



Comprehensive US Legal & Trade Compliance Governance Policy

GI Corporation

Effective Date: January 01, 2026

1. Message from the Chief Executive Officer

At GI Corporation, our leadership in the aerospace, defense, software, and manufacturing sectors relies entirely on our unwavering commitment to regulatory compliance, national security, and fundamental human rights. Because we develop and distribute critical technologies, our global operations are strictly governed by United States law. This document is a holistic, self-contained, and strictly enforceable policy that dictates our exact operational procedures regarding US export controls, economic sanctions, human rights legislation, anti-corruption laws, and supply chain integrity. We do not compromise our regulatory obligations for commercial gain. Strict, documented adherence to US legal frameworks is a non-negotiable condition of employment and partnership with GI Corporation.

2. Jurisdictional Scope & Applicability

This policy governs all GI Corporation global operations and establishes our compliance baseline under United States federal law.

- **Global Applicability:** This policy applies to all GI Corporation subsidiaries, executives, directors, employees, and contractors worldwide. US laws often carry extraterritorial jurisdiction; therefore, this policy applies regardless of where a transaction physically occurs.
- **US Persons & Technology:** This policy strictly governs the conduct of all "US Persons" (citizens, green card holders, and entities organized under US law) anywhere in the world, as well as foreign persons dealing with US-origin goods, software, technology, or utilizing the US financial system.
- **Supply Chain Extension:** All vendors, distributors, and third-party intermediaries must certify compliance with US export, anti-corruption, and human rights laws as a condition of receiving a GI Corporation vendor number.

3. OFAC Sanctions & Economic Embargoes

GI Corporation strictly complies with all economic and trade sanctions administered by the **US Department of the Treasury's Office of Foreign Assets Control (OFAC)**. We do not conduct unauthorized business with comprehensively embargoed countries, regions, or restricted parties.

- **Screening Protocol:** We systematically screen all clients, suppliers, financial institutions, and end-users against the OFAC Specially Designated Nationals (SDN) list and Sectoral Sanctions Identifications (SSI) list.

- *Actionable Protocol:* We utilize automated screening software that runs daily batch checks against the consolidated US government screening lists.
- *The OFAC 50% Rule:* Our Due Diligence team must independently verify ownership structures. If an entity is not explicitly on the SDN list but is 50% or more owned, directly or indirectly, by one or more blocked persons, the entity is automatically treated as a blocked party.
- **Geographic Embargoes:** GI Corporation prohibits all business dealings involving comprehensively embargoed jurisdictions (e.g., Iran, North Korea, Syria, Cuba, and specific regions of Ukraine/Russia, subject to real-time OFAC updates).
 - *Actionable Protocol:* Our IT and Software divisions must maintain automated IP-blocking protocols to prevent the downloading of our software, or access to our cloud portals, from any IP address originating in an OFAC-embargoed jurisdiction.
- **Hit Resolution:** * *Actionable Protocol:* Any positive or ambiguous hit in our screening software places an automatic financial and logistical freeze on the transaction. The Global Trade Compliance (GTC) department has 48 hours to manually clear the false positive or formally block and report the entity to OFAC.

4. ITAR & EAR Export Controls

As a manufacturer of aerospace and defense technologies, our hardware, software, and technical data are heavily regulated by the **International Traffic in Arms Regulations (ITAR)** administered by the Directorate of Defense Trade Controls (DDTC), and the **Export Administration Regulations (EAR)** administered by the Bureau of Industry and Security (BIS).

- **Product Classification Protocol:** * *Actionable Protocol:* Before any item is marketed or sold, the GTC engineering liaison must formally classify the item, assigning either a United States Munitions List (USML) category or an Export Control Classification Number (ECCN).
- **Licensing & End-User Verification:** We do not export US-origin items without verified authorization.
 - *Actionable Protocol:* Sales teams must secure a signed End-User Statement (EUS) detailing the exact end-use and end-user for all international transactions. The Logistics Department is strictly prohibited from releasing shipments to freight forwarders without a formally documented DDTC license, BIS license, or a formally recorded license exception/exemption.
- **Deemed Exports & Technology Control:** Under US law, releasing controlled technical data to a foreign national *within* the United States is deemed an export to that person's home country.
 - *Actionable Protocol:* HR and GTC must conduct an I-129 deemed export assessment for every foreign national employee prior to onboarding.

- *Actionable Protocol:* Facilities housing ITAR-controlled technical data must implement strict Technology Control Plans (TCPs), utilizing badge-restricted physical access zones and partitioned, encrypted servers limited strictly to authorized US Persons.

5. Foreign Corrupt Practices Act (FCPA) Compliance

GI Corporation strictly complies with the **Foreign Corrupt Practices Act (FCPA)**, which prohibits offering, paying, or authorizing the payment of money or anything of value to a foreign government official to obtain or retain business.

- **Anti-Bribery Protocol:** Employees and third-party representatives are strictly forbidden from offering bribes, kickbacks, or facilitation payments (grease payments), even if such payments are customary in the local jurisdiction.
- **Gifts, Meals, and Entertainment:**
 - *Actionable Protocol:* Employees may not spend more than \$50 USD on nominal gifts or meals for any foreign official without express, pre-approved written authorization from the Chief Compliance Officer.
- **Books and Records Provision:** The FCPA requires GI Corporation to keep meticulously detailed and accurate financial records.
 - *Actionable Protocol:* All expenses must be recorded exactly as they occurred with corresponding receipts. Disguising a bribe or inappropriate gift under categories like "marketing expenses" or "consulting fees" is a severe federal crime and will result in immediate termination.
- **Third-Party Intermediaries:** * *Actionable Protocol:* Because GI Corporation can be held strictly liable under the FCPA for the actions of third-party agents, all international sales representatives, brokers, and customs clearing agents must undergo a rigorous, DOJ-aligned FCPA background check and sign specific anti-corruption certifications before acting on our behalf.

6. Human Rights & Ethical Technology Export

GI Corporation aligns its operations with US foreign policy objectives prioritizing human rights. We strictly comply with the **Global Magnitsky Human Rights Accountability Act** and **BIS regulations** restricting exports to entities implicated in human rights abuses.

- **Global Magnitsky Sanctions Screening:**
 - *Actionable Protocol:* Our automated screening software must specifically flag individuals or entities designated under the Global Magnitsky Act (tagged [GLOMAG] on the SDN list). Any attempt by a foreign entity to utilize GI Corporation funds or technology to facilitate human rights abuses will result in an immediate block and a mandatory report to the US Treasury Department.

- **Preventing Tech-Enabled Internal Repression:** US export laws (EAR) restrict the export of certain items if there is a risk they will be used for human rights violations, such as mass surveillance, biometric tracking, or arbitrary detention.
 - *Actionable Protocol:* Before exporting advanced software, facial recognition technology, or surveillance-capable hardware, the Sales and GTC teams must execute a "Human Rights End-Use Assessment." If the end-user is a foreign police, military, or intelligence agency with a documented history of civil rights abuses (as verified by the US State Department's annual Country Reports on Human Rights Practices), the transaction must be denied, regardless of whether a specific export license could theoretically be obtained.
- **Combating Trafficking in Persons:** In strict adherence to the **Trafficking Victims Protection Act (TVPA)** and **FAR 52.222-50**, GI Corporation maintains a zero-tolerance policy regarding forced labor, debt bondage, and human trafficking.
 - *Actionable Protocol:* All GI Corporation facilities and Tier-1 suppliers must post the US National Human Trafficking Hotline number in workspaces.
 - *Actionable Protocol:* Human Resources and Procurement must enforce a strict "Employer Pays" principle. We forbid GI Corporation entities and external suppliers from charging recruitment fees to workers, destroying or confiscating identity documents (passports, driver's licenses), or utilizing misleading recruitment practices.

7. Supply Chain Integrity & Forced Labor Prevention

GI Corporation operates in strict compliance with US federal mandates regarding ethical sourcing, specifically the **Uyghur Forced Labor Prevention Act (UFLPA)**.

- **UFLPA Compliance:** US law establishes a rebuttable presumption that any goods mined, produced, or manufactured wholly or in part in the Xinjiang Uyghur Autonomous Region (XUAR) of China are produced with forced labor and are barred from entering the United States.
 - *Actionable Protocol:* Procurement teams must map our supply chain down to Tier-3 raw material suppliers. Any vendor sourcing polysilicon, aluminum, or other high-risk materials must provide certified, traceable bills of material proving the origin of the inputs are entirely outside the XUAR.
- **Supplier Enforcement:**
 - *Actionable Protocol:* Suppliers who fail to provide transparent supply chain mapping, or who are found violating US labor and trafficking laws, will have their contracts immediately terminated, be placed on our internal denied-parties list, and be reported to US Customs and Border Protection (CBP).

8. Internal Governance & Empowered Officials



Decisions regarding controlled technologies and federal contracting involve severe legal risks and require structural oversight.

- **Empowered Officials (EO):** * *Actionable Protocol:* In accordance with the ITAR, GI Corporation has designated specific executive "Empowered Officials" who are US Persons legally authorized to sign license applications. Only an EO has the authority to inquire with the State Department regarding defense trade issues.
- **Cross-Functional Veto Power:** * *Actionable Protocol:* All international contracts exceeding \$1 Million, or any contract involving USML hardware/software, must be reviewed by the Legal, Risk, and GTC departments. Any of these three departments holds unilateral authority to halt a transaction if it presents an unmitigated US regulatory or human rights risk.

9. Whistleblower Protection & Reporting Channels

In alignment with the Sarbanes-Oxley Act (SOX), the Dodd-Frank Act, and Department of Justice Corporate Enforcement guidelines, GI Corporation requires the immediate reporting of any suspected federal law violations.

- **Actionable Reporting Protocols:**
 - *Direct Escalation:* Employees must report FCPA, OFAC, Human Rights, or Export Control violations immediately to the Global Chief Compliance Officer at compliance@gicorp.com.
- **Investigation & Disclosure Protocol:**
 - *Actionable Protocol:* The Legal Department triages all reports within 48 hours. If an investigation substantiates a violation of ITAR, EAR, OFAC, or FCPA regulations, GI Corporation's strict policy is to draft and submit a Voluntary Self-Disclosure (VSD) to the appropriate US federal agency to mitigate corporate liability.
- **Strict Non-Retaliation (Zero Tolerance):** * *Actionable Protocol:* GI Corporation absolutely prohibits any retaliation or adverse employment action against anyone reporting a concern in good faith. Under federal whistleblower protections, managers found retaliating against employees will face immediate termination and potential civil liability.