracture — the same failure mode as retroactively imposed grant conditions.

1.2 What This Architecture Does and Does Not Claim

ARCHITECTURE SCOPE	
This Architecture DOES	**This Architecture DOES NOT**
Target documented enabling conduct and illicit facilitation	Claim authority to compel collective punishment of PRC nationals broadly
Apply evidence-gated measures at each tier with documented records	Promise complete economic decoupling via executive action alone

Maintain reversibility upon verified PRC behavior change	Authorize automatic or pre-set escalation without documented record
Gate coalition-sensitive actions on allied coherence review	Target conduct based on ethnicity, national origin, or viewpoint
Distinguish lawful trade from military-relevant technology transfer	Treat any single mechanism as a total solution
Operate each pillar independently to eliminate single points of failure	Override congressional appropriations or treaty obligations
Maintain stability architecture: crisis communications, off-ramps, guardrail index	Assert extraterritorial reach beyond recognized international law limits

SECTION 2: AUTHORITY RAILS — WHAT DEFINES THE PLAYING FIELD

Authority rails define what legal instruments govern each pressure mechanism, where each instrument's hard limits are, and what drafting or process discipline is required to keep actions within those limits. The function of this section is identical to that of constitutional rails in domestic enforcement architecture: tell the reader what cannot be crossed, so the rest of the framework reads as engineered rather than aspirational.

2.1 Export Controls Rail (ECRA / BIS Authorities)

The Export Control Reform Act of 2018 (50 U.S.C. §§ 4801–4852) and the Export Administration Regulations (15 C.F.R. Parts 730–774) govern U.S. dual-use and military-relevant technology export controls. The Bureau of Industry and Security (BIS) administers the Entity List, the Military End User List, and the Foreign Direct Product Rule. These are the primary instruments for technology denial targeting semiconductor manufacturing equipment, advanced computing, AI infrastructure, and related enabling technologies.

This is the primary action rail for Pillar 1 and Pillar 3. BIS has broad regulatory discretion, but that discretion is constrained by the APA's arbitrary-and-capricious standard, the due process requirements of the Entity List notice and response process, and the Foreign Direct Product Rule's jurisdictional predicates. A designation or control that cannot survive administrative record review is a hard limit, not a drafting preference. Record hygiene under this rail is as consequential as it is under a grant certification framework.

DRAFTING RULE

Entity List additions require documented evidence of diversion risk, military end-use concern, or export-control evasion. Politically motivated additions without evidentiary basis are vulnerable to challenge and create adverse precedent that weakens future legitimate designations.

Foreign Direct Product Rule extraterritoriality is bounded by allied coordination. Unilateral application to third-country entities without allied concurrence risks coalition fracture and generates legal challenge in foreign jurisdictions.

Licensing clarity is a durability rule. Ambiguous control parameters produce compliance failures and litigation that constrain legitimate denial authority.

2.2 Sanctions Rail (IEEPA / OFAC)

The International Emergency Economic Powers Act (50 U.S.C. §§ 1701–1708) grants the President broad authority to regulate transactions involving foreign countries or nationals during a declared national emergency. The Office of Foreign Assets Control (OFAC) administers sanctions programs including Specially Designated Nationals (SDN) designations, sectoral sanctions, and secondary sanctions exposure rules.

IEEPA authority is broad but not unlimited. This is a hard structural limit: IEEPA requires a declared national emergency with a nexus between the designated conduct and the declared emergency. Designations that cannot document that nexus — or that designate based on nationality rather than conduct — are vulnerable to reversal and generate adverse judicial precedent that constrains future legitimate sanctions programs. The evidentiary record built before each designation is the primary defense against reversal.

DRAFTING RULE

SDN designations require documented evidentiary basis tied to the declared emergency. Due process hygiene — notice, opportunity to challenge, administrative record — reduces reversal risk and selective-enforcement vulnerability.

Secondary sanctions exposure for third-country entities requires clear, published criteria. Ambiguous secondary exposure rules produce coalition friction and compliance over-reaction that erodes allied participation.

Evidence-gating is not optional at Tier 2 and above. Designations made on credible signal alone — without confirmed attribution — are the most common source of legal reversal and political discrediting of broader programs.

2.3 Investment Screening Rail (CFIUS)

The Committee on Foreign Investment in the United States (CFIUS), operating under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), reviews foreign investments for national security implications. CFIUS authority covers covered transactions involving U.S. critical technology, critical infrastructure, and sensitive personal data.

DRAFTING RULE

CFIUS jurisdiction is bounded by FIRRMA's covered transaction definitions. Mandatory filing requirements apply to specific sectors; voluntary filing is available for others. Actions outside these categories require new legislative authority.

Outbound investment screening — covering U.S. investments in PRC entities in specified sectors — operates under separate executive authority (E.O. 14105) and is more legally contested. Document authority basis explicitly for each outbound action.

2.4 Defense Cooperation Rail

Security assistance, arms transfer, and defense cooperation authorities govern the provision of military capability and technology to allies and partners. Relevant instruments include the Arms

Export Control Act (22 U.S.C. §§ 2751–2799), Foreign Military Sales, Direct Commercial Sales, and AUKUS-enabling legislative provisions.

DRAFTING RULE

Congressional notification requirements apply to arms transfers above specified thresholds. Failure to comply with notification discipline creates statutory and political vulnerability that adversaries exploit to delay allied capability delivery.

Prioritization of Taiwan asymmetric defense capability (UAS, coastal defense, air defense) and Philippines/Japan/South Korea deterrence architecture investment requires sustained budget and transfer discipline across administration transitions. Document the policy rationale for each prioritization decision.

2.5 Speech and Information Rail

The information pillar operates under the most constrained authority environment. Lawful instruments include: support for independent journalism and civil society organizations operating within rule-of-law frameworks; exposure of illicit PRC influence operations through declassified intelligence and open-source analysis; and enforcement of the Foreign Agents Registration Act (22 U.S.C. §§ 611–621) against unregistered PRC-linked influence networks.

DRAFTING RULE

The information pillar does not authorize deceptive content, manufactured attribution, or covert influence operations directed at any population — domestic or foreign. Activities that cross into covert influence operations undermine the rule-of-law transparency rationale and create First Amendment and international law exposure.

Foreign Agents Registration Act enforcement must be conduct-based and viewpoint-neutral. Targeting organizations based on their political positions rather than their failure to register as foreign agents converts legitimate enforcement into viewpoint discrimination.

2.6 International Law and Alliance Rail

Coalition coordination is not optional at Tier 2 and above. The extraterritorial reach of U.S. export controls, sanctions, and technology denial measures is legally and politically sustainable only where: (a) allied governments have agreed to coordinate or not actively oppose U.S. measures; (b) actions are consistent with WTO obligations or justified under recognized national security exceptions (GATT Art. XXI); and (c) the measures do not require allied governments to impose domestic penalties on their own nationals without their own legislative authority.

DRAFTING RULE

Coalition-first sequencing is a durability rule. Tier 2+ measures imposed without prior allied coordination generate retaliatory measures, WTO challenges, and diplomatic friction that erode the coalition the framework depends on.

The live contradiction between technology denial coordination and simultaneous trade friction with the same allied partners (Netherlands, Japan, South Korea) is the largest implementation gap in this architecture. Resolve it before escalating to Tier 2. Acknowledge it explicitly in any public framing.

SECTION 3: TIERED ESCALATION LADDER

The escalation ladder converts competitive pressure into procedure. No tier is automatic. Every action at every tier flows from a documented evidentiary record, a completed coalition-risk review at Tier 2 and above, and a guardrail index check at Tier 3. The ladder is designed so that each tier is reversible upon verified behavior change, and so that Tier 3 actions require independent findings not available from Tier 1 evidence alone.

TIERED ESCALATION LADDER — PERSIST FRAMEWORK

Tier / Label	Activation Threshold	Available Instruments	Risk Profile	Suspension / Reversal Trigger
Tier 0 — Baseline	No special triggering event required; ongoing condition of competition.	Allied coordination and coherence review; defensive cyber hardening; supply chain resilience investment; counterintelligence capacity; asymmetric partner defense capability; open-source monitoring infrastructure.	No significant systemic risk; actions are defensive and capacity-building.	Verified baseline. No Tier 0 measure triggers suspension.
Tier 1 — Coordinated Denial + Transparency	Credible signal (OSINT + allied assessment) of military-relevant technology acquisition or illicit influence operation. Not action-triggering alone; initiates enhanced monitoring and allied consultation.	Coordinated semiconductor/equipment export control tightening; Entity List additions with documented evidentiary basis; Foreign Agents Registration Act enforcement; PRC elite offshore asset exposure through open-source and declassified channels; independent journalism and civil society support.	Low systemic market risk; primary risk is allied coherence friction if unilateral.	Verified cessation of the specific documented enabling conduct. Allied agreement that suspension is warranted.
Tier 2 — Targeted Financial Integrity	Confirmed attribution: documented PRC-linked entity facilitation of export-control evasion, illicit weapons-relevant procurement, or systematic transnational repression. Coalition-risk review completed.	Evidence-gated SDN designations; sectoral sanctions on specific military-civil fusion entities; secondary sanctions exposure for documented third-country facilitators; coordinated allied financial intelligence sharing.	Higher coalition and market risk. Tier 2 requires prior coalition-risk review. Guardrail index reviewed before action.	Verified cessation of designated conduct; OFAC administrative record supports delisting; allied coalition concurs.
Tier 3 —	Systemic-risk	Comprehensive entity-	Significant	Verified, sustained,

Systemic Actions	threshold: documented pattern of behavior constituting a material threat to allied security architecture. Guardrail index must not show red-zone indicators. Presumptive pause active if guardrail threshold breached.	category restrictions; broad foreign direct product rule application; systemic financial mechanism restrictions. Rare; each action individually authorized with documented evidentiary record.	systemic and market risk. Requires: (a) documented systemic-risk threshold finding; (b) guardrail index in green zone; (c) allied coalition concurrence; (d) public off-ramp statement.	and independently confirmed behavior change across all identified threat vectors. Requires allied coalition agreement and public off-ramp completion.

COALITION-RISK REVIEW — REQUIRED RECORD (Tier 2 and Above)

Before any Tier 2 or Tier 3 action is initiated, the coordinating agency must complete and retain a Coalition-Risk Review Memorandum. This memo is the required record; no Tier 2 or Tier 3 action proceeds without it.

- INPUTS: The memo must identify: (a) which allied governments were consulted or notified, by name; (b) which U.S. agencies participated in the review; (c) the date of consultation and method (bilateral, multilateral, or written notification); and (d) any allied objections or conditions raised during the review period.
- CONCURRENCE vs. NON-OBJECTION: Tier 2 actions require documented non-objection from at least one primary technology-denial partner (Netherlands, Japan, or South Korea, as applicable to the instrument). Tier 3 actions require affirmative written concurrence from at least two primary partners. Silence does not constitute concurrence at Tier 3.
- DISSENT RECORDING: Any allied government that raises a formal objection to a proposed action must have its objection recorded in the memo. If the action proceeds over a recorded objection, the memo must document: (a) the nature of the objection; (b) the overriding national security rationale; and (c) what mitigation was offered to the objecting partner. A recorded objection triggers an automatic 30-day review hold unless the coordinating agency documents an emergency exception.
- RETENTION: Coalition-Risk Review Memoranda are retained as part of the administrative record for each designated action and are available for interagency review. They are the primary defense exhibit against coalition-fracture and arbitrary-action challenge.

GUARDRAIL INDEX — AUTOMATIC PAUSE TRIGGERS FOR TIER 3

The guardrail index monitors four systemic stability indicators. A red-zone reading on any indicator triggers a presumptive pause on Tier 3 initiation or continuation. Pause categories are public; specific thresholds require classified baseline calibration.

- Indicator A: Dollar reserve share trajectory (sustained decline below [X]% threshold signals

systemic financial fragmentation risk).

- Indicator B: CIPS adoption among non-sanctioned entities (rapid adoption signals sanctions evasion infrastructure scaling beyond addressable threshold).
- Indicator C: Allied coalition cohesion (defection of two or more primary technology-denial partners from coordinated action triggers presumptive pause).
- Indicator D: PRC countermeasure activation (documented activation of rare earth export restrictions, market access retaliation, or cyber-infrastructure targeting at critical-infrastructure scale).
- GOVERNANCE: The guardrail index is owned by the interagency coordinating committee responsible for Tier 3 action authorization. The index is reviewed on a standing quarterly basis and on an ad hoc basis before any Tier 3 initiation. Reviewing officials must be at the Assistant Secretary level or above, and must include representation from NSC, Treasury/OFAC, Commerce/BIS, and State. Review minutes are retained as part of the administrative record.
- PAUSE MECHANICS: A presumptive pause is not a permanent stop. It is a hold pending a documented override review. To override a presumptive pause, the coordinating agency must produce a written override memorandum documenting: (a) which guardrail indicator is in red zone; (b) why the proposed Tier 3 action is warranted despite the indicator reading; (c) what risk-mitigation measures are in place; and (d) which senior official authorized the override. The override memo is retained as part of the administrative record. Proceeding with Tier 3 action without a completed override memo when a guardrail indicator is in red zone is a procedural violation under this framework.

SECTION 4: STANDARDS OF PROOF

This section prevents the central failure mode in competitive statecraft: acting on credible concern rather than confirmed finding, losing legal or coalition credibility when the evidentiary basis is challenged, and generating adverse precedent that constrains future legitimate action. The four-tier proof framework maps the evidence threshold required before each category of action. Lower tiers trigger monitoring and consultation; higher tiers trigger action. No mechanism at any tier is available below its required evidentiary threshold.

STANDARDS OF PROOF — PERSIST FRAMEWORK

Standard	Definition	Action Threshold	Required Documentation
Credible Signal / Indicator	OSINT-derived pattern; allied intelligence assessment; financial intelligence indicator. Not independently action-triggering.	Initiates enhanced monitoring, allied consultation, and Tier 1 review. Does not support designation, sanctions action, or public attribution.	Classified and open-source analytical record; allied assessment documentation.
Confirmed Attribution	Independently verified finding from two or more classified or forensic sources; corroborated by	Supports Entity List addition, FARA enforcement action, and public exposure	Attribution report with corroborating sources; legal review confirming evidentiary sufficiency; interagency

	financial intelligence or technical forensics. Required before any public attribution or Tier 2 action.	measures. Required predicate for any Tier 2 SDN or sectoral sanctions action. NOTE: Some Tier 1 instruments (e.g., Entity List additions) are legally available at lower 'reasonable cause to believe' standards under the EAR. This architecture voluntarily imposes the confirmed-attribution standard as a durability rule — it is the threshold this framework chooses, not the minimum the statute requires. The durability rationale: designations made at lower standards are more frequently reversed and generate adverse precedent that weakens future legitimate actions.	coordination record.
Material Enabling Behavior	Documented, confirmed pattern of conduct by a specific entity that materially enables PRC military-relevant acquisition, transnational repression, or export-control evasion — beyond isolated incident.	Required threshold for Tier 2 financial integrity measures (SDN designation, secondary exposure). Pattern must be documented across multiple verified incidents.	Evidentiary file with specific transactions, entities, dates, and documented nexus to PRC military or coercive program. Legal counsel review. Due process notice where applicable.
Systemic-Risk Threshold	Sustained, documented pattern across multiple confirmed-attribution findings establishing material threat to allied security architecture or critical infrastructure. Not met by single-entity findings.	Required threshold to initiate Tier 3 systemic actions. Guardrail index must be in green zone. Presumptive pause active if systemic-risk finding is based solely on extrapolation from Tier 1 or 2 evidence without independent Tier 3-level verification.	Comprehensive analytical record; classified National Intelligence Estimate or equivalent; interagency legal review; allied consultation documentation; public off-ramp statement.

EVIDENTIARY INTEGRITY RULE

No action at Tier 2 or above may be initiated based on a credible signal alone. The evidentiary gap between 'we believe this is occurring' and 'we can document this occurred' is the primary point of legal and political challenge. Documenting that gap — and closing it before action — is what distinguishes this framework from postures that collapse under review.

SECTION 5: NEUTRAL DESIGNATION-SELECTION RULE

5.1 The Selection Problem

Designation and enforcement targeting are the primary vectors for selective-enforcement and viewpoint-discrimination challenge. Challengers argue that a specific entity was targeted because of its identity, political associations, or nationality rather than its conduct. The complete defense is a documented, neutral selection methodology applied uniformly across all entities regardless of affiliation, nationality, or public statements — applied before the targeting decision, documented at the time, and preserved as a litigation-ready record.

NEUTRAL DESIGNATION-SELECTION CRITERIA (Required Documentation)

A designation, Entity List addition, or equivalent action under this framework may be initiated only when one or more of the following objective triggers is documented in the selecting authority's record before the targeting decision:

(a) DOCUMENTED FACILITATION: The entity has verifiable transactions or relationships demonstrating direct facilitation of PRC military-relevant technology acquisition, weapons-relevant procurement, or systematic transnational repression — documented through financial intelligence, forensic analysis, or confirmed-attribution-standard intelligence.

(b) EXPORT-CONTROL EVASION PATTERN: The entity has two or more documented instances of transshipping, re-exporting, or acquiring controlled items in violation of applicable export control regulations — supported by BIS or equivalent agency investigative record.

(c) REPEATED VIOLATIONS: The entity has a prior confirmed finding of the same category of conduct within the preceding [36] months that was not remediated within the applicable cure period.

(d) REFERRAL FROM ALLIED AUTHORITY: A referral from a partner nation export control, financial intelligence, or law enforcement authority based on the partner's independent investigation, corroborated by at least one U.S. government source.

(e) INSPECTOR GENERAL OR OVERSIGHT REFERRAL: A referral from an agency Inspector General or congressional oversight body based on independent investigation.

SELECTION PROHIBITION: No designation or targeting action may be initiated based on: the entity's national origin, ethnicity, or the nationality of its beneficial owners absent documented conduct; the entity's political statements or advocacy; the entity's participation in litigation challenging U.S. government action; or any other factor related to viewpoint or expression rather than documented conduct.

DOCUMENTATION REQUIREMENT: The selecting authority must maintain a designation-selection log recording, for every entity selected: (1) the objective trigger(s) documented; (2) the date the trigger was documented; (3) the identity of the selecting official and reviewing authority; (4) confirmation that no prohibited selection factor was considered; (5) the applicable authority rail under Section 2; and (6) the remediation or off-ramp criteria — specifically, what verified conduct cessation or behavior change by the entity would support delisting or removal from the Entity List, and whether that pathway was communicated to the entity where legally permissible. Item (6) reinforces the reversibility principle across the framework and converts the selection log into a full defense exhibit: it demonstrates not only that the targeting was evidence-based, but that the framework is designed to remove pressure when conduct changes. This log is the primary defense exhibit in any selective-enforcement or viewpoint-retaliation challenge.

5.2 Prohibited Factor List

- National origin, ethnicity, or race of entity owners or employees, absent documented conduct.
- Political or advocacy positions taken by the entity on U.S. or PRC policy.
- Participation in legal proceedings challenging U.S. government export control, sanctions, or investment screening actions.
- Media coverage or public profile of the entity, unaccompanied by documented conduct.
- Diplomatic relationship between the entity's home country and the PRC, without evidence the entity itself participated in the relevant conduct.

SECTION 6: THE FIVE INDEPENDENT PILLARS

Each pillar is independently operative and severable. Constraint or failure of one pillar does not disable the others. The five pillars are designed so that the failure of any single pillar does not create a decisive gap — each pillar addresses a distinct PRC vulnerability, and the combination creates compounding pressure that is harder to absorb than any single-instrument approach.

6.1 Pillar 1 — Economic Performance Constraint

Strategic logic: PRC regime legitimacy rests substantially on delivering economic growth and improving living standards. Technology denial and export friction that raise the cost of military-civil fusion, slow advanced semiconductor access, and increase manufacturing input costs degrade the economic performance the regime depends on for internal legitimacy. This pillar does not target PRC consumers or the civilian economy broadly — it targets the military-relevant technology acquisition and illicit facilitation networks that convert civilian economic activity into coercive military capacity.

- Coordinated semiconductor manufacturing equipment denial (Netherlands, Japan, United States; ASML, Tokyo Electron, KLA, Applied Materials) targeting sub-14nm process capability.
- Advanced computing export controls targeting A100/H100-equivalent and above GPU and AI accelerator hardware.
- Entity List additions with documented evidentiary basis for PRC military-civil fusion entities and front-company procurement networks.
- Evidence-gated secondary exposure rules for third-country facilitators with documented transshipment patterns — not blanket national exposure.

6.2 Pillar 2 — Information Control Disruption

Strategic logic: The PRC information environment sustains a specific internal narrative: that the CCP delivers prosperity, that external criticism is hostile, and that domestic dissent is manufactured. Accurate data about youth unemployment, property market distress, elite corruption, and offshore asset concentration introduces friction into that narrative — not through deception, but through rule-of-law transparency. This pillar uses no deceptive content. Every instrument is attributable and lawful.

- Circumvention infrastructure support for PRC citizens to access non-censored information.
- Open-source and declassified exposure of PRC elite offshore asset holdings and corruption documentation.

- Independent journalism support for organizations covering PRC domestic governance and military-civil fusion activity.
- United Front Work Department and PRC-linked influence operation exposure through FARA enforcement and public attribution at confirmed-attribution evidentiary standard.

6.3 Pillar 3 — Military Readiness Uncertainty

Strategic logic: The PRC military's ability to credibly threaten Taiwan and regional partners depends on its ability to close the military-technological gap with the United States and its allies. Technology denial that prevents gap closure, combined with visible allied military capability demonstration, creates uncertainty in PRC military planning that raises the expected cost of coercive action. This pillar does not seek to provoke military confrontation — it seeks to make the expected cost of attempted coercion too high to make the attempt rational.

- Technology denial targeting PRC military-relevant AI, advanced computing, quantum sensing, and hypersonic guidance systems through coordinated export control architecture.
- Allied military exercise tempo and capability demonstration in the South China Sea, Taiwan Strait, and Indo-Pacific operating areas.
- Taiwan asymmetric defense capability acceleration: coastal defense cruise missiles, UAS networks, air defense systems, and reserve force modernization.

6.4 Pillar 4 — Deterrence Architecture

Strategic logic: The PRC's Taiwan commitment is the central nationalist narrative and the primary driver of timeline pressure on PRC leadership. A visible, credible deterrence stack — Taiwan asymmetric defense, AUKUS submarine capability, Japan self-defense expansion, Philippines basing access, and combined arms exercise demonstration — imposes a growing military cost on any Taiwan crossing attempt while creating political space for deferral. Deterrence-by-denial is not provocation. It is miscalculation prevention.

- AUKUS nuclear-powered submarine capability delivery on accelerated timeline.
- Japan Self-Defense Force offensive strike capability development under revised national security strategy.
- Philippines Enhanced Defense Cooperation Agreement basing expansion.
- Incident-at-sea protocols and military-to-military hotlines at operational (not solely diplomatic) level to reduce miscalculation risk in high-tempo operating environments.

6.5 Pillar 5 — Allied and Domestic Resilience

Strategic logic: All four preceding pillars are only sustainable if allied partners maintain coherence and if domestic political and economic systems can absorb PRC countermeasures. This pillar is the enabling condition for the others. Without it, PRC countermeasures — rare earth export restrictions, market access retaliation, cyber infrastructure targeting — can fracture the coalition or impose domestic costs that force political reversal before the compounding logic of the framework has time to operate.

- Critical mineral and rare earth supply chain diversification and strategic reserve investment.
- Pharmaceutical active pharmaceutical ingredient (API) supply chain hardening — particularly for antibiotic starting materials where PRC upstream concentration is documented.

- Counterintelligence capacity expansion targeting PRC technology transfer and research espionage networks.
- Economic adjustment assistance for sectors most exposed to PRC countermeasure retaliation — preventing domestic political reversal before the framework's compounding logic operates.
- Allied information sharing on PRC-linked financial crime, sanctions evasion, and export-control circumvention networks.

SECTION 7: STABILITY ARCHITECTURE

The stability architecture addresses the escalation spiral objection procedurally rather than rhetorically. An escalation spiral is not prevented by asserting it will not happen — it is prevented by building the specific procedural mechanisms that make uncontrolled escalation less likely. Three components:

7.1 Crisis Communications Infrastructure

- Military-to-military hotlines at operational level — not solely at diplomatic leadership level — so that incident management can occur in real time without requiring political authorization for each communication.
- Pre-agreed incident-at-sea and incident-in-air protocols covering rules of engagement notification, post-incident reporting, and de-escalation sequencing.
- Pre-designated escalation channels that remain functional when diplomatic relations are formally strained — modeled on Cold War-era direct communication architecture.

7.2 Pressure-to-Behavior Linkage (Published Off-Ramps)

Each pressure line in the tiered escalation ladder specifies publicly, in advance, what verified PRC behavior change triggers suspension or reversal of that pressure line. The off-ramps are:

- Specific — they name the conduct whose cessation triggers suspension, not a general improvement in relations.
- Verifiable — they specify what independent verification is required before suspension (allied assessment, inspection regime, financial intelligence).
- Pre-committed — they are published before pressure is applied, so PRC decision-makers can factor them into cost-benefit calculations.

Pressure without a published, specific off-ramp is punishment, not deterrence. Punishment does not generate behavior change — it generates entrenchment and coalition erosion.

7.3 Guardrail Index

The guardrail index is described in Section 3. Its function in the stability architecture is to create a procedural pause trigger that operates below the threshold of political decision-making — a systemic check that automatically requires review before Tier 3 escalation proceeds when leading indicators suggest that escalation is approaching systemic risk territory. The guardrail index does not prevent Tier 3 action; it requires that the action be affirmatively authorized after the systemic risk indicators are reviewed and found acceptable.

SECTION 8: PRESCRIPTIVE SUBSTITUTION GUIDE

The substitutions below replace the most commonly deployed attacker framings of competitive statecraft with maximum-pressure equivalents that remain within authority rails and resist legal and political challenge. These are not weaker versions of the original language. They are stronger versions — because they will not be immediately discredited. Each right-column substitute is written as a rule, not persuasion: it anchors to objective conduct, evidence gating, reversibility, coalition durability, and stability architecture.

Attackable Language (Avoid)	Durable Substitute (Use)
"Regime change / collapse strategy."	Deterrence + constraint to reduce coercive capacity, with reversible measures upon verified behavior change. Published off-ramps specify what conduct cessation triggers suspension.
"Collective punishment / harm the Chinese people."	Entity-specific, evidence-gated measures targeting documented enabling conduct. Explicit prohibition on indiscriminate measures. Civilian and lawful commercial activity maintains a compliance pathway.
"Economic warfare to 'cripple' China."	Defensive denial of military-relevant inputs and financial integrity enforcement against documented illicit facilitation, bounded by predictable compliance pathways and published evidentiary standards.
"Propaganda / psychological operations."	Rule-of-law transparency, independent journalism support, and lawful exposure of documented illicit influence operations. No deceptive content. All attribution is accurate and attributable.
"Forced decoupling / autarky."	Targeted de-risking and resilience-building to reduce coercive leverage in specific military-relevant and critical-dependency sectors. Lawful trade with non-designated entities maintains a compliance pathway.
"Unilateral U.S. extraterritorial coercion."	Coalition-first coordination; actions sequenced to allied coherence review; Tier 2+ measures gated by coalition-risk assessment. Unilateral action at higher tiers is not authorized under this framework.
"Escalation spiral strategy."	Procedural stability architecture: crisis communications infrastructure, explicit pressure-to-behavior linkages with published off-ramps, and guardrail-index pause triggers before Tier 3 initiation.
"Politicized / arbitrary designation targeting."	Neutral designation-selection rule: objective triggers documented before targeting decision, prohibited-factor list, and designation-selection log as primary defense exhibit. No designation without documented evidentiary record.
"Blank-check Taiwan escalation."	Deterrence-by-denial with visible defensive capability; explicit purpose is miscalculation reduction, not provocation. Bounded by incident-management protocols and published pressure-to-

	behavior off-ramps.

SECTION 9: COMPOUNDING LOGIC

Each pillar's pressure compounds with the others rather than operating in parallel. The sequence:

- Economic constraint raises the cost of delivering prosperity, which is the primary source of regime legitimacy under conditions of political restriction.
- Information pressure introduces accurate data about governance failures, which creates internal credibility risk for a system that cannot tolerate accurate external comparison.
- Military uncertainty raises the expected cost of the Taiwan option at the moment economic and political pressure make that option more tempting as a legitimacy-restoring action.
- Deterrence architecture makes the military option increasingly costly and less certain of success, which creates tension between Xi's stated timeline and PLA's honest operational assessment.
- Allied and domestic resilience absorbs PRC countermeasures — rare earths, market access, cyber — that would otherwise fracture the coalition or force domestic political reversal before the compounding logic has time to operate.

The compounding mechanism is that each PRC defensive move — information suppression, military buildup, economic retaliation — costs something the regime cannot easily afford. Suppressing information requires more resource and creates more internal credibility risk as economic conditions worsen. Military buildup consumes economic resources at the moment economic performance is already under pressure. Economic retaliation against allied partners accelerates allied coalition cohesion rather than fracturing it, if the resilience pillar is functioning.

SECTION 10: KNOWN FAULT LINES AND HOW THIS ARCHITECTURE ADDRESSES THEM

This section is not a concession of weakness. It is armor. An architecture that acknowledges the principal vulnerabilities to which it is exposed, and demonstrates how its specific design addresses each, is substantially harder to discredit than one that ignores those vulnerabilities. This section should be read alongside any legal, political, or academic challenge filed against this framework.

10.1 Allied Fracture Risk

FAULT LINE: The coalition required to make technology denial and financial integrity enforcement effective — primarily Netherlands, Japan, South Korea, Taiwan — is simultaneously subject to U.S. trade friction that conflicts with the coordination ask. No allied government will sustain coordination on technology denial while absorbing unreciprocated tariff exposure.

HOW THIS ARCHITECTURE ADDRESSES IT: The framework explicitly identifies allied coherence review as a required gate for Tier 2+ measures. The live contradiction between technology-denial coordination and simultaneous trade friction is acknowledged as the largest implementation gap between framework design and current execution environment. The framework recommends resolving this contradiction — not papering over it — before escalating to Tier 2.

RESIDUAL RISK

- Any version of this framework that does not address the trade-friction contradiction will produce nominal allied compliance and actual defection at the moment of greatest pressure. Name the contradiction publicly and resolve it structurally.
- Secondary sanctions on third-country entities without allied concurrence generate the exact fracture this pillar is designed to prevent.

10.2 Blowback and Inflation Risk

FAULT LINE: PRC countermeasures — rare earth export restrictions, critical mineral market manipulation, market access retaliation against U.S. exporters — impose domestic costs that create political pressure for reversal before the framework's compounding logic has operated for a sufficient period.

HOW THIS ARCHITECTURE ADDRESSES IT: The resilience pillar (Pillar 5) is the enabling condition for all other pillars precisely because this risk is real. Supply chain diversification, strategic reserve investment, and economic adjustment assistance for exposed sectors reduce the leverage that countermeasures would otherwise provide. The framework cannot be sustained without the resilience investment.

RESIDUAL RISK

- Rare earth export restrictions remain the PRC countermeasure with the greatest short-term domestic impact. U.S. strategic reserve and allied diversification investment is materially insufficient as of the paper's writing. This is the largest unaddressed vulnerability in the framework.
- Pharmaceutical API concentration (particularly penicillin and key antibiotic starting materials) is a documented vulnerability. Strategic reserve and domestic production investment requires sustained appropriations discipline across administration transitions.

10.3 Accelerated Substitution Risk

FAULT LINE: Sustained technology denial accelerates PRC domestic development of the denied technologies. Semiconductor denial has demonstrably accelerated SMIC, Huawei HiSilicon, and broader PRC chip design and fabrication investment. The window in which denial is effective may be shorter than the political will required to maintain it.

HOW THIS ARCHITECTURE ADDRESSES IT: The framework does not assume that denial is permanent — it assumes that denial buys time for allied resilience, partner capability development, and deterrence architecture investment to reduce the strategic importance of the denied technologies to PRC military capability. Time-buying is valuable even if denial eventually fails. Document the denial window explicitly and invest in parallel tracks that reduce dependence on denial as the sole mechanism.

RESIDUAL RISK

- If denial investment does not produce allied technological advantage within the denial window, the framework produces cost without strategic benefit. Allied advanced computing and AI capability investment must be treated as the other half of the technology denial pillar.
- Denial of equipment while tolerating continued sale of chip designs creates a logical gap that adversaries exploit. Ensure consistency across the control architecture.

10.4 Escalation and Countermeasure Risk

FAULT LINE: PRC cyber infrastructure targeting of U.S. critical infrastructure (documented in Volt Typhoon CISA/NSA/FBI assessment) represents a pre-positioned retaliatory capability that could be activated in response to Tier 2+ measures. Rare earth and critical mineral market manipulation is the economic equivalent.

HOW THIS ARCHITECTURE ADDRESSES IT: The stability architecture (Section 7) is the primary procedural response: crisis communications infrastructure, published off-ramps, and guardrail-index pause triggers before Tier 3 initiation. Defensive cyber hardening is a Tier 0 baseline measure — it does not wait for escalation. The framework does not eliminate escalation risk; it reduces miscalculation-driven escalation by ensuring that PRC decision-makers have both cost information and a clear off-ramp at every tier.

RESIDUAL RISK

- Pre-positioned cyber capabilities in U.S. critical infrastructure (Volt Typhoon) represent a deterrence-by-punishment capability that operates asymmetrically. Defensive hardening is necessary but not sufficient. Acknowledge this asymmetry explicitly.
- Any Tier 3 measure that does not include a simultaneously published off-ramp removes the off-ramp from PRC cost-benefit calculation and increases the probability of countermeasure activation.

10.5 Legitimacy and Credibility Risk (Information Pillar)

FAULT LINE: The information pillar's effectiveness depends entirely on its rule-of-law credibility. Any use of deceptive content, manufactured attribution, or covert influence operations — even if discovered years later — retroactively destroys the credibility of all accurate information produced by the same infrastructure.

HOW THIS ARCHITECTURE ADDRESSES IT: The information rail in Section 2.5 prohibits deceptive content categorically. The drafting rule applies to all instruments under this pillar: every attribution must be accurate, every document must be attributable, every supporting organization must operate within rule-of-law frameworks. The pillar's value is zero if its credibility is compromised.

RESIDUAL RISK

- Covert influence operations, even if successful short-term, create the exact legitimacy deficit they are designed to exploit in PRC information operations. Do not use them.
- Exposure of PRC elite offshore assets requires confirmed-attribution standard before public release. Premature or inaccurate exposure generates defamation exposure, diplomatic friction, and — most importantly — discrediting of the broader transparency architecture.

10.6 Legal and Administrative Record Risk

FAULT LINE: Arbitrary, poorly documented, or viewpoint-motivated designations and enforcement actions generate legal reversals, create adverse precedent that constrains future legitimate action, and — at political level — discredit the framework as weaponized rather than evidence-based.

HOW THIS ARCHITECTURE ADDRESSES IT: The neutral designation-selection rule (Section 5) and the standards-of-proof framework (Section 4) are the primary procedural defenses. Every designation is preceded by a documented evidentiary record, a prohibited-factor confirmation, and a selection log entry.

The designation-selection log is the primary defense exhibit in any selective-enforcement challenge. Courts that review these records and find documented neutral methodology sustain the designation. Courts that find no record enjoin it.

RESIDUAL RISK

- The selection log must be maintained contemporaneously — not reconstructed after challenge. Reconstructed records do not survive discovery.
- Any expansion of the prohibited-factor list — specifically, any move toward treating national origin or ethnicity as a designation trigger — converts evidence-based enforcement into collective punishment and produces the exact legal and coalition vulnerability the framework is designed to prevent.

SECTION 11: CONCLUSIONS

The architecture presented in this paper delivers the maximum lawful competitive pressure available against PRC coercive capacity, technology acquisition, and transnational influence operations under existing U.S. statutory authority and multilateral frameworks. It achieves this not by overstating authority, but by deploying every available instrument precisely, procedurally, and in a sequence that builds an evidentiary and policy record that supports escalation while maintaining reversibility.

The five-pillar architecture is designed so that each pillar operates independently. Legal challenge, political constraint, or coalition friction affecting one pillar does not disable the others. The tiered escalation ladder ensures that every action is grounded in a documented evidentiary record rather than credible concern alone. The stability architecture ensures that pressure is accompanied by published off-ramps and procedural pause triggers that reduce miscalculation risk. The neutral designation-selection rule and standards-of-proof framework ensure that every action can be defended on its evidentiary merits rather than its political rationale.

The most important principle this paper advances is the distinction between conduct and identity. Every pressure mechanism in this architecture targets documented acts — enabling conduct, illicit facilitation, military-relevant technology acquisition — not political positions, national origin, or ethnic identity. This distinction is not a concession to critics of competitive statecraft. It is the reason this architecture sustains legal, coalition, and public credibility while broader postures that ignore this distinction do not.

SUMMARY: THE FIVE INDEPENDENT PILLARS

- Pillar 1: Economic Performance Constraint — coordinated technology denial, evidence-gated secondary exposure, entity-specific export control targeting.
- Pillar 2: Information Control Disruption — circumvention infrastructure, open-source transparency, independent journalism, FARA enforcement against documented influence operations.
- Pillar 3: Military Readiness Uncertainty — technology denial targeting military-relevant AI and advanced computing; allied capability demonstration.

- Pillar 4: Deterrence Architecture — Taiwan asymmetric defense acceleration; AUKUS/Japan/Philippines deterrence stack; incident-management protocols.
- Pillar 5: Allied and Domestic Resilience — supply chain hardening; critical mineral diversification; counterintelligence expansion; economic adjustment for exposed sectors.

Prepared by:
Center for Competitive Statecraft and Strategic Policy
Independent Policy Research Division

Working Paper WP-2026-PERSIST-01 | March 2026

APPENDIX A: TOOL-BY-TOOL AUTHORITY MAPPING

This appendix maps each principal instrument in the PERSIST framework to its governing authority, the evidentiary threshold required (both the statutory minimum and the framework's voluntary durability standard), the hard limits that constrain its use, the required record artifacts, and the off-ramp criteria. It is the operational equivalent of the program-by-program grant authority mapping in WP-2026-IMMPOL-04. A sophisticated reader or implementing official should be able to determine from this table, for any proposed action: what authority governs it, what record is required, and what the limits are.

APPENDIX A — TOOL-BY-TOOL AUTHORITY MAPPING

Instrument	Governing Authority	Evidentiary Threshold (Statutory Min / Framework Standard)	Hard Limits	Required Record	Off-Ramp / Reversal
Entity List Addition	ECRA § 1754(c); 15 C.F.R. § 744.11	Reasonable cause to believe the entity is involved in activities contrary to U.S. national security or foreign policy (statutory minimum). This framework voluntarily applies confirmed-attribution standard as durability rule.	APA arbitrary-and-capricious review of administrative record; due process notice-and-response process (Entity List respondent may submit a request for removal).	BIS evidentiary memorandum documenting the factual basis; legal review; interagency concurrence. Confirm no prohibited selection factor. Document off-ramp criteria in selection log.	Delisting upon demonstrated change in conduct; BIS administrative review of removal request; multilateral coordination where entity is subject to parallel allied controls.
SDN Designation (OFAC)	IEEPA (50 U.S.C. §§ 1701–1708); applicable Executive Order	Nexus between designated conduct and declared national emergency. This framework applies material-enabling-behavior standard (Section 4) as durability rule.	IEEPA nexus requirement is a hard limit. Designations without documented emergency nexus are subject to reversal. Administrative process: OFAC administrative reconsideration; judicial review under APA.	OFAC evidentiary file; legal review; interagency coordination record; Coalition-Risk Review Memo (Tier 2). Due process: publish designation with factual basis; administrative reconsideration pathway available.	OFAC administrative delisting upon verified cessation of designated conduct; submission of delisting petition; allied coalition concurrence at Tier 2+.
Sectoral Sanctions	IEEPA; applicable	Conduct within designated	Sector-wide designations	Sector-definition memorandum	Sector redefinition or

	Executive Order (e.g., E.O. 13959 series for military-civil fusion entities)	sector meeting the Executive Order's criteria; documented nexus to military-civil fusion or relevant program.	that do not individually document nexus for each covered entity create elevated reversal risk. Overbroad sectoral coverage is a hard limit when APA review requires individualized nexus.	documenting the nexus for each entity category; legal review; Coalition-Risk Review Memo at Tier 2.	removal of individual entities upon verified cessation of qualifying conduct or structural separation from qualifying activities.
Foreign Direct Product Rule (FDPR) Extension	EAR 15 C.F.R. § 734.9; ECRA authority	Items produced using U.S. technology, software, or equipment; use for military end-use or by designated entity; bilateral nexus to U.S.-origin items meeting applicable thresholds.	FDPR extraterritoriality is bounded by bilateral jurisdictional predicates — items must contain qualifying U.S.-origin content. Unilateral application beyond these predicates generates WTO and diplomatic exposure. This is a hard structural limit.	FDPR memorandum documenting item-level nexus; bilateral consultation record with affected third-country allies; BIS legal review of jurisdictional predicate.	FDPR rescission upon removal of designated entity from Entity List or verified cessation of qualifying end-use.
CFIUS Mitigation / Block	FIRRMA (50 U.S.C. § 4565); 31 C.F.R. Part 800	Covered transaction involving U.S. critical technology, critical infrastructure, or sensitive personal data; credible threat to national security that cannot be mitigated by conditions short of prohibition.	CFIUS jurisdiction is bounded by FIRRMA covered-transaction definitions. Transactions outside those definitions require new legislation. Mitigation agreements must be proportionate; overbroad prohibitions create WTO and treaty exposure.	CFIUS administrative record; national security risk assessment; legal review of jurisdictional basis; written findings and mitigation terms or prohibition order.	Mitigation agreement modification upon verified compliance and changed risk assessment; withdrawal of prohibition if jurisdictional basis changes.
Outbound Investment	E.O. 14105 (Aug. 9,	Covered transaction by	Outbound screening	Treasury determination	Regulatory revision upon

Restriction	2023); implementing Treasury regulations	U.S. person involving national security technology or product sectors in PRC as defined in applicable regulations.	authority is more legally contested than CFIUS inbound authority. E.O. 14105 is the current operative authority; its scope is subject to judicial and congressional challenge. Document authority basis for each covered-sector determination explicitly.	memorandum; legal review of covered-transaction definition; public comment record where applicable.	congressional authorization or changed risk assessment in covered sectors.
FARA Enforcement Action	22 U.S.C. §§ 611–621; DOJ NSD implementing authority	Person acting as agent of foreign principal within the United States; failure to register or file required disclosures; conduct meets FARA statutory elements (agency relationship, foreign principal nexus, covered activities).	FARA enforcement must be conduct-based and viewpoint-neutral. This is a hard limit: enforcement based on political positions or advocacy rather than failure to register converts legitimate enforcement into viewpoint discrimination under the First Amendment.	DOJ investigative record documenting agency relationship and failure to register; legal review confirming element fit; neutral selection log confirmation of no viewpoint-based trigger.	Registration compliance; enforcement action closed upon full compliance with disclosure requirements.
Defense Cooperation / Arms Transfer	AECA (22 U.S.C. § 2751 et seq.); FMS / DCS authorities; ITAR (22 C.F.R. Parts 120–130)	Recipient eligibility; end-use certification; congressional notification for transfers above statutory thresholds; Leahy Law vetting for security force assistance.	Congressional notification requirements are mandatory above dollar thresholds. Failure to comply generates statutory and political vulnerability. Leahy Law vetting is a hard limit for security force assistance —	Congressional notification filings; end-use monitoring plan; Leahy Law vetting record; documented policy rationale for prioritization decisions.	N/A — arms transfers are affirmative approvals, not pressure measures subject to suspension. Sustainment and follow-on sales may be conditioned on continued end-use compliance.

			violations generate congressional and judicial exposure.		

APPENDIX A — READING NOTE

Column 3 (Evidentiary Threshold) distinguishes the statutory minimum from the standard this framework voluntarily applies. Where the framework's standard is higher than the statutory minimum, the higher standard is a durability rule — it is not legally required, but it is what makes actions more resistant to reversal and adverse precedent. Implementing officials may not lower the framework standard without a documented waiver and senior-official authorization.

- Column 4 (Hard Limits) identifies structural constraints that cannot be addressed by drafting improvement. A hard limit means the instrument cannot be used for the described purpose regardless of how the action is framed. Attempting to circumvent a hard limit through creative framing produces the exact adverse precedent the framework is designed to prevent.

APPENDIX B: MODEL RECORD ARTIFACTS

The following four model memoranda are the required record artifacts for the principal action categories under this framework. They are not optional. Each action at Tier 2 and above requires the completion of the applicable memorandum before the action proceeds. The memos are designed to be litigation-ready: they document the evidentiary basis, the authority rail, the prohibited-factor confirmation, the coalition coordination record, and the off-ramp criteria in a single instrument. A record that cannot be produced in this format did not meet the requirements of this framework before the action was taken.

B.1 Designation Memorandum (Entity List / SDN)

MODEL: DESIGNATION MEMORANDUM	
TO:	*[Reviewing Authority / Senior Official]*
FROM:	*[Selecting Official / Agency]*
DATE:	*[Date of Memorandum]*
RE:	Proposed [Entity List Addition / SDN Designation] — [Entity Name]
AUTHORITY RAIL:	*[ECRA / IEEPA / applicable Executive Order — cite Section 2 rail]*
EVIDENTIARY BASIS:	*[State the specific objective trigger from Section 5 that has been documented. Attach supporting record.]*
FRAMEWORK STANDARD MET:	*[Confirmed Attribution / Material Enabling Behavior — state which Section 4 standard applies and why it is met]*
PROHIBITED FACTORS CONFIRMED ABSENT:	I confirm that the following factors were not considered in the targeting decision: national origin, ethnicity, or nationality of beneficial owners absent documented conduct; political statements or advocacy; participation in litigation challenging U.S. government action; any viewpoint-related factor. [Selecting Official Signature]
COALITION COORDINATION:	*[State whether Coalition-Risk Review Memo has been completed. If Tier 2, attach completed memo. If Tier 1, state basis for determination that coalition-risk review is not required.]*
OFF-RAMP CRITERIA:	*[State specifically what verified conduct change by the entity would support delisting or removal. State whether this pathway has been communicated to the entity where legally permissible.]*
LEGAL REVIEW:	*[Confirm legal counsel review completed. Note any concerns raised and how addressed.]*
RECOMMENDATION:	*[State recommended action and any conditions or monitoring requirements.]*

B.2 Coalition-Risk Review Memorandum (Tier 2 and Above)

MODEL: COALITION-RISK REVIEW MEMORANDUM	
TO:	*[Interagency Coordinating Committee / Senior Official]*
FROM:	*[Lead Coordinating Agency]*

DATE:	*[Date of Memorandum]*
RE:	Coalition-Risk Review — [Proposed Action Description] — [Tier Level]
ALLIES CONSULTED:	*[List allied governments consulted or notified, by name. Include date of consultation and method (bilateral, multilateral, written notification).]*
U.S. AGENCIES PARTICIPATING:	*[List agencies. Confirm Assistant Secretary level or above representation for NSC, Treasury/OFAC, Commerce/BIS, and State.]*
ALLIED RESPONSES:	*[Describe each ally's response: concurrence, non-objection, conditional support, or objection. Quote or summarize written communications where available.]*
CONCURRENCE / NON-OBJECTION STANDARD MET:	*[For Tier 2: state whether non-objection from at least one primary partner is documented. For Tier 3: state whether affirmative written concurrence from at least two primary partners is documented.]*
RECORDED DISSENT:	*[If any ally raised a formal objection: (a) state the nature of the objection; (b) state the overriding national security rationale; (c) describe mitigation offered to the objecting partner; (d) confirm 30-day review hold has been observed or emergency exception has been documented.]*
RISK ASSESSMENT:	*[Summarize coalition fracture risk, market risk, and retaliatory action risk at the proposed tier. Confirm guardrail index status for Tier 3.]*
RECOMMENDATION:	*[State whether action should proceed, proceed with modifications, or be deferred pending further consultation.]*

B.3 Delisting / Off-Ramp Memorandum

MODEL: DELISTING / OFF-RAMP MEMORANDUM	
TO:	*[Reviewing Authority / Senior Official]*
FROM:	*[Selecting Official / Agency]*
DATE:	*[Date of Memorandum]*
RE:	Proposed Delisting / Suspension — [Entity Name] — [Original Designation Date and Reference]
ORIGINAL DESIGNATION BASIS:	*[State the evidentiary basis for the original designation, by reference to the original Designation Memorandum.]*
OFF-RAMP CRITERIA MET:	*[State specifically which off-ramp criteria from the original Designation Memorandum have been satisfied. Describe the verification method: allied assessment, financial intelligence, independent audit, or other.]*
VERIFICATION RECORD:	*[Describe the specific evidence confirming conduct cessation or behavior change. Attach supporting record.]*
ALLIED COORDINATION:	*[State whether allied partners have been notified and whether their concurrence is required at the applicable tier. Document responses.]*
RESIDUAL RISK ASSESSMENT:	*[State any residual risk that the conduct may resume and what monitoring or conditions are recommended post-delisting.]*
RECOMMENDATION:	*[State recommended action: full delisting, partial delisting with conditions, suspension pending verification, or continued designation with updated*

	evidentiary basis.]

B.4 Guardrail Override Memorandum (Tier 3)

MODEL: GUARDRAIL OVERRIDE MEMORANDUM	
TO:	*[Interagency Coordinating Committee / Senior Official — Assistant Secretary Level or Above]*
FROM:	*[Lead Coordinating Agency]*
DATE:	*[Date of Memorandum]*
RE:	Guardrail Override Authorization — [Proposed Tier 3 Action] — [Relevant Guardrail Indicator]
GUARDRAIL INDICATOR IN RED ZONE:	*[Identify which of the four guardrail indicators (A/B/C/D) is in red zone and the current reading that triggered the presumptive pause.]*
PROPOSED ACTION:	*[Describe the specific Tier 3 action proposed to proceed despite the red-zone indicator.]*
RATIONALE FOR OVERRIDE:	*[State specifically why the proposed Tier 3 action is warranted despite the red-zone indicator. This rationale must address: (a) why the national security benefit of proceeding outweighs the systemic risk signaled by the indicator; (b) what evidence supports the conclusion that the indicator reading does not reflect an imminent escalation risk in the relevant dimension; and (c) what makes the indicator reading addressable or manageable in the context of the proposed action.]*
RISK MITIGATION MEASURES:	*[Describe specific risk-mitigation measures in place or proposed to address the systemic risk flagged by the indicator. Include stabilization measures, allied coordination steps, and contingency plans if the risk materializes.]*
SENIOR OFFICIAL AUTHORIZATION:	*[Name and title of the senior official authorizing the override. Signature required. Override cannot be authorized below the Under Secretary level for IEEPA-based Tier 3 actions.]*
RETENTION NOTE:	This memorandum is retained as part of the administrative record for the proposed Tier 3 action. Proceeding with Tier 3 action without a completed and signed override memorandum when a guardrail indicator is in red zone is a procedural violation under this framework.

Prepared by:
Center for Competitive Statecraft and Strategic Policy | Independent Policy Research Division
WP-2026-PERSIST-01 | March 2026 | Appendix B