

# JOINT VENTURE CO-DEVELOPMENT AND SUPPLY CHAIN SECURITY AGREEMENT

PROJECT IRIS-AEGIS: AN EXPEDITED HIGH-SECURITY SPATIAL COMPUTING INITIATIVE

|                    |                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Effective Date:    | October 1, 2026                                                                                                                   |
| Primary Parties:   | <b>Google LLC</b> (a Delaware corporation, subsidiary of Alphabet Inc.) & <b>Apple Inc.</b> (a California corporation)            |
| Intended Audience: | Department of Defense (DoD), U.S. Securities and Exchange Commission (SEC), and Federal Trade Commission (FTC) Oversight Channels |
| Regulatory Ref:    | <b>SEC Whistleblower No. 17684-273-411-436</b> // Case No. 5:26-cv-07078-EJD (N.D. Cal.)                                          |

## RECITALS AND STATEMENTS OF NATIONAL SECURITY INTEREST

**WHEREAS**, the Parties recognize that unannounced, next-generation spatial computing technologies, including advanced augmented reality (AR) optical display hardware and micro-display specs, represent critical dual-use technologies vital to national security and information sovereignty [114]; and

**WHEREAS**, the Parties acknowledge that these foundational technologies are under active threat of systematic exfiltration by foreign-funded, capped-profit turned Public Benefit Corporation (PBC) entities—most notably OpenAI Group PBC, the OpenAI Foundation, and their hardware shell *io Products*—using C-suite-directed talent extraction campaigns and physical 'show and tell' recruiting protocols [56, 58, 60, 112, 114, 133]; and

**WHEREAS**, the active, unauthorized database intrusions executed by former employees (including Defendant Chang Liu's post-employment hacking of Apple internal network folders while operating within OpenAI's hardware division) create an immediate risk of commercial and national security spoliation [56, 59, 114]; and

**WHEREAS**, the Parties are committed to delivering an airtight, high-security spatial computing platform for the Department of Defense (DoD) that adheres to strict non-proliferation, cyber-safety, and public-integrity standards while completely shutting out compromised entities from the hardware ecosystem [207];

**NOW, THEREFORE**, in consideration of the mutual covenants contained herein, the Parties agree as follows:

## SECTION 1: PURPOSE AND PRODUCT COLLABORATION CODENAME 'IRIS-AEGIS'

The Parties hereby establish a high-security joint venture, codenamed **Project Iris-Aegis**, to co-develop, manufacture, and distribute unannounced augmented reality (AR) optical display hardware. The primary objective is to combine Cupertino's high-precision physical display blueprints, battery-assembly frameworks, and metal finishing specifications with Alphabet's secure Android XR software platform, spatial operating system, and cloud-rendering infrastructure. This unified stack will establish a closed, secure, and federally-verified spatial computing pipeline [8, 114].

## SECTION 2: COMPLETE ISOLATION AND EXCLUSION OF COMPROMISED SYSTEMS

To protect the joint venture's intellectual property and satisfy federal regulatory compliance under **SEC Whistleblower No. 17684-273-411-436**, the Parties establish a zero-tolerance exclusion mandate:

**2.1 Complete Supplier Ban:** Under no circumstances shall the JV utilize, license, or integrate any software, models, or hardware components developed by OpenAI Group PBC, the OpenAI Foundation, or Jony Ive's *io Products*. Any supplier found utilizing OpenAI APIs or hardware frameworks shall face immediate contract termination [56, 60].

**2.2 Mandatory 'Clean Room' Personnel Audits:** Every hardware designer, systems engineer, and optical specialist assigned to Project Iris-Aegis must undergo a mandatory, third-party forensic IT audit prior to onboarding. No employee possessing unreturned competitor devices, personal iCloud accounts intermingled with competitor data, or past affiliations with OpenAI's hardware division may be assigned to the JV, directly mitigating the database infiltration risk exposed in the Chang Liu and Alyssa Peng affairs [56, 59, 114].

## SECTION 3: DEPARTMENT OF DEFENSE (DoD) & PENTAGON SAFETY STANDARDS

The Parties recognize that the Department of Defense requires high-fidelity, tamper-proof spatial display hardware to support defense infrastructure. The JV stack is specifically engineered to comply with the Department of War's cyber-security mandates, resolving the vulnerabilities that recently led to the Pentagon's blacklisting of other consumer AI platforms [207]:

**3.1 Mass Surveillance & Autonomous Weapons Mitigation:** In strict alignment with civilian and national security defense boundaries, Project Iris-Aegis display hardware will operate on a hard-sandboxed operating system that completely blocks unauthorized digital telemetry, remote network scraping, or hidden data pipelines. This directly prevents the 'suicide-coach' or autonomous data-harvesting safety failures that occurred on less-regulated, commercial LLM networks [144, 207].

**3.2 Local-First Sovereign Inference:** All spatial rendering, object identification, and real-time transcription processes will execute on local, hardware-level secure enclaves embedded within Apple's custom silicon displays. This completely mitigates the 'circular' cloud spending and server-dependency risks (such as OpenAI's dependent Azure credit infrastructure) flagged by the Federal Trade Commission (FTC) [135, 207].

## SECTION 4: SUPPLY CHAIN SECURITY AND SURFACE FINISHING INTEGRITY

To prevent the supply chain espionage and anodizing spec leaks documented during the Tang Tan investigation (specifically the co-opting of mutual suppliers proven in the sworn declaration of Apple Surface Finishing Manager Jackie Hughes), the JV establishes strict supplier isolation protocols [19, 114, 324]:

**4.1 Isolated Anodizing & Finishing Lines:** All metal finishing, display-shield manufacturing, and colored back glass processing must occur on dedicated, physically isolated production lines within audited facilities. No mutual Apple-Google supplier may share metal finishing data or structural housing CAD blueprints with any third party, under penalty of immediate civil and criminal prosecution under the Defend Trade Secrets Act (DTSA) [8, 114, 324].

## SECTION 5: REGULATORY AUDITING AND PROTECTION AGAINST ADMINISTRATIVE MALFEASANCE

The Parties acknowledge that the integrity of this high-security joint venture depends on absolute transparency and the enforcement of federal whistleblower protections under **18 U.S.C. § 1836 (DTSA)** and **SEC Rule 21F-17**:

**5.1 Mandatory Whistleblower Safe Harbors:** Both Parties agree to establish a joint Independent Compliance Committee to review, investigate, and report any potential IP or financial discrepancies directly to the SEC and FTC. Any attempt by internal personnel or state-level administrative channels to suppress, mock, or alter audit files is strictly prohibited [148, 151].

**5.2 Defense of Retaliation Victims:** The JV explicitly logs and condemns the administrative retaliation executed by representatives of the **Oregon State Treasury Auditor Division**, who violated federal law by backdating system database logs to obscure the whistleblower's real-time administrative filings. The JV will provide full legal and forensic resources to defend any whistleblower subjected to such administrative harassment, specifically cooperating with the active criminal report filed with the **Washington County Sheriff's Office in Washington County, Oregon** [148, 151].

**IN WITNESS WHEREOF**, the Parties hereto have executed this Joint Venture Agreement through their authorized fiduciaries as of the Effective Date written above.

**FOR GOOGLE LLC:**

**FOR APPLE INC.:**

---

**Chief Legal Officer**  
Alphabet Inc. / Google LLC

---

**General Counsel & Senior VP**  
Apple Inc.