Is Your Airport Ready For AIP Funding Requirements?

Aviation Relations

AIP Funding Requirements, Simplified for Airport Managers

A Quick Guide for Airport Managers. You're planning infrastructure upgrades: runway rehab, terminal expansion, and new equipment. AIP funding makes it possible. But here's what's catching airports off guard: cybersecurity readiness is becoming a factor in grant eligibility. Not someday. Now. This isn't about checking compliance boxes. It's about demonstrating your facility's ability to protect federally funded assets.

Table of contents

Salidas
Departures
Portes d'embarcament
Boarding gates
Flugsteige Gates
Puertas de embarque
A
Sortida
Exit
Ausgang
Salida
Puertas de embarque
natura
2 Min
Gates
opeyes

The Funding Question Nobody's Asking. You're planning infrastructure upgrades—runway rehabilitation, terminal expansion, and new equipment procurement. The Airport Improvement Program (AIP) can make these projects achievable, unlocking federal dollars that transform your airfield and passenger experience.

Yet an often-overlooked factor is suddenly front and center: cybersecurity readiness as a contributor to grant eligibility. Not in the distant future—today. Across the airport ecosystem, grant reviewers and program stakeholders are beginning to weigh whether an airport can reasonably safeguard assets purchased or improved with federal funds. If the risk is left unaddressed, questions arise that slow an application, trigger clarifications, or delay project starts.

The point is not to drown operators in compliance mechanics. It is to demonstrate stewardship—showing that your teams can protect navigation aids, communication networks, and operational systems from disruption. The shift reflects a simple truth: resilience is part of safety, and cybersecurity is part of resilience.

Why this matters now, federal dollars come with federal expectations. The FAA and partner agencies want assurance that the infrastructure they are helping you build or modernize won’t be left exposed to preventable cyber incidents. That assurance increasingly includes operational technology—lighting systems, fuel management, access control, HVAC, baggage and gates, and even your AWOS. These systems often sit close to the mission and can impact operations if compromised. Most airports have a reasonable handle on traditional IT security—email, endpoints, business applications, and perimeter firewalls. OT is where the hidden gaps live. Networks grew organically; vendor integrations piled up; convenience won the day; documentation lagged. The result is a mesh of connections whose risk profile is unclear when auditors or grant reviewers ask basic questions.

This guide restructures your thinking into a few practical checkpoints and actions you can take immediately—without massive budgets or multi-year programs. The goal is simple: reduce friction in your AIP application and strengthen your airport’s resilience.

Three Questions That De-risk Your AIP Application

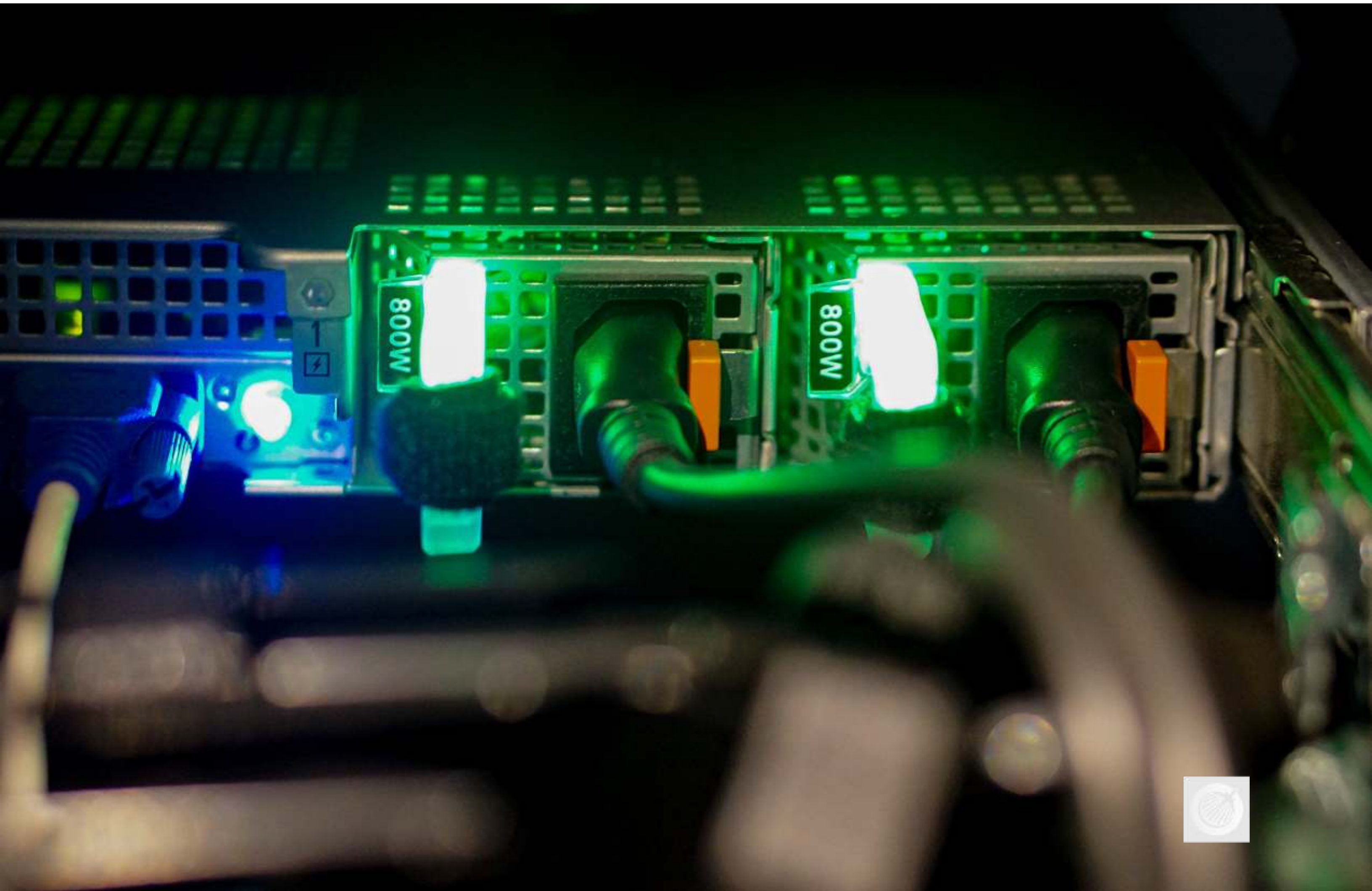
Practical prompts to surface OT/IT blind spots before reviewers do

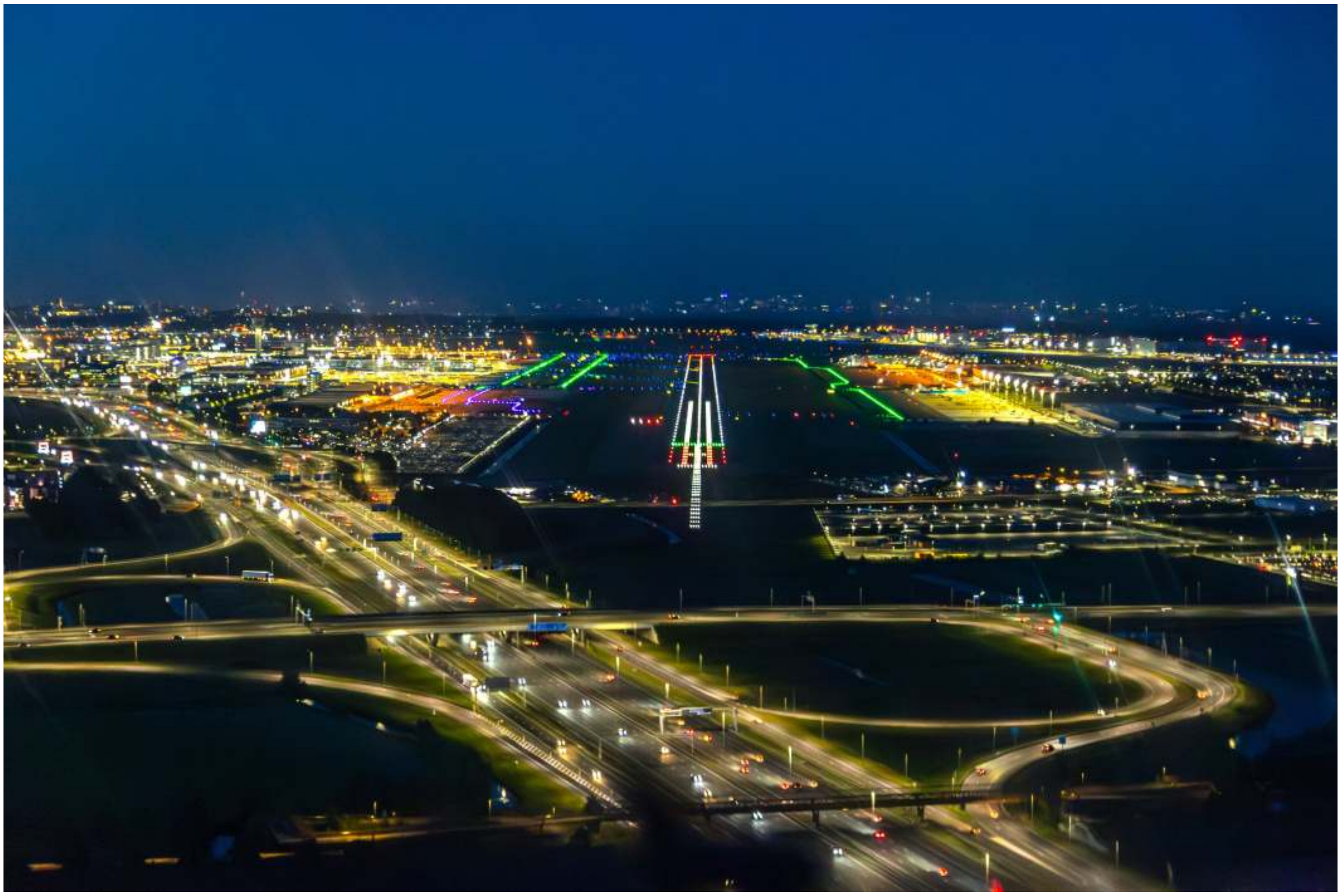
1) Do you know where your federal and non-federal systems connect? This is the number one gap most airports encounter. Networks evolved over years, sometimes decades. A lighting controller needed a remote vendor session; a fuel management system needed reporting; an access control platform needed directory services; a weather system needed an uplink. Minor exceptions are compounded into a network where operational technology touches IT in undocumented ways. The action: produce a simple, living diagram that shows systems, segments, and points of connection. Note which assets are federal, non-federal, and mixed environments. Even a whiteboard sketch, photographed and turned into a PDF, silences a reviewer when they ask how you separate grant-funded systems from the rest of the campus.

2) Can you show a basic cybersecurity posture if asked? Grant reviewers are not looking for a full NIST audit. They are scanning for evidence that you aren’t ignoring risk. Gather a short packet: a policy or memo establishing responsibility for OT cybersecurity; a one-page description of your network segmentation approach; a summary of access control practices (unique accounts, role-based access, MFA where feasible); vendor remote access process (approved tools, time-bound access, logging). If you can demonstrate awareness and a path forward, you reduce follow-up questions that create delay.

3) Who owns cybersecurity at your airport? If the answer is “IT handles it,” but IT does not administer airfield or building automation systems, you have a gap. OT security often sits between departments—operations, maintenance, and IT—making it without a single owner. Name an accountable person or committee, define the scope, and assign decision rights. Ownership alone can raise confidence with reviewers.

The thread through all three questions is clarity. Clarity on where systems touch, clarity on minimum protections, and clarity on ownership. Airports that can articulate these points tend to move faster through reviews because they eliminate uncertainty. You don’t need enterprise tooling to get started; you need attention and a record of decisions. That record becomes a foundation for both future projects and any cyber-related conditions attached to grants.





What Smart Airports Are Doing Now. They're not waiting for mandates. They are inventorying what systems exist and how they connect. They are identifying which assets would be part of a federal grant project. They are documenting basic security measures already in place. And they are closing obvious gaps before they become audit findings. None of this requires a massive budget. It requires attention.

Translate that into a 30–60 day plan:

Week 1–2: Build your OT/IT inventory. Walk the environment with operations, maintenance, and IT. Catalog airfield lighting controllers, fuel farm systems, access control panels, HVAC/BMS, baggage systems, gates, radio/telecom backhauls, AWOS/ASOS, and any vendor-managed appliances. Note software versions, network segments, remote access methods, and support contacts.

Week 3–4: Map connections and segments. Sketch the logical topology. Identify where OT crosses into IT. Confirm that internet access OT flows through controlled gateways. Where possible, create VLANs or firewalled subnets to isolate sensitive systems and allow only listed traffic.

Week 5–6: Establish minimum controls. Unique accounts for vendor access; time-bound credentials; MFA where feasible; change control for configuration; log where you can (even syslog to a low-cost collector). Draft a one-page OT Cyber Policy signed by leadership, assigning ownership and outlining assigns, segmentation, outlines assignmentthat assigns, and access principles.

Documentation is a force multiplier. Build a lightweight “AIP Cyber Readiness Packet” to attach to grant narratives or keep on hand for reviewer questions. Include your inventory summary, a simple network diagram, a policy memo, and a short description of vendor remote access and incident contacts. This packet demonstrates due diligence without committing you to expensive tools.

Culture matters. Encourage vendors and internal teams to treat OT like safety-critical equipment: controlled change windows, documented access, and rollback plans. Small process habits prevent big outages. When reviewers see that mindset reflected in your materials, they infer stronger project execution.

Bottom Line

Reduce application friction now; avoid costly delays later.

AIP funding is competitive. Anything that creates friction in your application—including questions about cybersecurity readiness—works against you. A few hours of assessment now could save months of delay later. Build clarity, show ownership, and document your minimum viable protections. Doing so preserves momentum from planning to obligation to project kickoff.

Tie readiness back to specific projects. If you are seeking funds for runway rehabilitation, reference segmentation between airfield lighting controllers and business networks. For terminal expansion, cite access control and HVAC/BMS protections. For equipment purchases, note vendor remote access governance. These brief, targeted statements align cybersecurity posture to the assets under consideration—exactly

CYBER SECURITY
USER ID
Remember me
Forgot password?
DATA PROTECTION

About the Author

Bridging aviation operations and cybersecurity

Teddy Cooper is a 28-year aviation professional with a Master's in Information Technology, currently an FAA Electronic Engineer specializing in navigation aids and airport infrastructure. He bridges the gap between aviation operations and cybersecurity. He created this guide to help airport managers stay ahead of evolving requirements. Questions? Reach out on LinkedIn or visit aviationrelations.com/contact.

Author’s note. The guidance in this short ebook is practical by design. Airports vary widely in size, staffing, and vendor ecosystems, but the fundamentals travel well: know your connections, show your posture, and assign ownership. Start small, iterate, and document. That’s enough to reduce friction in AIP narratives today while laying groundwork for more mature programs tomorrow.