Humanoid Industrial Security & Standards Initiative (HISSI)

Protecting America's Future in Defense Robotics and AI Manufacturing

Executive Summary — Policy Brief, October 2025

Overview

As China dominates over 50% of global robotics production and critical materials, the U.S. faces urgent risks in its defense supply chain. Humanoid robotics are transitioning from experimental platforms to mission-critical assets for logistics, maintenance, humanitarian operations, and eventually combat support within 5–10 years. Yet most precision components, sensors, and AI compute modules are sourced from globally distributed suppliers—some in adversarial nations. Without a secure, on-shore or allied manufacturing base, the U.S. risks strategic dependence, sabotage, and loss of operational control.

Mission

Establish the Humanoid Industrial Security & Standards Initiative (HISSI) to ensure every humanoid system integrated into U.S. or allied defense is:

1. Manufactured within trusted facilities inside the U.S. or allied nations.
2. Architected with modular open interfaces that enable inspection and rapid patching.
3. Certified for secure AI and firmware provenance. HISSI upholds an ethical commitment to "do no harm," ensuring systems protect lives without introducing vulnerabilities that could endanger U.S. or allied forces.

Strategic Goals

1. Trusted Components & Manufacturing	Extend DoDI 5200.44 to define Humanoid Critical Components (HCCs)—actuators, powertrains, AI SoCs, comms modules—requiring Trusted Supplier Certification.	OUSD(A&S), DoD CIO
2. Domestic & Allied Capacity	Incentivize domestic production using CHIPS-style grants and tax credits; establish Allied Co-Production Agreements with Japan, South Korea, NATO partners.	DoD, DoC, State

3. MOSA-H Architecture Standard	Publish a Modular Open Systems Approach for Humanoids (MOSA-H) to enforce open interfaces, signed firmware, and cybersecurity compliance.	OUSD(R&E), NIST, DARPA
4. Certification & Testing	Create the Humanoid Test & Evaluation Center (HTEC) for red-team validation, firmware signing audits, and end-to-end C-SCRM testing.	DARPA, Army Futures Command

Implementation Roadmap

I — Foundation	2025–2026	Publish HISSI charter; define HCC registry; form MOSA-H working group.
II — Pilot Programs	2027–2028	Launch trusted manufacturing hubs; initiate HTEC testing; begin incentive grants.
III — Fielding & Certification	2029–2031	Require MOSA-H compliance in contracts; deploy DoD-certified logistics humanoids.
IV — Full Operationalization	2032–2035	Expand allied production; certify combat-support variants; continuous C-SCRM audits.

Budget & Economic Impact

- **Federal Investment**: $5–15 billion over 5 years (grants, loans, tax credits, comparable to CHIPS Act).
- **Stand-up Cost**: $300–500 million for HTEC and MOSA-H development.
- **ROI**: Creates ~40,000 high-skill manufacturing and AI jobs by 2030; secures a $50 billion domestic robotics sector.

Feasibility & Sustainability

Technically achievable using existing robotics and semiconductor toolchains. Leverage NIST SP 800-161 for supply-chain risk management and DoDI 5200.44 for trusted systems. Economically feasible with CHIPS Act-like political will; dual-use benefits offset costs. Sustainability ensured through allied co-production to diversify cost and risk.

Performance Metrics

1. ≥ 75% of HCCs domestic or ally-produced by Year 6.
2. < 24 hr firmware patch pipeline for certified humanoids.

3. ≥ 90% supplier SBOM coverage within 4 years.
4. Zero validated supply-chain compromises in certified platforms.

Legislative & Regulatory Path

- Introduce a Humanoid Security and Standards Amendment to the NDAA.
- Update ITAR and EAR to protect HCCs and signed AI stacks.
- Align Commerce and DoD grant criteria with HISSI standards.

Conclusion

The United States cannot allow the next generation of defense and industrial robotics to depend on untrusted global supply chains. HISSI provides a structured, economically viable path to secure, ethical, and sustainable humanoid manufacturing—protecting national security while accelerating innovation.

Authored by: Collin George, Independent Researcher in Computer Science, Cybersecurity, and Biomedical Innovation.