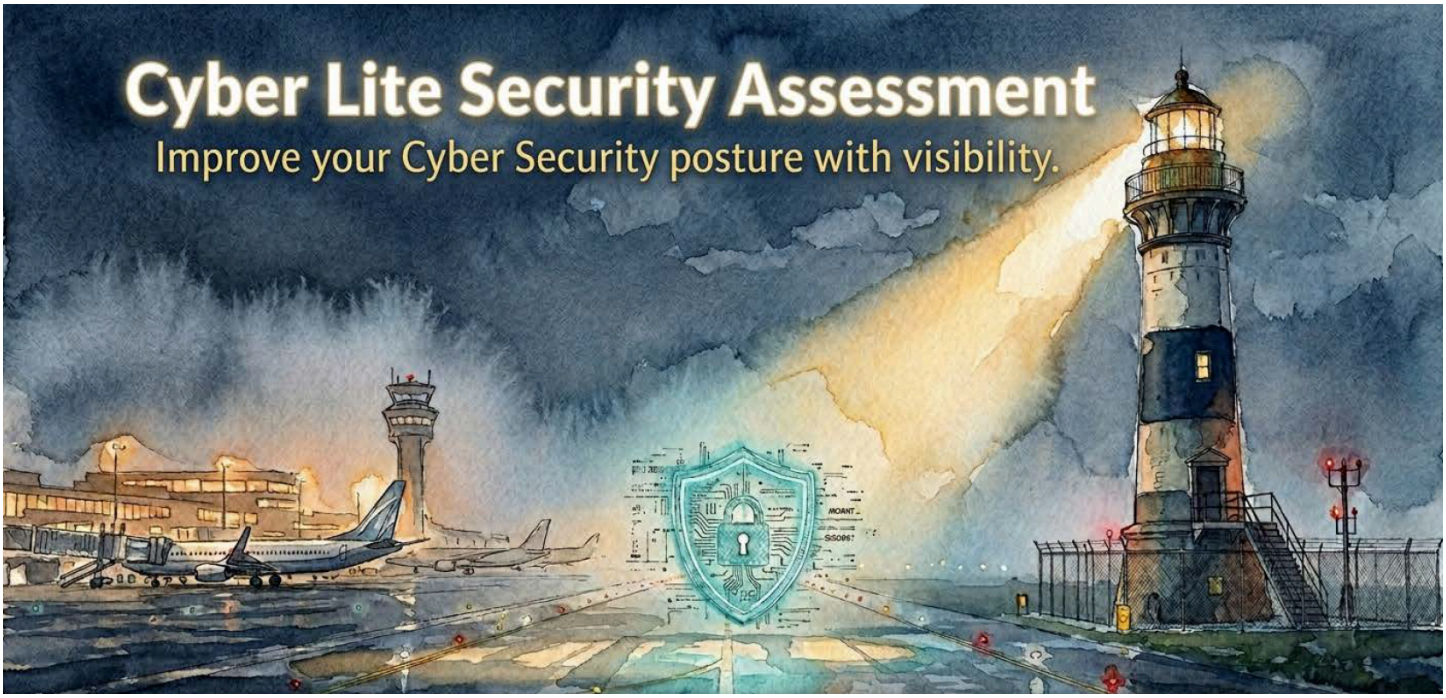


Testing a Practical Approach to Airport Cyber Risk

ACT Cyber Lite is an AAAE Airport Consortium on Transformation pilot that brings airports and industry partners together to evaluate a focused cybersecurity assessment in a real airport environment. Each pilot covers one wireless and one wired network segment, showing how gaps are found and addressed. There is no cost to participating airports, and the airports determine whether it delivers value.

WHY IT MATTERS

$1.4M+

Average loss from cyber incidents across connected airport and airline systems last year.

Source: Bridewell, via Cybersecurity Insiders (2026)

Focused
Covers a single wireless and a single wired network segment.

Practical
Shows how gaps are found and how to address them.

Airport-Led
Participating airports evaluate the results and judge the value.

What Each Pilot Assessment Covers

Scope is confirmed with each airport before testing and governed by approved rules of engagement.

ASSESSMENT AREA	WHAT WE EVALUATE	PRIMARY OUTPUT
Wireless / RF	Wireless spectrum conditions, rogue or suspicious access points, unauthorized wireless services, and misconfigured infrastructure.	Wireless findings and recommendations
Wired & External Exposure	Approved public-facing exposure, internal standard-user testing, lateral movement and egress risk, and critical-system testing when authorized.	Exposure and attack-path report
Governance, Risk & Compliance	Governance practices, control ownership, risk management, maturity, and alignment to NIST CSF 2.0 and applicable control considerations.	Maturity assessment, integrated risk register, and roadmap
Executive Reporting	Analysis that translates technical findings into business priorities.	Executive summary and leadership briefing

Developed in Collaboration With

ACT industry partners contribute specialized wireless, technical testing, and governance expertise, delivered by personnel with multiple years of experience working at airports.

Air Sheriff: Wireless and radio-frequency assessment.

Leidos / Scythe: Wired, external exposure, and attack-path assessment.

Mead & Hunt: Program coordination, governance and maturity analysis, and integrated risk reporting.

What Pilot Airports Receive

- **Executive summary** describing the most important risks and recommended leadership actions.
- **Integrated risk register** with severity, evidence, affected areas, recommended actions, ownership, and target timing.
- **Wireless findings package** with methodology, observations, detailed findings, and supporting evidence.
- **Wired and external exposure report** with identified attack paths, technical findings, and control observations.
- **NIST CSF 2.0 maturity assessment** and prioritized improvement roadmap.
- **Leadership briefing** to review results, answer questions, and establish next steps.

What the Pilot Asks of Airports

Estimated airport staff time: 2–4 hours per week

- An executive sponsor and designated technical point of contact.
- Confirmation of in-scope facilities, systems, network segments, and internet-facing assets.
- Approved rules of engagement, testing windows, onsite access, escorts, and escalation contacts.
- Relevant network diagrams, security policies, and asset information where available.
- Availability of selected IT, cybersecurity, operations, and system-owner staff for focused interviews.
- Participation in the final briefing and a closing feedback session on the pilot.

How the Pilot Works

Anticipated timing. Pilot duration will be assessed and refined after the first two pilot airports.

PHASE	TIMING	KEY ACTIVITIES	AIRPORT OUTPUT
1 **Confirm**	Week 1	Kickoff, scope confirmation, rules of engagement, access planning, and reporting alignment.	Approved assessment plan
2 **Assess**	Weeks 2–3	Wireless monitoring, approved outside-in and inside-wired testing, and focused critical-system testing if authorized.	Technical findings packages
3 **Integrate**	Week 4	Consolidation, validation, risk rating, and control mapping.	Draft integrated risk register
4 **Prioritize**	Week 5	Maturity scoring, executive analysis, and roadmap development.	Executive summary and prioritized roadmap
5 **Brief & Evaluate**	Week 6	Leadership readout and airport feedback session on the pilot.	Final report; airport evaluation of the pilot

Airports Decide the Value

Participating airports, not AAAE or industry partners, determine whether the assessment is worthwhile. ACT provides the framework and partners provide the technical expertise. At the close of each pilot, airports share structured feedback on:

Usefulness
Were the findings relevant and actionable?

Clarity
Was the reporting clear for leadership and staff?

Effort vs. Benefit
Was the staff time worth the insight gained?

Roadmap
Does the roadmap support real planning decisions?

Airport Fit
Does it address a meaningful airport need?

Broader Value
Would other airports benefit from it?

Security and Authorization

The ACT Cyber Lite partners are well versed in airport security protocols and in handling security-sensitive data. Testing is limited to the approved scope and rules of engagement; critical or isolated systems are tested only when expressly authorized. Evidence is handled under agreed data-handling and retention requirements.

Scope Considerations

Each pilot is intentionally limited to a single wireless and a single wired network segment; it is not an unrestricted penetration test or enterprise audit. Final scope and testing techniques are documented before the pilot begins. Results will help airports and ACT decide whether a broader assessment should be developed.

Sharing Lessons Learned

Anonymized, aggregated insights may be shared with the broader ACT airport community to benefit the industry. No airport-identifying or security-sensitive findings are shared without the participating airport's consent.

INTERESTED IN EXPLORING A PILOT?

Help ACT evaluate a practical cyber resource for airports. There is no cost to participating airports during the pilot.

To share your perspective or express interest, contact AAAE ACT Cyber:
Jeremy Valcich, Director, Innovation Programs
valcichj@aaae.org