IRONWIFI

Capability Statement

CLOUD-NATIVE RADIUS AUTHENTICATION & WIFI IDENTITY THREAT DETECTION

COMPANY

IronWiFi, LLC — Florida, est. 2014
Martin Benuska, CEO
+1 800-963-6221
martin@ironwifi.com
ironwifi.com
100 E Pine St Ste 110, Orlando, FL 32801-2759

REGISTRATION

SAM.gov: Active
UEI: TB1XW4HNNUG9
CAGE: 21ER8
Size: Small business (NAICS 541512, $34M threshold)
Accepts: Credit cards / P-cards

CERTIFICATIONS

SOC 2 Type II — Johanson Group LLP (May 2026; unqualified opinion; Security + Availability)
HIPAA-capable contracting (BAA available)
U.S. patents pending

NAICS CODES

541512 Computer Systems Design (primary)
518210 Computing Infrastructure Providers
541519 Other Computer Related Services
541511 Custom Computer Programming
541690 Scientific & Technical Consulting

PSC CODES

DA10 IT & Telecom: Cybersecurity
DA01 IT & Telecom: SaaS Application
D399 IT & Telecom: Other IT

CONTRACT VEHICLES

SEWP / OMNIA through an approved federal reseller on named opportunities
Cisco / Oracle / AWS marketplaces
Federal Pilot: $14,400 fixed / 12 months, one site, up to 80 users or 40 guest APs, 120-day ITDR evaluation included (under the $15,000 micro-purchase threshold)
Government rates (billed annually): $15 per user per month (802.1X); $30 per access point per month (guest); WiFi ITDR $18,000 / $54,000 / $180,000 per year for 1,000 / 5,000 / 25,000 identities

IronWiFi is the cloud-native RADIUS, identity, and threat-detection layer behind enterprise WiFi — vendor-agnostic to the controller / AP OEM, serving real-time 802.1X / EAP authentication decisions at scale across multiple regions. Among the first commercial providers to apply ITDR to the 802.1X / RADIUS authentication tier.

CORE COMPETENCIES

- **Cloud-native RADIUS authentication** — 802.1X / EAP-TLS / TTLS / PEAP, vendor-agnostic to any standards-compliant controller and AP OEM (Cisco Meraki, Aruba, Juniper Mist, CommScope Ruckus).
- **WiFi identity threat detection & response (ITDR)** — multi-engine behavioral analysis of credential attacks, identity anomalies (impossible travel, endpoint anomalies), certificate and device threats (MAC spoofing, cloning, rogue devices), and AI-agent-identity drift.
- **MITRE ATT&CK-mapped detection & automated containment** — composite risk scoring; shadow / detect / enforce modes; RADIUS Change-of-Authorization (disconnect, MAC block, VLAN quarantine).
- **AI-agent identity management** — purpose-scoped X.509 provisioning and behavioral monitoring for non-human autonomous agents on enterprise WiFi.

DIFFERENTIATORS

- **Patent-pending, ITDR-first** — U.S. patents pending across WiFi authentication, RADIUS ITDR, AI-agent identity, and autonomous self-healing; among the first to bring ITDR to the RADIUS layer.
- **Globally consistent architecture** — built on Google Cloud Spanner with anti-hotspot sharding and region-aware routing for high-throughput authentication.
- **OEM & standards credentials** — Cisco Networking App Marketplace (app 382011); Wireless Broadband Alliance member (OpenRoaming, RADIUS Accounting Assurance).
- **Two engagement models** — direct use under the agency's own ATO (FedRAMP public data + SOC 2 Type II as inputs), or a dedicated deployment inside a prime / OEM authorization boundary.

PAST PERFORMANCE (commercial, in lieu of federal)

- **Scale & reach** — serves a large commercial base across enterprise, education, hospitality, and MSP verticals on a multi-region cloud (North America, Europe, Asia-Pacific, Australia).
- **Mission-critical authentication** — live RADIUS / 802.1X authentication and identity-threat-detection layer for production enterprise WiFi, making real-time access decisions at scale.
- **Production integrations** — validated against Cisco Meraki, Aruba, Juniper Mist, and CommScope Ruckus. Named references available on request under NDA.

FEDERAL ENGAGEMENT & COMPLIANCE

- **WaaS sub-component model** — beneath the OEM / integrator controller-AP stack: 802.1X / EAP-TLS with agency PKI, MITRE-mapped detection, CoA containment per playbooks, structured incident records for SIEM (Splunk / Sentinel / Chronicle / Elastic).
- **Section 889 / TikTok** — FAR 52.204-25 and 52.204-27 affirmative (no covered Huawei / ZTE / Hytera / Hikvision / Dahua equipment; no ByteDance apps on company devices).
- **FedRAMP 20x** — listed on the FedRAMP Marketplace (FedRAMP ID FR2631154499, Initial Implementation Phase, 12 Aug 2026); Class A Certification application targeted September 2026; hosted on Google Cloud (FedRAMP High covers the infrastructure, not the IronWiFi service). Public data: ironwifi.com/fedramp.
- **Not held** — not FedRAMP Authorized or Certified; no DoD Provisional Authorization or CMMC at any level. No federal accreditation claims are made.