Janus Protocol Risk Register & Operational Playbook (SDAM-CMRA)

Purpose: This playbook documents the high-severity adversarial risks to the Janus Protocol's physical assets (SDC concessions) and financial integrity (Treasury) and defines the **Standard Operating Procedures (SOPs)** for the **Structural Dispute Adjudication Mechanism (SDAM)** and **Consortium Market Recognition Agreement (CMRA)** signatories to execute counter-coercion.

I. Kinetic / Sovereign Coercion Threats (Physical Enforcement)

Risk Category	Adversarial Action (Threat)	Structural Countermeasure	SDAM/CMRA SOP & Response Flow
A. Asset Seizure	State/Municipality uses police power or eminent domain to physically seize the SDC-conceded asset (e.g., occupies the Code-Toll booth, redirects revenue).	**Structural Credit Blockade (SCB)** enforced by the CMRA network.	**SOP K.1 (Kinetic Response):** 1. SDAM Oracle confirms physical seizure (Satellite/Telemetry failure). 2. SDAM Arbiters trigger **Provisional Solvency Warning** (72-hour hold). 3. Legal team files immediate injunction in international arbitration (London LCIA). 4. If hold expires, Warning is confirmed: **CMRA signatories immediately execute contractual credit withdrawal (SCB).**
B. Ban/Criminalization	State passes emergency legislation criminalizing the Code-Toll mechanism or SMT ownership.	**Financial Parasitism & Economic Leverage.**	**SOP K.2 (Legal/Political Response):** 1. Legal team secures an immediate stay based on the SDC's binding international arbitration clause. 2. Code-Corps (logistics, finance) publicly issue statements detailing the catastrophic economic

Risk Category	Adversarial Action (Threat)	Structural Countermeasure	SDAM/CMRA SOP & Response Flow
			costs of non-compliance (e.g., "40% of state freight stops moving"). 3. CMRA banks privately signal the credit consequences to the legislative opposition.
C. Sensor/Oracle Disruption	State forces local utilities to cut power or jam GPS/5G to disrupt tolling sensors and SDAM monitoring.	**Multi-Source Redundancy & Private Networks.**	**SOP K.3 (Operational Continuity):** 1. Automated switch to Starlink/Iridium backup comms. 2. **Warning Trigger:** If telemetry fails for >6 hours, SDAM issues a **"Structural Violation Warning,"** increasing the State's actuarial risk rate on the IAL (precursor to SCB). 3. DRT deploys decentralized power backups (solar/battery redundancy) to the toll points.

II. Code / Protocol Integrity Threats (Technical & Governance)

Risk Category	Adversarial Action (Threat)	Structural Countermeasure	SDAM/CMRA SOP & Response Flow
D. Hostile Fork	A major political faction sponsors a competing fork of the protocol, attempting to seize treasury control.	**Fork Futility Clause** & **Constitutional Consensus Majority (CCM).**	**SOP C.1 (Fork Response):** 1. SDAM monitors the competing chain for **98% usage shortfall**. 2. If the competing chain fails to achieve 98% usage within 30 days, SDAM executes the **Treasury Burn Protocol** on the hostile chain's treasury address, rendering the attack financially catastrophic for the sponsors. 3. CMRA

Risk Category	Adversarial Action (Threat)	Structural Countermeasure	SDAM/CMRA SOP & Response Flow
			signatories issue public advisories affirming allegiance to the original chain.
E. Oracle Manipulation	Malicious actor feeds false data (e.g., fakes a low PCI score) to crash SMT prices or trigger SCB.	**Multi-Source Oracle Architecture (MSOA).**	**SOP C.2 (Data Integrity):** 1. Any Warning requires **Consensus Trigger:** Agreement between the Technical Data Feed (IAL), the Physical Data Feed (Satellite/Local Inspector), and the Legal Status Feed (Court Registry). 2. If consensus fails, the Arbiters rule a **No-Action Consensus.** 3. Any single data feed being compromised (e.g., a known bad inspector report) is disregarded until ratified by the other two sources.

III. Financial / Economic Threats

Risk Category	Adversarial Action (Threat)	Structural Countermeasure	SDAM/CMRA SOP & Response Flow
F. Financial Contagion	Failure of an early SDC pilot causes market panic, triggering a widespread run on SMTs and the main Janus Treasury.	**Tiered Reinsurance Layers & UPCC Covenants.**	**SOP F.1 (Contagion Management):** 1. **Code-Guaranteed Resilience:** The **UPCC** ensures all asset revenue is immediately directed to maintenance first, protecting the physical asset's value. 2. **CMRA Coordination:** Reinsurer CMs activate the pre-funded **Stabilization Reserve Pool** to underwrite

Risk Category	Adversarial Action (Threat)	Structural Countermeasure	SDAM/CMRA SOP & Response Flow
			SMT liquidity, preventing a systemic run. 3. DRT publishes real-time asset PCI scores, proving the physical asset is secure, regardless of market sentiment.
G. Predatory SMT Capture	A single hedge fund accumulates >50\% of SMTs in a region to demand excessive dividends or control.	**SMT Governance Caps & UPCC.**	**SOP F.2 (Anti-Plutocracy):** 1. DRT governance is capped: no single entity may cast more than **15% of the Usage-Weighted Vote,** regardless of SMT holding. 2. **Profit Ceiling:** The UPCC waterfall includes a provision capping SMT profits at X \% over a risk-free rate, forcing capital to be reinvested into other distressed SDC assets rather than extracted.