LOCH TECHNOLOGIES

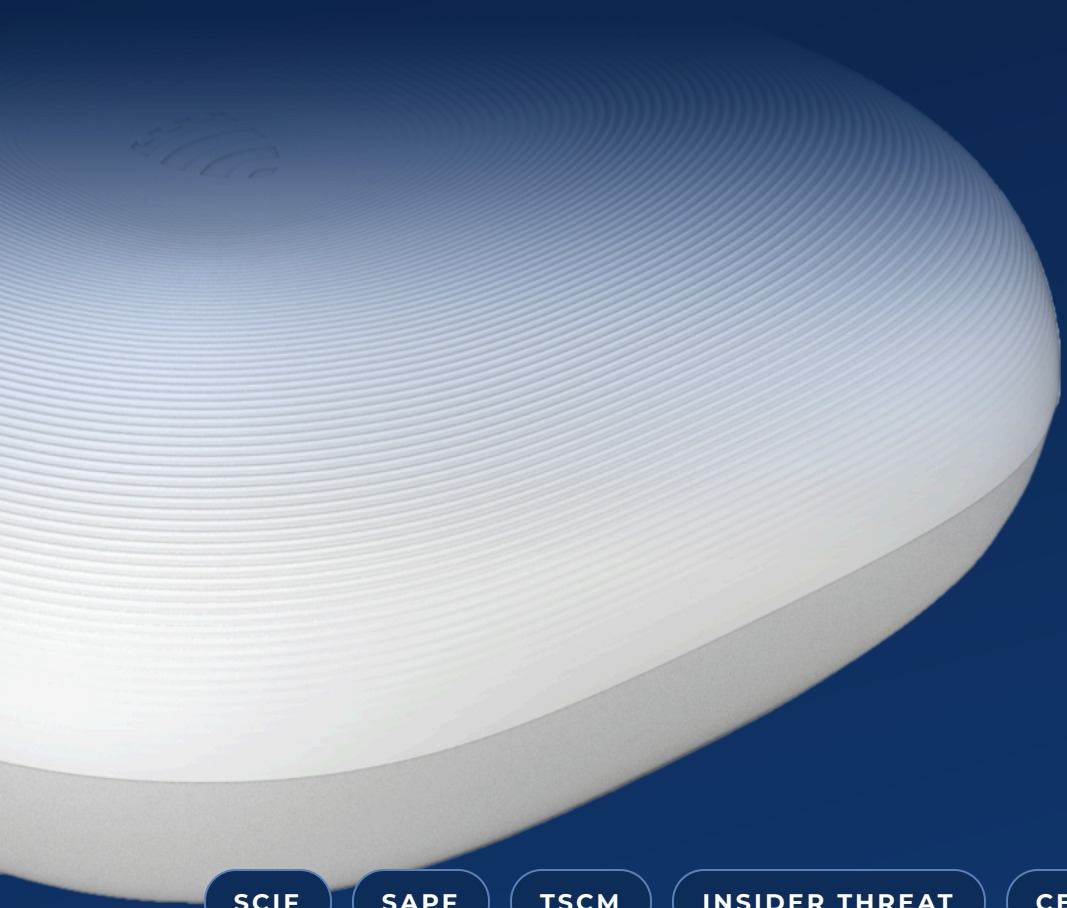
AirShield

WIRELESS AIRSPACE DEFENSE FOR GOVERNMENT

A bug sweep shows one moment in time.
AirShield watches every moment after it.

Use Case · From Manual TSCM Sweeps to Continuous SCIF Monitoring

Software-Defined RF Sensor · 300 MHz – 6 GHz · Zero Trust for the Airspace



SCIF | SAPF | TSCM | INSIDER THREAT | CELLULAR | DRONES

LOCH TECHNOLOGIES

www.loch.io

Classified spaces are built to keep signals out.
Few are watched for the signals that get in.

The Government Wireless Problem

SCIFs and SAPFs rely on construction standards, device bans and periodic technical surveillance countermeasures (TSCM) inspections. Each control works at a point in time. Between inspections, nobody is listening for a transmitter that should not be there, and the person most able to place one already has access.

All
DoD SCIFs and SAPFs were directed in 2023 to program for electronic device detection

45 days
the DoD security review, after a classified leak, that led to that directive

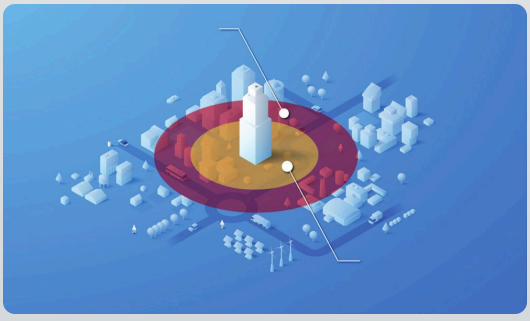
80%
of new IoT deployments connect wirelessly

2.5 / day
new wireless CVEs published during 2025

Secretary of Defense memo, Security Review Follow-on Actions, June 30, 2023 · LOCH Technologies · NIST NVD analysis

Why classified spaces are exposed

- **A sweep is a snapshot.** An inspection covers hours. A device planted the next day waits for the next visit.
- **Policy without detection.** A no-device rule runs on the honor system unless something detects violations.
- **Threats go beyond Wi-Fi.** Bluetooth, cellular and IoT radios sit outside what Wi-Fi intrusion detection sees.
- **The insider already has access.** No perimeter control stops a cleared person from carrying a device in.
- **Transmitters are small and common.** Phones, watches, earbuds, trackers and cameras all carry radios.
- **The threat is also outside the wall.** Rogue cell towers, drones and parked vehicles target the facility.



Wireless creates a recon zone and an attack zone

Why it matters

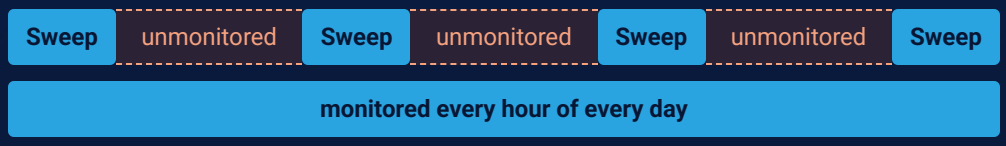
01 **The mission.** One compromised classified discussion can expose sources, plans and people.

02 **The mandate.** Policy now expects electronic device detection, not only device bans.

03 **The insider.** Trusted access defeats scheduled inspections. Detection cannot run on a calendar.

Move from manual TSCM bug sweeps to continuous monitoring.

A Sweep Is a Snapshot. Monitoring Is a Record.



	MANUAL TSCM SWEEP	CONTINUOUS MONITORING
Coverage in time	Hours, on a schedule	Every hour of every day
Device planted after a sweep	Unseen until the next sweep	Flagged when it first transmits
Burst and timed transmitters	Missed unless active during the sweep	Captured whenever they transmit
The insider	Can see the schedule and work around it	Passive and always on, with no schedule
Cost and disruption	Specialist teams, travel, rooms offline	Fixed sensors and no downtime
Evidence	A point-in-time report	A continuous record with playback
Scale	One room at a time	Every SCIF on one console

FIELD RESULT

AirShield found a hidden spy camera inside a SCIF. It had been planted by an insider.

An insider knows the sweep schedule and the device policy. Continuous monitoring has no schedule to work around: a transmitter is flagged whenever it is active, and the Threat Hunting app leads security to it.

How the move works

01 Baseline
AirShield learns the normal RF picture of each accredited space.

02 Monitor
Any new or unauthorized transmitter raises an alert, day or night.

03 Respond
Security walks to the device. TSCM teams inspect with a known target.

Continuous RF monitoring detects devices when they transmit. Physical inspection still matters for wired and dormant devices, and AirShield tells sweep teams where and when to look.

Top 10 use cases: protecting the SCIF.

01 Find the Device an Insider Planted

SCIF · INSIDER THREAT

PROVEN IN THE FIELD

AirShield found a hidden spy camera inside a SCIF, planted there by an insider.

A cleared insider does not need to defeat the perimeter. A camera, recorder or transmitter small enough to hide in a ceiling tile, a power strip or a desk item can be carried in and left behind. Device bans and entry checks depend on people. Sweeps depend on timing.

WITHOUT AIRSHIELD

A planted device runs until the next sweep.

No alert when a new transmitter appears.

No record of when the device arrived.

WITH AIRSHIELD

Unknown transmitters are flagged when active.

Threat Hunting app locates it within 1 inch.

Playback shows when it first appeared.

USES Zone-based alerts | Device fingerprinting | Threat Hunting app | Historical playback

Why it matters. The insider is the threat a SCIF is least built to stop. Detection must keep working after the door closes.

02 Replace Periodic Sweeps with Continuous TSCM

TSCM

TSCM teams are scarce, sweeps are costly, and rooms go offline while they happen. Between visits the space is unmonitored. Burst transmitters and devices on timers can stay silent for the hours a sweep lasts.

WITHOUT AIRSHIELD

Assurance is valid only for the day of the sweep.

Specialist teams travel from room to room.

Findings are a point-in-time report.

WITH AIRSHIELD

Every accredited space is monitored 24/7.

Sweep teams go where anomalies appear.

A continuous record supports inspections.

USES Passive RF monitoring | Behavioral baselining | Forensic playback

Why it matters. TSCM becomes a standing capability, and scarce experts go where they are needed.

Use cases 3 to 5: people, policy and sensitive rooms.

03 Enforce the No-Device Policy in SCIFs and SAPFs DEVICE DETECTION

Phones, smartwatches, fitness trackers and earbuds are prohibited in classified spaces, yet they are the devices people forget they are wearing. In 2023 the Secretary of Defense directed DoD components to program for electronic device detection and mitigation in all DoD SCIFs and SAPFs.

WITHOUT AIRSHIELD

Compliance relies on lockers and the honor system.

Violations surface only if someone notices.

WITH AIRSHIELD

No-phone zones alert on any active device.

Each event is logged with time and location.

Why it matters. Policy now expects detection, not only prohibition. AirShield enforces the rule.

04 Stop Wireless Data Exfiltration INSIDER THREAT · FORENSICS

Classified information leaves by the path nobody is watching. A personal hotspot, a Bluetooth link or a covert transmitter can carry data out without ever touching the monitored network.

WITHOUT AIRSHIELD

Off-network transmissions leave no log.

Investigators have nothing to reconstruct.

WITH AIRSHIELD

Unauthorized links and pairings are flagged live.

DVR-like forensics replay what, when and where.

Why it matters. User activity monitoring covers the network. AirShield covers the air around it.

05 Secure Conference Rooms and Leadership Spaces LEADERSHIP

Sensitive discussions also happen outside the SCIF: in command centers, conference rooms, executive suites and temporary secure spaces. These rooms see more visitors, more equipment and fewer inspections.

WITHOUT AIRSHIELD

Rooms are checked before major events only.

Visitor and vendor devices go untracked.

WITH AIRSHIELD

Zone policies cover each room continuously.

Trust levels separate approved from unknown.

Why it matters. Adversaries target the least protected room in which sensitive matters are discussed.

Use cases 6 to 8: threats from outside the wall.

06 Detect Rogue Cell Towers and Stingrays CELLULAR · 5G

A cell-site simulator near a government facility can capture identifiers and intercept the communications of the people who work there. Cellular hotspots and modems inside the building bypass network controls altogether.

WITHOUT AIRSHIELD

A fake tower looks like any carrier tower.

Cellular devices bypass firewalls and NAC.

WITH AIRSHIELD

AirCell rates towers known, unknown or suspicious.

Unauthorized cellular devices are detected.

Why it matters. Personnel are targets before they reach the door. The cellular environment is part of the perimeter.

07 Detect Drones Over Bases and Facilities COUNTER-UAS

Small drones survey installations, track movements and can carry a wireless device onto a rooftop. Drone detection is usually a separate system from cyber and counterintelligence tools, so nobody links the aircraft to the device it delivered.



WITHOUT AIRSHIELD

No awareness of drones near sensitive sites.

Separate consoles for drones and signals.

WITH AIRSHIELD

Unauthorized drones are detected and geolocated.

Drone and wireless findings share one console.

Why it matters. A drone is often the delivery method for a wireless attack. One platform connects the two.

08 Protect GPS Timing and Navigation GPS · PNT

Installations depend on GPS for timing, navigation, communications and fleet operations. Jamming and spoofing can shift time or position without raising an alarm.

WITHOUT AIRSHIELD

Interference looks like equipment failure.

No record of when or where it occurred.

WITH AIRSHIELD

GPS Canary flags jamming and spoofing.

Epoch-based history shows time and location.

Why it matters. Early warning keeps a GPS problem from becoming a mission problem.

Use cases 9 and 10: inventory, evidence and policy.

09 Inventory Wireless IoT Under Zero Trust ZERO TRUST · IoT

Smart buildings, fleet telematics, sensors and medical devices bring thousands of wireless endpoints onto government property. Most are unmanaged, and Zero Trust starts with knowing every device.

WITHOUT AIRSHIELD

Unmanaged devices never reach the inventory.

Risk is unknown until there is an incident.

WITH AIRSHIELD

Every RF-emitting device is found and classified.

Risk scores inform Zero Trust access decisions.

Why it matters. Zero Trust cannot be applied to a device nobody knows exists.

10 Support Accreditation with Continuous Evidence AUDIT · AIR-GAPPED

Accrediting officials, inspectors and auditors ask for proof that controls work. Point-in-time reports cannot show what happened between inspections. Many classified sites also need a system that runs without a cloud connection.

WITHOUT AIRSHIELD

Evidence is assembled by hand before reviews.

Gaps between inspections are undocumented.

WITH AIRSHIELD

Logs, playback and reports are ready on demand.

On-prem deployment suits air-gapped sites.

Why it matters. A continuous record shows controls worked every day, not only on inspection day.

How AirShield supports the policies that govern classified spaces

Policy	What it addresses	AirShield capability
ICD 705 and IC Tech Specs	SCIF construction, accreditation and portable electronic devices	Continuous detection of unauthorized emitters in and around the SCIF
SECDEF memo, June 2023	Electronic device detection and mitigation in DoD SCIFs and SAPFs	Always-on device detection, location and alerting
DoDI 8420.01	Wireless intrusion detection for DoD networks	Wi-Fi intrusion detection plus Bluetooth, cellular and IoT
CNSSP 17	Wireless communications that protect national security information	Zero Trust policy enforcement and no-phone zones

Policy summaries are for orientation. Confirm applicability with your accrediting official.

Ten ways AirShield protects classified spaces.

A software-defined RF sensor passively monitors 300 MHz to 6 GHz and reports to a single LOCH console, in the cloud or on-premises.

Continuous TSCM

Always-on RF monitoring fills the gap between sweeps and tells inspection teams where to look.

Passive by design

Passive monitoring with no agents and no network changes. Nothing is added to classified systems.

No-phone zones

Zone-based policies and trust levels alert on any unauthorized device in a restricted space.

Insider threat forensics

DVR-like playback with geo-positioning reconstructs what transmitted, when and where.

Find it and fix it

The Threat Hunting app locates devices to within 1 inch. AirTerminate breaks unacceptable connections.

Rogue tower and Stingray detection

AirCell scores every tower across LTE, CBRS and 5G and flags the ones that do not belong.

Far beyond Wi-Fi

One sensor covers Wi-Fi, Bluetooth, cellular, CBRS, 802.15.4, LPWAN and GPS from 300 MHz to 6 GHz.

Air-gapped deployment

On-prem hosting for restricted and air-gapped networks, with no dependence on a cloud connection.

Audit-grade evidence

Continuous logs, incident tracking and reports support accreditation, inspections and investigations.

Fits the mission stack

SIEM, SOAR, ITSM, CMDB, NAC and MDM integrations, plus an open API for automated response.

One sensor, the whole spectrum

Most wireless security stops at Wi-Fi. AirShield listens from 300 MHz to 6 GHz.

300 MHz	600 MHz	900 MHz	1.5 GHz	2.4 GHz	3.5 GHz	5 GHz	6 GHz
LPWAN	LTE	Z-Wave LoRa	GPS L1	Wi-Fi BT	CBRS	Wi-Fi	5G

Stop sweeping for yesterday's bug.
Monitor the airspace continuously.

Summary: From Snapshot to Continuous

CAPABILITY	LOCH AIRSHIELD	PERIODIC TSCM SWEEPS AND WI-FI WIDS
Protocol coverage	Wi-Fi, Bluetooth, LTE/5G, CBRS, 802.15.4, LPWAN, GPS	Wi-Fi only between sweeps
Monitoring	Continuous, in every accredited space	Scheduled, one room at a time
Insider-planted devices	Flagged when they transmit	Found only if a sweep catches them
Device policy enforcement	No-phone zones with alerts	Lockers and the honor system
Rogue cell tower detection	Included	Not supported
Drone detection	Included, in the same console	Separate system or none
Device location	To within 1 inch	Handheld search during a sweep
Forensics	Continuous record with playback	Point-in-time report
Air-gapped deployment	On-prem option	Varies by tool

SCIFs are built to the highest physical standards in government. The spectrum inside them deserves the same attention. AirShield moves counter-surveillance from a periodic event to a continuous capability, and it has already found what an insider hid inside a SCIF.



10.2 × 10.2 in · PoE powered

AirShield at a glance

Frequency	300 MHz – 6 GHz
Coverage	25,000+ sq ft per sensor
Backhaul	GbE PoE · LTE optional
Hosting	LOCH Cloud or on-prem

See your airspace

www.loch.io
info@loch.io
1-888-725-9434