PARAS

PROGRAM FOR APPLIED
RESEARCH IN AIRPORT SECURITY

PARAS 0064

May 2026

AI in Airport Security

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Royce Holden
Mead and Hunt, Inc.
Asheville, NC

Pauline Norstrom
Anekanta® AI
Daresbury, UK

Stephanie Lane
Mead and Hunt, Inc.
Dallas, TX

DeMeakey Williams
Crane Consulting and Technology Solutions
Duluth, GA

Ben Pecheux
Mead and Hunt, Inc.
Park City, UT

Dominic Nessi
5 X 5 Cyber Solutions
Las Vegas, NV

Sebastian Fischer
Washington, DC

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0064 PROJECT PANEL

Mike Baden *Portland International Airport*

Frank Capello *Broward County Aviation Department (Retired)*

Scott Creager *NW Natural*

Kim Dickie *KPD Consulting, LLC*

Enrique Melendez *The JW Group, Inc.*

David Peeples *Intellisoft, Inc.*

Rick Sanchez *John Wayne Airport*

Chris Scott *Port of Huntsville*

Jodi Spencer *Boise Airport*

Michael Stubblefield *National Safe Skies Alliance*

AUTHOR ACKNOWLEDGMENTS

The PARAS 0064 research team extends its deepest appreciation to the many individuals and organizations whose expertise, insights, and collaboration made this guidebook possible. We are especially grateful to the airport operators, law enforcement professionals, cybersecurity specialists, and technology vendors who generously contributed their time and perspectives through interviews, outreach sessions, and peer reviews. Their real-world experiences and thoughtful feedback were instrumental in shaping a guidebook that reflects the operational realities and strategic challenges faced by airports of all sizes.

We also wish to thank the representatives from local, state, and federal agencies—including those from the TSA, FAA, and other critical infrastructure partners—whose frameworks provided valuable input on regulatory requirements, risk management, and policy alignment. These contributions helped ensure this guidebook is grounded in both practical application and legal compliance.

Special recognition goes to the PARAS 0064 Project Panel, whose volunteer service, technical guidance, and subject-matter expertise were essential throughout the life cycle of this project. Their commitment to advancing airport security through applied research is commendable and deeply appreciated.

Finally, we acknowledge the support of National Safe Skies Alliance and the FAA for sponsoring this research and for their continued dedication to improving aviation security through the PARAS program. It is through this collaborative ecosystem that Safe Skies can deliver meaningful, actionable resources to the aviation community.

Thank you for helping us create a guidebook that not only informs but empowers airport leaders to navigate the evolving landscape of artificial intelligence in security operations.

CONTENTS

TABLES & FIGURES

SUMMARY

This guidebook offers a comprehensive framework for integrating artificial intelligence (AI) into airport security operations. It is designed for airport security professionals, policymakers, and stakeholders, and emphasizes both the transformative potential of AI and the critical need for responsible, risk-informed deployment.

The guidebook establishes foundational knowledge of AI technologies machine learning, deep learning, neural networks, natural language processing, computer vision, and generative AI and their relevance to airport environments. It references global standards such as the Organisation for Economic Co-operation and Development (OECD) AI Principles, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 22989, and the National Institute of Standards and Technology AI Risk Management Framework to define AI systems and ensure regulatory alignment. A comparative summary table outlines the strengths, limitations, and use cases of each AI type, providing a practical reference for decision-makers.

In the application domain, the guidebook explores how AI enhances threat detection, operational efficiency, and human-machine collaboration. It presents real-world examples such as the Automated Prohibited-Item Detection System, which integrates multiple AI techniques to improve aviation worker screening. Law enforcement applications include predictive policing, facial recognition, gunshot detection, and digital forensics. Case studies illustrate successful deployments, while a phased implementation strategy is recommended to manage costs and risks.

The guidebook provides information on building a business case for AI adoption, including methods for conducting cost-benefit analysis, calculating net present value, and evaluating ROI. The report emphasizes the importance of quantifying both tangible and intangible benefits, such as improved safety and enhanced passenger experience.

The guidebook also addresses the risks associated with AI, including data privacy concerns, system reliability, cybersecurity threats, algorithmic bias, and lack of transparency. It outlines mitigation strategies such as human-in-the-loop oversight, vendor accountability, regular audits, and adherence to international standards like ISO/IEC 42001. Data management is explored through the DIKW (Data-Information-Knowledge-Wisdom) model and Big Data principles, with technical guidance on infrastructure, integration, and cybersecurity controls.

Legal and regulatory considerations are extensively covered, including US federal and state laws, The European Union’s (EU) General Data Protection Regulation, Canada’s Personal Information Protection and Electronic Documents Act, and the EU AI Act (Regulation (EU) 2024/1689). The guidebook stresses the importance of informed consent, ethical AI usage, and early involvement of legal counsel. A detailed table summarizes applicable legal frameworks, and compliance strategies are provided to ensure transparency and accountability.

Deployment is framed as a five-phase process: establishing governance, selecting vendors, implementing and testing systems, preparing personnel, and sustaining performance. Each phase is linked to earlier sections of the report, creating a cohesive life cycle approach. The guidebook concludes with recommendations for future research, including Explainable AI (XAI), digital twins, federated learning, and neuro-symbolic AI. It also includes a technical security controls checklist and a comprehensive list of funding resources to support AI initiatives in airport environments.

PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

AGI	Artificial General Intelligence
AI	Artificial Intelligence
API	Application Programming Interface
APIDS	Automated Prohibited-Item Detection System
CAPEX	Capital Expense
CBA	Cost-Benefit Analysis
CNN	Convolutional Neural Network
CV	Computer Vision
DIKW	Data → Information → Knowledge → Wisdom
DL	Deep learning
GDPR	General Data Protection Regulation
HITL	Human-in-the-loop
IoT	Internet of Things
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
LLM	Large Language Model
MD	Markdown
ML	Machine Learning
NCIC	National Crime Information Center
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NPV	Net Present Value
OECD	Organisation for Economic Co-operation and Development
OPEX	Operational Expense
PCII	Protected Critical Infrastructure Information
RAG	Retrieval-Augmented Generation

RNN	Recurrent Neural Network
ROI	Return on Investment
SIA	Security Industry Association
ViT	Vision Transformer
XAI	Explainable AI

SECTION 1: INTRODUCTION

In the realm of airport security, the integration of artificial intelligence (AI) is increasingly appealing due to its potential to significantly enhance operational efficiency, bolster threat detection capabilities, and support the human workforce. However, the adoption of AI in this context also presents several challenges that must be addressed, including financial costs, the complexities of integrating AI into existing operational frameworks, and ethical considerations.

AI is crucial for addressing modern business challenges compared to traditional solutions because it leverages data to create real-time, evidence-based, and informed decision-making processes, resulting in sophisticated business intelligence.

1.1 Purpose of this Guidebook

This guidebook provides a comprehensive resource for airport security professionals to understand the potential applications, benefits, and challenges of implementing AI in airport security. It aims to facilitate informed decision-making and strategic planning for the integration of AI technologies into airport security operations while incorporating scenario-based recommendations, real-world case studies, and operational checklists that speak directly to the day-to-day realities of airport security work.

Figure 1. AI-Generated Rendering of "AI in Airport Security"

AIRPORT CONSIDERATIONS

Airport security professionals face rapidly evolving threats, increasing operational complexity, and growing demands for efficiency and compliance. Each airport has unique characteristics given the wide variation in airport sizes and operational volumes. As a result, there is no one-size-fits-all method for integrating AI into airport security operations. Similarly, there is no single correct approach to procuring, implementing, and utilizing AI. Each airport must thoroughly assess its current security operations to identify and address its specific AI needs. Out of the sixteen airports and non-aviation organizations the research team contacted, nine participated in our outreach efforts, providing valuable input that helped validate and inform the guidebook.

AUDIENCE AND USE CASES

This guidebook is intended for airport security operators, IT professionals, policymakers, legal counsel, and other stakeholders involved in airport security. It provides practical insights and guidance on how to leverage AI technologies to enhance security measures, improve operational efficiency, and ensure compliance with regulatory requirements. While policymakers and technology partners may also benefit, the primary focus is on empowering airport security professionals to lead successful, responsible AI initiatives.

1.2 Overview of the Guidebook Sections

This guidebook is structured to provide a comprehensive, step-by-step understanding of how AI can be responsibly and effectively integrated into airport security operations. Each section builds upon the previous ones, guiding readers from foundational concepts to practical deployment strategies, risk mitigation, and future research directions. The organization of the guidebook ensures that readers can navigate the complexities of AI adoption with clarity and confidence. The sections are as follows:

- **Section 2: Understanding AI: Key Concepts and Terminology**
  Introduces the core types of AI—including machine learning (ML), deep learning (DL), neural networks, natural language processing (NLP), computer vision (CV), and generative AI—along with definitions, use cases, and global standards. This section establishes a shared vocabulary and technical foundation for all stakeholders.
- **Section 3: AI Applications in Airport Security**
  Explores how AI is currently used across airport security domains, including law enforcement, operational security, and cybersecurity. Real-world examples and case studies illustrate the impact of AI on threat detection, surveillance, and resource optimization.
- **Section 4: Potential Risks of AI Use**
  Identifies and analyzes risks such as algorithmic bias, automation bias, cybersecurity vulnerabilities, and lack of transparency. This section offers mitigation strategies and emphasizes the importance of human oversight and ethical governance.
- **Section 5: Privacy, Legal, and Regulatory Considerations**
  Details the legal frameworks and compliance obligations associated with AI use, including US federal and state laws, the European Union's (EU) General Data Protection Regulation (GDPR), and the EU AI Act. It also addresses consent, ethical usage, and vendor accountability.
- **Section 6: Data Management, Integration, and Infrastructure Considerations**
  Covers the technical requirements for successful AI implementation, including data quality, system interoperability, cybersecurity controls, and scalable infrastructure. It introduces the data modeling and Big Data principles relevant to airport environments.
- **Section 7: Developing a Business Case for AI in Airport Security**
  Provides guidance on building a compelling financial justification for AI adoption. It includes cost-benefit analysis (CBA), net present value (NPV), and return on investment (ROI) models, with templates and examples to support strategic decision-making.
- **Section 8: Deployment Considerations**
  Outlines a five-phase deployment strategy—from governance and vendor selection to implementation, training, and ongoing management. This section emphasizes the importance of cross-functional collaboration and continuous performance monitoring.
- **Section 9: Recommendations for Future Research**
  Suggests areas for continued exploration, including Explainable AI (XAI), digital twins, federated learning, and neuro-symbolic AI. It highlights the need for research that enhances trust, reliability, and scientific validity in AI systems.
- **Section 10: Conclusion**
  Summarizes the guidebook's key insights and reinforces the importance of strategic, ethical, and well-governed AI adoption in airport security. It calls for leadership, transparency, and stakeholder engagement to ensure successful outcomes.

CALLOUT BOXES

Throughout this guidebook, “callout boxes” highlight supplementary information relevant to the current section. These boxes may feature insights from cited sources or direct comments gathered during research outreach, and serve to illustrate practical examples and potential applications of AI in airport security. Callout boxes will be visually distinct, as shown to the right.

AI Implementation Insight: A common challenge in deploying AI for airport security relates to data quality. For AI systems to perform effectively, the underlying data must be meticulously organized, accurately labeled, and consistently managed.

SECTION 2: UNDERSTANDING AI: KEY CONCEPTS AND TERMINOLOGY

This section introduces fundamental AI concepts and terminology, including machine learning (ML), deep learning (DL) and neural networks, natural language processing (NLP), computer vision (CV), and generative AI. The goal is to establish a common language for airport operators, planners, and technical teams. By outlining the distinct functionalities and typical applications of each technology, readers will gain the necessary insights to assess emerging AI solutions in relation to strategic goals and operational needs.

This approach to defining common language around AI not only clarifies overlapping terms but also fosters collaboration between technical and non-technical stakeholders, enabling airports to integrate AI in ways that enhance efficiency, improve passenger experience, and bolster overall security.

This section also introduces foundational IT terminology critical to airport environments and references globally accepted standards around AI to ensure consistent understanding, precise implementation, and support for regulatory alignment in the United States.

GLOBAL DEFINITION FOR AI SYSTEMS

Since its initial endorsement in May 2019 and update in May 2024, the Organisation for Economic Co-operation and Development's (OECD) AI Principles have provided an intergovernmental standard for "trustworthy AI." These principles guide developers in embedding ethical safeguards into AI systems and help policymakers build interoperable AI risk-management frameworks across jurisdictions.[1]

A core outcome of these principles is a harmonized global definition of an AI system—now embedded in numerous international and national standards and regulations. Regardless of the underlying technique, this definition distinguishes AI systems from conventional software by emphasizing inference from data to produce outcomes that can affect real-world or virtual environments:

> AI system
>
> A machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.[2]

This definition has been adopted by:

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 22989 (Information technology — Artificial intelligence — Artificial intelligence concepts and terminology), which standardizes AI terms and life cycle concepts.[3]
- National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF 1.0), which builds on the OECD and ISO definitions to support US federal agencies and industry in identifying and managing AI risks.[4]

---

[1] "AI Principles Overview," *Organisation for Economic Co-Operation and Development*, 2019, updated 2024, https://oecd.ai/en/principles.
[2] "AI Principles Overview."
[3] International Organization for Standardization, "ISO/IEC 22989:2022 Information Technology - Artificial Intelligence - Artificial Intelligence Concepts and Terminology" (Geneva, Switzerland, July 2022), https://www.iso.org/standard/74296.html .
[4] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, January 2023, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

- EU AI Act (Regulation (EU) 2024/1689), the first comprehensive AI regulation in the EU, which aligns its scope and obligations with the OECD's definition of an AI system.[5]
- Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (adopted May 17, 2024), the first binding international treaty on AI, which explicitly references the OECD definition to ensure AI life cycle activities respect human rights and the rule of law.[6]

By anchoring AI policy and regulation to this single, robust definition, industry and regulators can more effectively:

1. Identify AI components within complex products. This clarity helps prevent the overreach of regulations to non-AI components while ensuring the specific parts of a system that leverage AI capabilities (e.g., ML models, neural networks, or inference engines) are correctly identified. This is crucial for applying appropriate oversight, assessing potential biases, and ensuring accountability where AI features might impact safety, fairness, or privacy within larger, integrated technological solutions.
2. Align risk, governance, and compliance measures. A unified definition allows for the development of consistent frameworks for assessing and managing AI-specific risks, such as algorithmic bias, data privacy breaches, or unintended consequences. This consistency is vital for establishing robust governance structures, streamlining internal compliance processes, and facilitating the adoption of best practices that address the unique challenges posed by AI systems, regardless of their specific industry deployment.
3. Ensure consistent oversight across borders and sectors (industries, domains, or areas of economic and social activity) to foster international interoperability and reduce regulatory fragmentation. A shared understanding of what constitutes an AI system simplifies cross-border collaboration for both businesses and regulatory bodies. It minimizes the potential for conflicting national regulations, promotes the development of harmonized standards, and facilitates the secure and ethical deployment of AI technologies on a global scale. This consistency supports innovation by providing a clearer regulatory landscape for developers and deployers alike, ultimately enhancing trust and confidence in AI systems worldwide.

2.1 Different Types of Artificial Intelligence

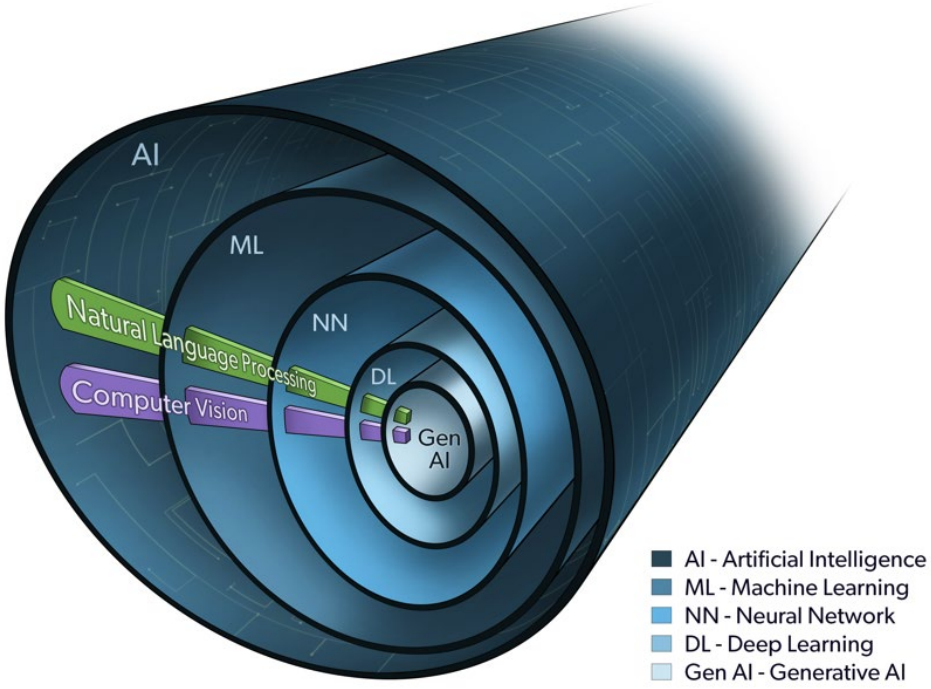
The term AI can refer to a range of technologies, including:

- ML (Machine Learning) – a subset of AI focused on learning from data
- NN (Neural Networks) – models within ML inspired by the human brain
- DL (Deep Learning) – Advanced NN architectures for complex tasks
- Gen AI (Generative AI) – Specialized DL models that create new content

Figure 2 illustrates the nested structure of AI technologies, showing how broad concepts like Artificial Intelligence encompass more specific types such as Machine Learning, Neural Networks, Deep Learning, and Generative AI, along with applications like NLP and Computer Vision.

[5] "Regulation - EU - 2024/1689 - EN - EUR-Lex," *European Union*, 2024, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
[6] "Understanding the Scope of the Council of Europe Framework Convention on AI," *Opinio Juris*, November 5, 2024, https://opiniojuris.org/2024/11/05/understanding-the-scope-of-the-council-of-europe-framework-convention-on-ai/.

Figure 2. Different Types of AI



2.1.1 Machine Learning

ML is a subset of AI that involves training algorithms to recognize patterns and make predictions based on data. It enables systems to learn from experience and improve their performance over time without being explicitly programmed. In the context of airport security, ML can be used to analyze vast amounts of data from various sources, such as surveillance cameras, sensors, and passenger records, to identify potential threats and enhance security measures. For example, ML algorithms can detect unusual patterns in passenger behavior or identify individuals who match profiles of known threats. Platforms like Netflix and Amazon use ML algorithms to analyze your viewing or purchasing history and suggest movies, shows, or products you might like. Types of ML include:

- **Supervised learning –** The algorithm is trained on labeled data and learns by comparing its predicted outputs to the known correct outputs (e.g., identifying known threat cases).
- **Unsupervised learning –** The algorithm explores patterns and structures in unlabeled data without predefined categories (e.g., clustering passenger behaviors).
- **Self-supervised learning –** Creates its own labels from unlabeled data by predicting one part of the input from another, reducing the need for manual labeling (e.g., pretraining language models).
- **Reinforcement learning –** The algorithm learns through trial and error in an interactive environment, receiving feedback based on actions taken (e.g., optimizing patrol routes for autonomous robots).

> A medium hub airport when asked about using ML for security at the airport stated, "We found it useful at analyzing behavioral patterns in the ID credentialing/badging system, such as swiping at unusual hours or through multiple doors quickly and then alerting on those activities."

- **Semi-supervised learning –** Combines a small, labeled dataset with a large unlabeled dataset, using the labeled data to guide the learning process (e.g., labeling new security footage with minimal manual effort).[7]

In airport security, ML is applied generally in:

- Anomaly detection based on surveillance data
- Risk-based passenger screening
- Predictive maintenance of security equipment[8]

2.1.2 Deep Learning and Neural Networks

DL is a branch of ML that uses neural networks with multiple layers (hence "deep") to model complex patterns in data. These layers allow the network to learn hierarchical representations, making DL particularly effective for tasks such as image and speech recognition or NLP (discussed below). Social media platforms like Facebook use DL models to recognize and tag faces in photos (photo tagging), making it easier to organize and share images with friends.

Within the realm of DL, neural networks are a type of ML model inspired by the structure and function of the human brain. They consist of interconnected nodes, or neurons, that process and transmit information. For example, email services like Gmail use neural networks to analyze email content and distinguish between spam and legitimate emails (filtering). In airport environments, DL can be used for:

- Facial recognition systems
- Threat detection in x-ray imagery (image-based tasks, see Convolutional Neural Networks below)
- Passenger voice interaction at self-service kiosks

Neural networks are particularly effective at handling complex tasks such as image and speech recognition, making them valuable tools in airport security. Both AI concepts are used in advanced software applications in airport security to enable systems to learn and identify complex patterns in various forms of data.

Types of neural networks include Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN). Each have their own specialization regarding how they handle different types of data.

RECURRENT NEURAL NETWORKS

RNNs are designed to handle sequential data by maintaining a memory of previous inputs through loops in their architecture. This makes them particularly effective for time-series analysis, such as processing sensor data or logs over time.[9] Airport security applications of RNNs can include:

- Behavioral analysis based on access logs and entry/exit patterns
- Incident detection through analysis of sequential surveillance events
- Detection of abnormal badge access behavior (e.g., frequent late-night access)
- Recognition of suspicious movement sequences from CCTV footage

[7] "Types of Machine Learning," *IBM*, December 20, 2023, https://www.ibm.com/think/topics/machine-learning-types.
[8] Misagh Haji Amiri and Ali Osman Kuşakcı, "A Scoping Review of Artificial Intelligence Applications in Airports," *CRPASE: Transactions of Industrial Engineering* 10, no. 2 (June 2024): 1–12.
[9] Jason Brownlee, *Deep Learning for Time Series Forecasting: Predict the Future with MLPs, CNNs and LSTMs in Python* (Machine Learning Mastery, 2018).

CONVOLUTIONAL NEURAL NETWORKS

CNNs are specialized neural networks designed to process unstructured visual data, such as images. They automatically learn to detect visual features such as edges, shapes, textures, or patterns by applying small filters (called convolutions) across the input. This makes CNNs highly effective for image classification, object detection, and scene understanding.[10] Airport security applications of CNNs can include:

- Automated threat detection in x-ray baggage scanning
- Identification of prohibited items (e.g., knives, firearms, liquids) in scanned images
- Anomaly detection based on visual characteristics of luggage
- Object recognition in CCTV or perimeter surveillance footage

TRANSFORMERS

Transformers are a new DL architecture that is designed to process entire datasets in parallel, rather than step-by-step as in older models like RNNs. They use an attention mechanism to weigh the importance of different elements in the input, allowing the model to focus on the most relevant information. This parallel processing and ability to grasp long-range dependencies make them incredibly powerful. While Transformers are the foundation of modern NLP systems, their influence extends beyond text. Vision Transformers (ViT) adapt the same architecture for image processing by treating image patches as tokens, enabling models to capture global context in visual data. This innovation has revolutionized computer vision tasks such as image classification, object detection, and segmentation. In everyday life, interaction with a transformer is common when using an AI chatbot or a tool that generates text. They also power the improved understanding of complex queries in search engines and make a phone's predictive text remarkably intelligent by anticipating the next word.[11] In an airport setting, Transformers can enable:

- Multilingual customer service chatbots
- Speech translation kiosks
- Analysis of unstructured threat intelligence from internal reports or open-source text

2.1.3 Natural Language Processing

NLP is a branch of AI that focuses on enabling machines to understand and respond to human language. NLP involves various statistical methods, ML processes, and language detection tasks to derive meaning from text or audio. Here are some key components:

- **Speech-to-text –** This process converts human speech into text. While NLP is not always necessary for this step, it helps manage the often disorganized nature of spoken language. NLP also applies to text-based messages, not just speech.
- **Tagging and categorizing –** In speech tagging, ML sorts words into categories like nouns and verbs. This is crucial for words with multiple meanings, depending on their context. This semantic analysis, also known as word sense disambiguation, helps determine the sentence's meaning.
- **Name and entity recognition –** An example includes a smart reader that picks out all the important "who, what, and where" details in a text. It automatically spots things like names of people, places, or companies.

[10] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, *Deep Learning* (Cambridge, Mass.: MIT Press, 2016).
[11] Ashish Vaswani et al., "Attention Is All You Need," August 2, 2023, https://arxiv.org/pdf/1706.03762.

- **Coreference resolution –** Think of this as the system figuring out when different words are talking about the same thing. For example, if a sentence mentions "Mary" and then later "her," the system knows "her" is still Mary. It can even connect "my computer" with "the Apple device" if they refer to the same item. This also helps it grasp more complex language, like when a word is used as a metaphor (e.g., understanding that calling a lawyer a "shark" means they are aggressive, not an actual fish).
- **Sentiment analysis –** NLP uses natural language understanding and DL models to detect emotions and determine whether the sentiment expressed is positive or negative.

NLP technologies can be used in airport security to analyze and interpret communication data, such as passenger interactions with airport systems and social media posts, to identify potential threats. For example, NLP algorithms can detect keywords and phrases associated with security risks and alert security personnel to investigate further. Additionally, NLP can be used to enhance customer service by enabling automated systems to understand and respond to passenger inquiries in real time.[12] An example of NLP usage is a customer service website that uses NLP-powered chatbots to understand and respond to customer inquiries in natural language, providing support and answering questions.

In airport security, NLP supports communication, translation, and threat identification. NLP components relevant to security include the following:

- Speech-to-text: Transcribes voice input from passengers
- Tagging and categorization: Sorts terms by linguistic function for deeper interpretation
- Named entity recognition: Identifies people, places, or objects
- Sentiment analysis: Gauges emotional tone to identify potential escalation risks

2.1.4 Computer Vision

CV is a field of AI that enables computers to interpret and understand visual information from the world, such as images and videos. CV relies on ML and DL techniques to analyze and process visual data. Fundamental tasks for CV include image acquisition, re-sampling, scaling, noise reduction, contrast enhancement, feature extraction, segmentation, and object detection and classification.[13] Retail stores use CV systems to scan and recognize items at self-checkout kiosks, allowing customers to quickly and accurately complete their purchases. Facial recognition software is another AI application based on CV techniques.

> A large hub airport representative, when asked about using CV for security at the airport stated, "I utilize AI in the security at our airport daily. Whether it is finding the right predictive actions that provide a higher indication of a car thief, and how to act before a theft occurs, rather than trying to identify after the fact. AI helps me do that, it helps me find the anomaly, or the action that might indicate an action is likely to occur."

CV enables AI systems to interpret and act on visual data. It uses ML and DL models to process images and video streams in real time. CV is arguably the most mature form of AI used in airport applications.

[12] Lloyd's Futureset, *Generative AI: Transforming the Cyber Landscape*, March 2024, https://assets.lloyds.com/media/439566f8-e042-4f98-83e5 b430d358f297/Lloyds_Futureset_GenAI_Transforming_the_cyber_landscape.pdf.
[13] International Organization for Standardization, "ISO/IEC 22989," July 2022.

Typical technical steps include image acquisition, scaling, noise reduction, contrast enhancement, segmentation, and object detection.[14] CV applications in airport security include:

- Baggage screening using x-ray imagery
- Facial recognition at checkpoints
- Detecting perimeter breaches
- Monitoring crowd density and suspicious activity

2.1.5 Generative AI

Generative AI refers to models that learn patterns from input data and generate new, synthetic content—such as text, images, audio, and video—that resembles the original data. According to NIST, these models emulate input data to produce synthetic content, making them versatile tools for a wide range of applications. Common uses include creating realistic simulations, augmenting datasets, and automating content generation. In the context of airport security, generative AI can enhance system performance by:

- Generating synthetic x-ray images to train detection algorithms without relying solely on real-world data
- Simulating rare threat scenarios for drills and preparedness, improving staff readiness
- Automatically generating post-incident summaries to support faster reporting and analysis

These applications help improve detection systems and operational readiness. However, tasks like real-time anomaly detection or equipment diagnostics are typically handled by other AI approaches, such as predictive analytics or machine learning classifiers.

Risks to consider include hallucinated or fabricated outputs, transparency concerns, and the potential for misuse (e.g., deepfakes) identified in Section 4: Potential Risks of AI Use.

LARGE LANGUAGE MODELS

Large Language Models (LLM) are a subtype of generative AI designed primarily for language tasks.[15] Generative Pre-trained Transformers (GPT) such as ChatGPT (OpenAI), Copilot (Microsoft's version of ChatGPT), Claude (Anthropic), and Gemini (Google) are the most widely used LLMs in both public and enterprise contexts. When used in airport environments, LLMs can:

- Summarize security briefings and incident reports
- Draft SOP content or assist with staff training modules
- Provide conversational access to incident logs, policy databases, or knowledge bases

Caution! LLMs can generate inaccurate or non-factual outputs ("hallucinations") and pose risks of data leakage through prompt inputs or injection

While each AI type serves a distinct function, airport security systems increasingly rely on combinations of these capabilities to address complex operational challenges. The next section explores how AI components are integrated into real-world systems to deliver coordinated, human-aligned outcomes.

[14] International Organization for Standardization, "ISO/IEC 22989," July 2022.
[15] Tom B. Brown et al., "Language Models Are Few-Shot Learners," July 22, 2020, https://arxiv.org/pdf/2005.14165.

2.2 AI Types Comparative Summary

Table 1 provides a comparative summary of AI types to support quick reference and decision-making. It highlights AI type definitions, their primary function, core techniques, security use cases, and key strengths and limitations.

Table 1. AI Technologies Comparative Summary

AI Type	Definition	Primary Function	Core Techniques	Strengths	Limitations	Security Use Cases
Machine Learning	A subset of AI that involves training algorithms to recognize patterns and make predictions based on data	Learning from data to make predictions or decisions without being explicitly programmed	Supervised learning, unsupervised learning, reinforcement learning	Ability to learn and improve from experience, adaptability to new data	Requires large amounts of data, potential for bias in training data	Analyzing data from surveillance cameras, sensors, and passenger records to identify potential threats
Deep Learning	A subset of ML involving neural networks with many layers, enabling the processing of large amounts of data	Handling complex tasks by learning from vast amounts of data through multiple layers of abstraction	CNNs, RNNs, Transformers	High accuracy, ability to learn from vast amounts of data, adaptability to various tasks	Requires significant computational resources, potential for overfitting, complexity in training	Enhancing image recognition, improving accuracy in detecting patterns and anomalies
Neural Networks	A type of ML model inspired by the structure and function of the human brain, consisting of interconnected nodes (neurons)	Handling complex tasks such as image and speech recognition	CNNs, RNNs, feedforward networks	High accuracy in complex tasks, ability to handle large amounts of data	Computationally intensive requires significant resources for training	Facial recognition, analyzing surveillance footage to detect suspicious activities
Natural Language Processing	A branch of AI focused on enabling machines to understand and respond to human language	Analyzing and interpreting communication data to identify potential threats or enhance customer service	Tokenization, parsing, sentiment analysis, machine translation, transformer-based models	Understanding and generating human language, real-time analysis	Challenges in understanding context and nuances of language, potential for misinterpretation	Detecting keywords and phrases associated with security risks, enhancing customer service

AI Type	Definition	Primary Function	Core Techniques	Strengths	Limitations	Security Use Cases
Computer Vision	A field of AI that enables computers to interpret and make decisions based on visual data	Interpreting and understanding visual information from the world	CNNs, image segmentation, object detection, transformer-based vision models	High accuracy in interpreting visual data, ability to process large datasets	Requires large datasets, computationally intensive, potential for privacy concerns	Surveillance, facial recognition, anomaly detection in images
Generative AI	A subset of AI that uses models to generate new data, such as text, images, or videos, based on learned patterns from existing data	Creating new content or data based on patterns learned from existing data	Transformer models, generative adversarial networks, variational autoencoders	Ability to create diverse and high-quality content, adaptability to various applications	Potential for misuse, ethical concerns, requires large amounts of data for training	Real-time anomaly detection, generating synthetic data for training security models

SECTION 3: AI APPLICATIONS IN AIRPORT SECURITY

AI has diverse applications within airport security, such as enhancing threat detection, improving operational efficiency, and supporting the workforce. The integration of AI in these areas has led to advancements in automated threat analysis, predictive capabilities, real-time systems, and more efficient communication systems. This section looks at the application of AI within the realms of airport operational security and law enforcement.

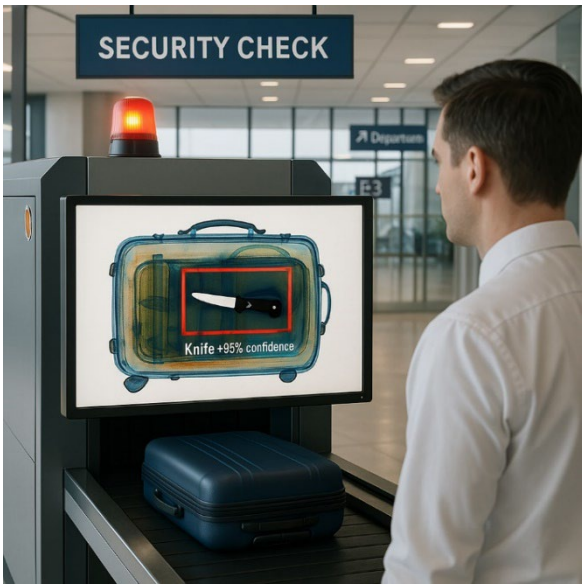
3.1 Application Domains and Techniques

The previous sections introduced foundational AI types including ML, neural networks, DL, NLP, CV, and generative AI, and how they enable systems to learn from data. This section focuses on the key application domains where these techniques are used to enhance airport security operations. Each domain discussed in this guidebook (airport security and law enforcement) leverages different aspects of AI to support real-time decision-making, threat detection, automation, and passenger engagement.

AI applications in airport security rarely rely on a single, standalone model. Instead, they typically involve multiple AI techniques operating in concert. This layered approach reflects the operational complexity of real-world scenarios, particularly those requiring object recognition, decision logic, anomaly detection, and human interaction. One example is the Automated Prohibited-Item Detection System (APIDS) in aviation worker screening areas, which integrates several AI techniques to support the identification of threat items in carry-on or personal property. In a typical APIDS deployment:

- CV algorithms first process 2D or 3D images from x-ray or computed tomography scanners, transforming raw pixel data into interpretable formats.
- Object detection models such as CNNs identify shapes that resemble objects of interest while image segmentation techniques isolate those shapes within cluttered environments.

Figure 3. Example of APIDS in Use for Airport Security



Source: Image generated by Google Gemini, July 15, 2025

- These outputs are passed to ML classifiers trained to recognize known prohibited items (e.g., firearms, explosives, blades; see Figure 3) and flag unknown threats using unsupervised learning or statistical outlier detection.
- A confidence-scoring system then applies probabilistic thresholds to determine which items are routed for human review.

In some systems, Explainable AI (XAI), which provides a means of understanding AI decisions, visually communicates the model's reasoning to support security officer decisions, improving trust, compliance, and auditability.[16] An example would be overlays such as bounding boxes or saliency heatmaps.

Importantly, some emerging systems embed generative AI interfaces to query and interact with these multi-component platforms. For example, LLMs can serve as unified, natural language interfaces that allow screeners or supervisors to query multiple subsystems using plain English prompts such as "Show me why this bag was flagged" or "Compare this detection to yesterday's flagged items." In this context, generative AI acts as an orchestration layer that abstracts complex ML operations behind intuitive commands, improving usability and reducing training time for new personnel.

Research in human-computer teaming and user-centered AI design highlights this trend as a promising development for high-stress environments such as airport security checkpoints.[17] These environments require fast decisions, minimal cognitive overload, and high levels of operator confidence in AI outputs.

This convergence of techniques represents the future of AI in aviation security: modular, interoperable systems that are transparent, explainable, and aligned with human workflows.

3.2 Airport Security and Law Enforcement

Airport security consists of the departments and divisions within an airport responsible for the physical security of the airport, including its perimeter. These security teams collaborate with local tenants, government agencies, law enforcement, and private security firms to ensure the safety of passengers, staff, and infrastructure. This section focuses on airport security, but it also speaks to areas of airport law enforcement that have many other AI use cases. For example, real-time data is collected through officer-worn camera equipment. Over time, technology companies providing these cameras have integrated many aspects of AI to analyze the large amounts of data collected and detect patterns of criminal behavior.

AI-driven solutions are increasingly being deployed to enhance threat detection, assist with aviation worker screening, and improve response times to security incidents. Key challenges in airport security include:

- **Evolving threat landscape:** Security threats are continuously changing, requiring constant updates to protocols, technologies, and response strategies.
- **Balancing security with passenger experience:** Maintaining rigorous security standards while minimizing inconvenience to travelers remains a critical challenge.
- **Data privacy and ethical considerations:** The use of AI in surveillance and biometric systems raises concerns around data protection, potential misuse, and algorithmic bias.
- **Cybersecurity risks:** As airport systems become more interconnected, protecting them from cyber threats is essential to prevent operational disruptions and data breaches.

[16] Javier Viaña et al., "Explainable Algorithm to Predict Passenger Flow at Cincinnati/Northern Kentucky International Airport," *Transportation Research Record* 2678(2) (2023): 839–62.
[17] Lauren Kahn, Emelia S. Probasco, and Ronnie Kinoshita, *AI Safety and Automation Bias: The Downside of Human-in-the-Loop* (Center for Security and Emerging Technology, November 2024), https://cset.georgetown.edu/wp-content/uploads/CSET-AI-Safety-and-Automation-Bias.pdf; U.S. Department of Homeland Security, "Screening at Speed," March 2024, https://www.dhs.gov/sites/default/files/2024-03/24_0304_st_ScreeningatSpeed_March2024.pdf.

- **Regulatory compliance:** Navigating complex and resource-intensive compliance requirements, including TSA, FAA, and GDPR regulations, and other applicable privacy laws—demands significant coordination and oversight.
- **System integration:** Integration of AI solutions into existing security frameworks must be seamless to avoid inefficiencies or operational gaps.
- **Human oversight and accountability:** Striking the right balance between automation and human judgment is vital. Clearly defined roles and responsibilities are necessary for monitoring AI system performance and ensuring accountability.
- **AI literacy and training:** Effective deployment of AI in airport security depends on operator understanding. Training must empower personnel to interpret AI decisions and know when and how to challenge them.

A medium hub airport reported that the usage of AI to improve license plate recognition of greater than the typical 95% has translated in to an improved process and vehicle signature identification.

Applications of AI in airport security and law enforcement aim to improve efficiency, enhance safety, and provide more effective responses to various situations. Table 2 provides a list of relevant AI uses.

Table 2. AI Uses in Airport Security and Law Enforcement Operations

Area Within Airport Security and Law Enforcement Operations	Description of How AI is Helping	AI Types Used
Responding to mental health emergencies	AI analyzes call data and behavioral cues to assist in triaging and dispatching appropriate responders.	ML, NLP, LLMs
Documenting perceived race at traffic stops	AI automates demographic data captured from bodycam footage and officer reports.	CV, ML, NLP
Real-time language translation during interactions	AI detects the spoken language of individuals and translates it for officers in real time. It also translates the officer's speech back to the individual's language, enabling two-way communication without delays or external translators. This reduces misunderstandings and improves safety during high-pressure situations.	NLP, Speech Recognition, ML
Predicting and preventing criminal activities	AI identifies high-risk individuals or locations by analyzing crime patterns and social data.	ML (graph-based), Neural Networks
Resource deployment decisions	AI forecasts demand and optimizes responder allocation using real-time and historical data.	ML, DL
Digital forensic image analysis	AI categorizes and flags relevant images from seized devices to accelerate investigations.	CV, DL
Public communication via chatbots	AI-powered bots handle routine inquiries and disseminate emergency updates.	NLP, Generative AI, LLMs

Area Within Airport Security and Law Enforcement Operations	Description of How AI is Helping	AI Types Used
Cybercrime defense and automation	AI detects anomalies, analyzes malware, and automates threat intelligence workflows.	Graph-based ML , Neural Networks, Anomaly Detection with DL, LLMs (intel summarization & playbooks)
Gunshot detection and tracking	AI identifies gunshot sounds, locates origin, and integrates with video feeds for tracking.	ML, CV
Facial recognition for watch lists	AI matches faces in real time against databases to alert authorities.	CV, DL, ViTs
Video redaction for public release	AI automates the removal of personally identifiable information from video footage.	CV, ML, DL for object/person detection
Biometric fraud detection	AI compares facial and fingerprint data to verify identities and detect fraud.	CV, ML, multi-modal biometrics (face + fingerprint + voice)
Network anomaly detection	AI learns normal traffic patterns to flag suspicious deviations.	ML, Neural Networks, unsupervised learning
Image object identification	AI detects and classifies objects in images for investigative use.	CV, DL, ViTs
Victim risk assessment	AI evaluates personal and environmental factors to assess victimization risk.	ML, NLP (text-based), LLMs
Crime data analysis	AI uncovers trends and correlations in crime reports and statistics.	ML, NLP, LLMs
Risk prediction	AI forecasts potential future threats based on behavioral and environmental data.	ML, Neural Networks
Evidence preservation and identity protection	AI redacts sensitive information to protect officers and witnesses.	CV, ML, NLP (text redaction)
Data correlation and pattern discovery	AI links disparate data sources to reveal hidden patterns and associations.	ML, Neural Networks

3.3 Airport Use Cases

AI technologies are creating operational efficiency in airports by automating and optimizing various processes. For example, AI-powered predictive maintenance systems analyze data from sensors embedded in airport infrastructure, such as escalators and HVAC systems, to predict potential failures and schedule proactive maintenance. This reduces downtime and avoids costly disruptions. AI-driven dynamic queue management systems are also being used to optimize resource allocation at security checkpoints, minimizing wait times and enhancing passenger flow. Airports implementing these AI solutions have demonstrated measurable benefits, including reducing equipment downtime and cutting

passenger wait times by up to 20%, which translates into significant operational cost savings and improved traveler satisfaction.[18]

The integration of AI into airport security has yielded numerous success stories, demonstrating how AI can enhance security protocols and operational efficiency in diverse airport environments. For instance, Punta Gorda Airport in Florida implemented an AI-based secure access monitoring system that seamlessly integrates with the airport's existing access control and security cameras. This system has significantly improved the accuracy of identifying unauthorized access incidents, such as piggybacking or tailgating, and reduced the need for round-the-clock staffing.[19]

AI can also be used to identify and pinpoint the origin of gunshots in an airport terminal. These types of systems alert law enforcement agencies of gunshot events and can integrate with video analytics to track a suspect's movements. This technology has been deployed at several US airports, including Charleston International Airport, Los Angeles International Airport, Columbus Airport, and West Virginia International Yeager Airport.[20]

Sofia Airport in Bulgaria piloted a system that integrates advanced computer vision and deep learning models to identify weapons and detect masked faces in real time to enhanced situational awareness and reduce reliance on manual screening. Tested under diverse operational conditions, the system demonstrated seamless interoperability with existing security infrastructure and incorporated human-in-the-loop oversight to minimize false positives. This initiative underscores how AI technologies can significantly improve security protocols and operational efficiency in complex airport environments.[21]

In the outreach phase of this project, the following additional case studies and pilots were uncovered:

Medium Hub Airport #1 – AI for Radio Transcription (Project 1)
This airport deployed AI-powered speech-to-text technology to transcribe radio communications between security teams and operations staff. The system creates searchable transcripts and keyword alerts, improving situational awareness and reducing manual documentation time.

Medium Hub Airport #1 – AI for Real-Time Alerts (Project 2)
AI analytics were applied to monitor operational data streams to trigger real-time alerts for anomalies, such as perimeter breaches or suspicious activity. This enhanced situational awareness and accelerated incident response compared to manual monitoring.

Medium Hub Airport #2 – Video Analytics for Perimeter Security
AI-driven video analytics were used to detect perimeter intrusions and classify objects (e.g., distinguishing humans from animals). The system aimed to reduce nuisance alarms and improve detection accuracy, although extensive model training was required to address false positives.

---

[18] Mahmood AlSeddiqi, "The Power of AI and Machine Learning for Airport Operations," *International Airport Review*, September 18, 2024, https://www.internationalairportreview.com/article/222537/the-power-of-ai-and-machine-learning-for-airport-operations/
[19] "Enhancing Airport Security: Transformative Role of AI Across the Industry," *Airport Cooperative Research Program | Applied Technology in Airports*, June 17, 2024, https://crp.trb.org/acrptransformativetech/applied-technology-in-airports/enhancing-airport-security-transformative-role-of-ai-across-the-industry/.
[20] "Enhancing Airport Security: Transformative Role of AI Across the Industry."
[21] Antoaneta Simeonova and Angel Krumov, "AI Integration in Airport Security: A Case Study of Sofia Airport within Bulgaria's Critical Infrastructure Framework," *International Scientific Journal "Security & Future"* VIII, no. 3 (2024): 76–78.

Large Hub Airport – Queue Monitoring
AI-powered dynamic queue management analyzed passenger flow at security checkpoints to optimize staffing and reduce wait times. The system leveraged real-time data to predict congestion and adjust resource allocation proactively.

Large Hub Airport – Cybersecurity Anomaly Detection
AI was deployed to monitor network traffic and detect anomalies indicative of cyber threats. The system used machine learning models to identify deviations from normal patterns and automate incident prioritization, reducing response times for cybersecurity events.

Non-Aviation Sector – Predictive Maintenance
AI analyzed Internet-of-Things (IoT) sensor data from escalators, HVAC systems, and other infrastructure to predict failures and schedule proactive maintenance. This reduced downtime and extended asset life, improving operational efficiency.

Non-Aviation Sector – Cybersecurity Automation
AI-driven cybersecurity tools automated threat detection and incident response workflows. These systems analyzed logs and threat intelligence feeds to identify vulnerabilities and initiate remediation actions without manual intervention.

See Appendix A for more detailed information on each of these airport use cases.

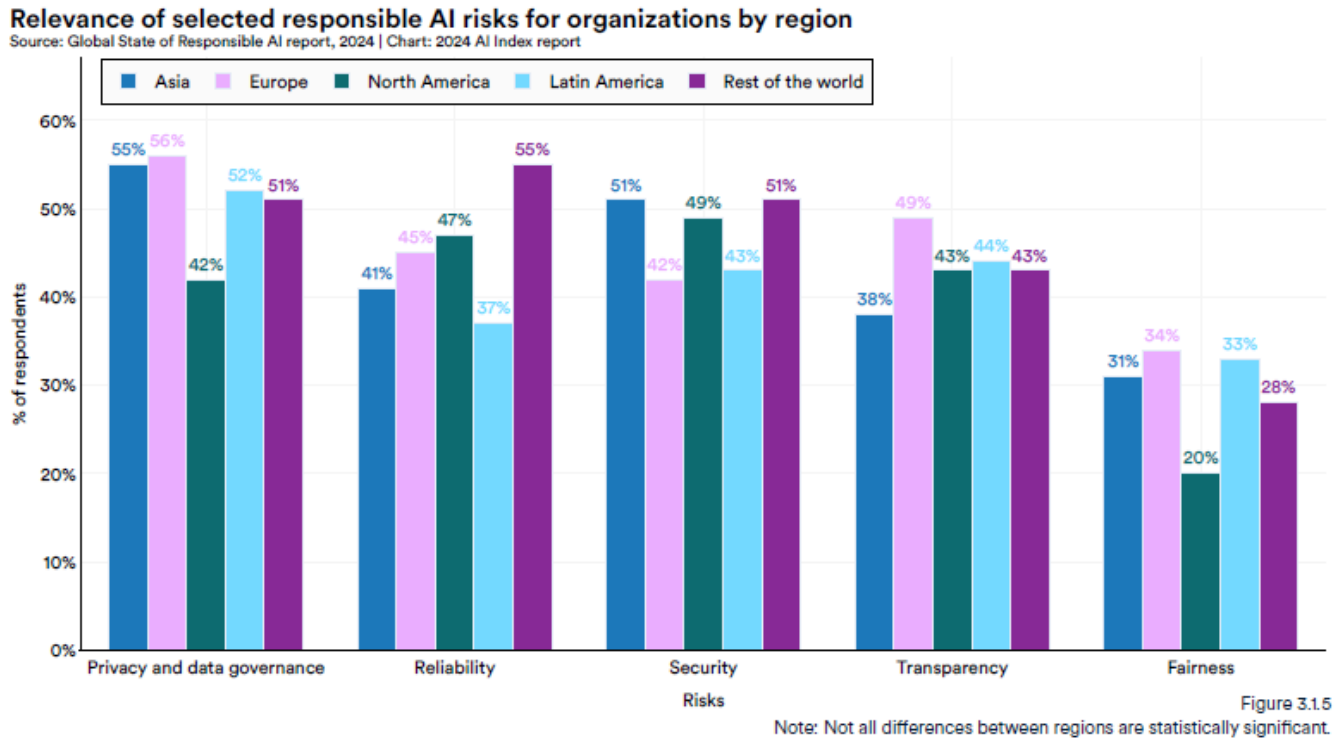
SECTION 4: POTENTIAL RISKS OF AI USE

The use of AI in security applications offers significant benefits, but it also presents various risks that must be carefully managed. Understanding these risks is crucial for informed decision-making and the responsible deployment of AI technologies. This section outlines the potential risks associated with AI use, including false positives/negatives, bias and fairness, over reliance on the machine (automation bias), the unexplainable "black box," lack of human-in-the-loop/human oversight, contract liability, and cybersecurity threats. Additionally, this section aims to help in identifying potential security risks, explore strategies for risk mitigation, and to perform continual assessment and create response plans.

4.1 Risk Perception

Researchers from Stanford teamed with global professional services company Accenture to find the relevance of selected responsible AI risks for organizations per region. The Stanford University Human-Centered Artificial Intelligence 2024 index report found that the following areas of organizational risks scored higher than most: privacy and data governance, reliability, security risks, transparency, and fairness, as depicted in Figure 4.[22] Comments made during outreach for this guidebook also touched on the same categories of concern.

Figure 4. Relevance of AI Risks for Organizations by Region



[22] Nestor Maslej et al., *The AI Index 2024 Annual Report* (Stanford University, Stanford, Calif.: AI Index Steering Committee, Institute for Human-Centered AI, 2024), https://hai.stanford.edu/assets/files/hai_ai-index-report-2024-smaller2.pdf.

4.2 Data and Privacy Risks

The integration of AI, particularly LLMs and advanced analytics, often requires access to vast amounts of data, some of which may be highly sensitive. Mismanagement of this data poses significant privacy and security risks. Airport security operations frequently deal with personally identifiable information, surveillance footage, and law enforcement data, making robust data governance paramount.

> Giving a large-language model (LLM) access to the organizational data is a big concern. The underlying data classification needs to be identified, processed, and secured first.
> – Medium Hub Airport

SENSITIVE DATA ACCESS AND USAGE

A primary concern is granting AI systems, especially public or general-purpose LLMs, access to internal organizational data, including sensitive information like video clips or law enforcement databases such as the National Crime Information Center (NCIC). Without stringent controls, this could lead to unintended data exposure or misuse. Personnel must question what data AI uses and how it is protected.

DATA CLASSIFICATION AND HYGIENE

Inadequate data classification (e.g., public vs. non-public documents) can inadvertently expose sensitive information to AI systems designed for broader access. Establishing clear data hygiene practices and ensuring data is correctly organized and marked are foundational to mitigating this risk. Section 6 provides considerations for working with airport data.

> Just like you wouldn't put an Alexa device in the same room as the NCIC computer, you should not have co-pilot on the computer that also has NCIC.
> – Small Hub Airport

LEGAL AND POLICY FRAMEWORKS

Airports must develop clear legal documents, IT systems, and written policies around AI use, especially concerning data privacy. This includes transparently informing the public and personnel about AI's role in generating or manipulating information and the cautious approach to sharing data for AI training. This area is explored in more detail and depth in Section 5: Privacy, Legal and Regulatory Considerations.

INTRUSION AND DATA LEAK POTENTIAL

AI processing large datasets increases the surface area for potential data leaks or intrusions into personal spaces. While AI can support enforcing privacy rules, AI systems themselves can become vulnerabilities if not properly secured.

SECURITY RISKS IN AI SYSTEMS

It is crucial to balance flexibility and scalability with considerations for data sovereignty and latency, particularly when using cloud-based solutions. Compliance with regulations such as GDPR and California Consumer Privacy Act (CCPA) is vital to mitigate reputational damage and financial penalties. AI developers must implement proactive security measures, including:

- Continuous monitoring and regular updates
- Rigorous penetration testing
- Strict adherence to regulatory requirements

4.3 AI System Reliability and Accuracy Risks

For security applications where precision is critical, the reliability and accuracy of AI systems are constant concerns. Errors or malfunctions can have serious consequences, impacting operational efficiency and safety.

FALSE POSITIVES / NEGATIVES

AI systems, particularly in surveillance or detection, can generate a high number of false positives. For example, security cameras using AI might detect squirrels or birds as potential threats, leading to nuisance alarms that can overwhelm personnel and desensitize them to genuine threats.

> "Until AI is better at determining false positives, we still see the need for the human interaction element (e.g., mass communications or reporting to TSA). Corrective actions are still around AI being reviewed by humans."
> – Medium Hub Airport

Facial recognition systems are increasingly deployed at airport security checkpoints to assist in verifying identities, automating entry/exit, and matching individuals against government watchlists. These systems typically function by comparing real-time or post-event surveillance images against enrolled biometric templates or watchlist images. Despite technological advancements, such systems remain vulnerable to false positives and false negatives, which can compromise security, infringe on civil liberties, and erode public trust. According to NIST testing, false positive rates (when the system incorrectly identified a non-threat as a threat) varied dramatically across demographic groups, by as much as a factor of 720, with one algorithm showing a false match rate of 1 in 26,000 for Polish men aged 35–50 compared to 1 in 35 for Nigerian women aged 65 and over. False negative rates (when the system failed to identify an actual threat), while less extreme, still varied by a factor of 3 across groups. Importantly, false negatives were often linked to poor image capture conditions, such as underexposed images of dark-skinned individuals, highlighting the role of environmental and technical factors like lighting, camera quality, and positioning in system accuracy.[23] These errors can lead to unnecessary interventions or missed security threats, respectively.

INACCURACY AND ERRORS

Airport personnel expressed wariness about the current accuracy of AI assistance. Systems may not always work as expected, or they might provide incorrect decisions or guidance, leading to incorrect assessments or missed threats. This underscores the need for continuous human review and correction.

DEPENDABILITY AND MALFUNCTIONS

The dependability of AI technology is still an issue. Like any technology, AI systems can malfunction, and a heavy reliance on them without sufficient human oversight can be dangerous, especially when quick, decisive action is required.

AUTOMATION BIAS

Automation bias is the tendency for an individual to over-rely on an automated system. It can lead to increased risk of accidents, errors, and other adverse outcomes when individuals and organizations favor the output or suggestion of the system, even in the face of contradictory information. Automation bias can erode the user's ability to meaningfully control an AI system. Meaningful human control requires that users understand the AI's role, limits, and uncertainty, and retain the authority to override it. Automation bias undermines this by shifting decision authority informally from the human to the system. In practice, this can create a false sense of accountability, where humans are responsible in theory but disengaged in execution. This gap poses ethical, legal, and operational risks. As AI systems have proliferated, so too have incidents where these systems have failed or erred in various ways, and human users have failed to correct or recognize these behaviors. The following examples were summarized from case studies detailed by Kahn, et al:[24]

[23] Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (NISTIR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280
[24] Kahn, Probasco, and Kinoshita, *AI Safety and Automation Bias: The Downside of Human-in-the-Loop*.

- Tesla Autopilot: Drivers placed excessive trust in automated driving features and failed to intervene despite clear environmental cues, demonstrating how user over-reliance can override situational awareness.
- Boeing: Commercial aircraft flight crews relied on automated system behavior without fully understanding system limitations, contributing to delayed or incorrect responses when the automation behaved unexpectedly.

These examples show that automation bias can emerge even among trained professionals and may be mitigated through clear policy, targeted training, and governance measures that reinforce human authority. The risk of automation bias is particularly high for autonomous systems and is further compounded by organizational culture and operator competence.

BLACK BOX AI

Black box AI refers to the operational characteristics of certain advanced AI models, particularly those based on DL architectures, where the intricate layers of computation make it exceptionally challenging to discern how specific inputs lead to outputs. These models, while capable of achieving high levels of predictive accuracy by identifying complex patterns in large datasets, often lack transparency in their decision-making processes. DL has demonstrated remarkable success in various security applications, including image recognition for threat detection in baggage and biometric identification. However, the complexity that enables these models' performance also contributes to their opacity, making it difficult for even the developers to fully comprehend the reasoning behind specific decisions. This lack of insight into the "how" of AI decision-making poses significant risks, especially in a safety-critical domain like airport security.[25]

The risks associated with deploying black box AI in airport security are multifaceted and warrant careful consideration. One primary concern involves security vulnerabilities and the potential for exploitation. The lack of transparency can make it harder to detect anomalies, data breaches, or even malicious manipulations of the AI system. For instance, if an AI-powered system flags a passenger as a potential threat, the inability to understand the basis for this decision can hinder effective intervention and may lead to erroneous actions. Furthermore, black box AI models are susceptible to biases present in their training data, which can result in discriminatory outcomes in applications like facial recognition. If an algorithm is disproportionately trained on certain demographics, it may exhibit lower accuracy or higher false positive rates for other groups, potentially leading to unfair targeting.[26]

HUMAN-IN-THE-LOOP VS. HUMAN OVERSIGHT

Human-in-the-loop (HITL) and human oversight are closely related yet functionally distinct mechanisms in AI risk governance. HITL refers to the real-time operational involvement of a human who reviews and interprets the AI system's outputs before action is taken. For example, in an APIDS deployment, if the AI flags a prohibited item in a carry-on bag, the HITL protocol requires a security officer to visually confirm the threat on-screen before initiating a physical bag search. This decision-making must be contextual, responsive, and bounded by procedural guidance.

In contrast, human oversight is a strategic, life cycle–wide framework embedded in design and policy that enables meaningful human control, such as HITL. It ensures that the human operator has the tools

[25] Brandon L. Garrett and Cynthia Rudin, "The Right to a Glass Box: Rethinking the Use of Artificial Intelligence in Criminal Justice," *Cornell Law Review* 109 (2024): 561–627.
[26] Eugene Pik, "Airport Security: The Impact of AI on Safety, Efficiency, and the Passenger Experience," *Journal of Transportation Security* 17, no. 1 (April 8, 2024): 9, doi:10.1007/s12198-024-00276-6.

and authority to intervene when necessary. Effective human oversight requires that the operator is provided with:

- Clearly defined decision boundaries
- A structured escalation pathway
- A chain of accountability tied to measurable outcomes and audit logs

This is especially vital in systems that are adaptive or interact with the environment, such as those using CV like in APIDS, or systems that apply reinforcement learning for optimized security resource deployment. These systems are susceptible to performance drift, where model accuracy may degrade over time due to environmental or data shifts. Baseline performance metrics should be established during validation and continuously compared to operational outcomes. This ensures deviations are traceable and attributed appropriately to either operator behavior or model instability.

NIST emphasizes that AI systems should support meaningful human control, enabling understanding, intervention, and override where necessary.[27] ISO/IEC 38507 reinforces that human oversight is not merely an operational task but a governance requirement.[28] Airport security operations must embed structures that support auditability, escalation, and accountability ensuring that human intervention is both possible and effective across the system life cycle.

Airport leadership should actively engage corporate governance teams to ensure AI technologies align with existing policies and ethical standards. Establishing clear policies and measures will support the responsible use of AI in operational environments.

4.4 Cybersecurity and Malicious AI Use Risks

AI can be a powerful tool for enhancing cybersecurity, but it can also become a target for attacks or be leveraged by malicious actors.

Dark LLMs, such as WormGPT, can be used by bad actors to generate malicious code, fabricate information, or analyze law enforcement movements, giving them an advantage in planning attacks against airport infrastructure or personnel.

> "As AI is easier to garner information or develop an attack or fabricate information and put out on internet, etc., it can be so real at times. Other tools and others are created for evil, such as WormGPT; it will generate code that is malicious."
> – Small Hub Airport

One airport expressed concern that widely available AI tools could be misused to undermine law-enforcement effectiveness by enabling impersonation, generating deceptive digital evidence, exploiting over-reliance on automated systems, or increasing the difficulty of verifying information. These uses could delay response, erode trust in legitimate authority, and increase risk to law-enforcement personnel.

By understanding and proactively addressing potential risks, airport personnel can implement AI solutions more responsibly, enhancing security operations while safeguarding privacy, ensuring reliability, and maintaining public trust.

[27] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*.
[28] International Organization for Standardization, "ISO/IEC 38507:2022 Governance Implications of the Use of Artificial Intelligence by Organizations" (Geneva, Switzerland, 2022), https://www.iso.org/standard/56641.html.

VULNERABILITY OF AI SYSTEMS

AI systems are software platforms that can themselves be targeted or misused if not properly secured. Common vulnerabilities include weak governance over who can access or configure AI tools, unclear acceptable-use policies, and insufficient monitoring of how AI systems are connected to sensitive data. For example, an AI system integrated with access-control logs or surveillance feeds could be misused, manipulated through crafted inputs, or accessed beyond its intended purpose.

AI deployments may also be exposed to risks such as unauthorized access, data leakage, prompt manipulation, or exploitation of system interfaces, sometimes without directly breaching the underlying infrastructure.

As AI systems increasingly rely on cloud services, frequent updates, and third-party components, weaknesses in any one area can cascade across connected security systems, making strong controls and clear accountability essential.

SUPPLY CHAIN AND TRAINING RISKS

Using AI systems developed or trained by third parties can introduce hidden security risks, particularly when airports do not have full visibility into how those models were built or what data was used to train them. For example, if training data is crowdsourced or drawn from external sources (not the airport client), sensitive operational information may be unintentionally exposed, reused, or embedded into models beyond the airport's control. Airports should therefore evaluate AI vendors' cybersecurity practices, data-handling policies, and training data sources to ensure sensitive information is protected and not incorporated into AI systems without appropriate safeguards.

4.5 Bias, Fairness, and Ethical Risks

AI systems can perpetuate and even amplify existing biases present in the training data. For example, facial recognition technology has been shown to have higher error rates for certain demographic groups, which can lead to unfair treatment and potential discrimination. Bias in AI systems can undermine public trust and lead to legal and ethical challenges.

Bias refers to measurable, often unintentional, differences in how AI systems perform across groups. One example is higher false match rates for people in certain racial or age demographics. Fairness, on the other hand, is a broader normative concept concerned with whether the system's outcomes are just, equitable, and aligned with legal or ethical expectations. While NIST Special Publication 1270 provides detailed statistical evidence of bias, such as the stark disparity in false match rates across demographic groups, it also acknowledges that achieving fairness requires more than technical improvements.

Fairness involves contextual judgement, including how risks and burdens are distributed across society, including which passenger groups, frontline personnel, and airport operators are most affected by system errors; whether the system reinforces or mitigates existing inequalities; whether those impacts are transparently understood, justified, and appropriately mitigated through policy and governance decisions; and whether affected individuals are aware of and can contest decisions.[29] For example, as noted by Kyriazanos et al., even when statistical bias is reduced, AI systems deployed at airport checkpoints may still be perceived as unfair if they lack transparency, explainability, or accountability

[29] National Institute of Standards and Technology, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, March 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

mechanisms. For airports, this means fairness must be addressed not only in algorithm performance, but also in policy, deployment practices, and stakeholder engagement.[30]

A key case that guides AI risk is that of the Federal Trade Commission v. Rite Aid.[31] This case is an example of federal regulatory enforcement tied to AI risk management failures. The Federal Trade Commission's complaint explicitly details how Rite Aid's facial recognition technology (e.g., algorithmic bias), deployed for loss prevention, disproportionately produced false matches for individuals based on race and gender, particularly affecting women and people of color. It underscores several key concerns: the risk of algorithmic bias, inadequate vendor oversight, harm to individuals, and regulatory non-compliance. It provides direct evidence of the potential risks of AI use, and can be considered essential guidance for addressing the privacy, legal, regulatory, and deployment aspects of airport AI initiatives. This case reinforces the need for proactive risk identification, mitigation strategies, and compliance frameworks tailored to high-risk AI applications.

AI bias arises when human biases inadvertently influence training data or algorithms, leading to skewed and potentially harmful outcomes. It is essential that AI applications in airport security avoid reinforcing human biases. Transparency and explainability play a critical role in this effort by allowing stakeholders to understand AI-driven decisions and fostering trust in technology. Additionally, safeguards must be implemented to protect privacy, civil rights, and civil liberties. Collaborating with vendors who prioritize responsible AI development is crucial to achieving these goals. Key vendor application considerations include the following:

- **Responsible and trustworthy implementation:** A vendor demonstrates responsible implementation by designing AI systems with HITL controls and human oversight, such as enabling supervisors to override or suspend systems when performance drift or elevated false positives are detected.
- **Rigorous effectiveness testing:** A vendor supports rigorous testing by validating AI performance through pilot deployments and phased rollouts, and by conducting ongoing performance monitoring, red-team testing, and false-positive analysis.
- **Robust safeguards for privacy, civil rights, and civil liberties:** A responsible vendor enforces safeguards such as data minimization, encryption, and role-based access control and ensures compliance with privacy laws, consent requirements, and ethical usage boundaries.
- **Avoidance of inappropriate biases:** A vendor addresses bias by testing AI models across demographic conditions, monitoring false-match disparities, and retraining models when inequities are detected while embedding fairness considerations into deployment and governance decisions, not solely technical tuning.
- **Transparency and explainability for stakeholders:** A vendor provides transparency by offering explainable AI outputs such as confidence scores, visual indicators, and audit logs. and by ensuring operators, supervisors, and legal stakeholders can understand, review, and contest AI-assisted decisions.

[30] Kyriazanos, Thanos, and Thomopoulos, "Automated Decision Making in Airport Checkpoints: Bias Detection Toward Smarter Security and Fairness."
[31] Federal Trade Commission v. Rite Aid Corporation (Eastern District of Pennsylvania Federal Court Pending).

ETHICAL RISKS IN AI DEPLOYMENT

Ethical risks stem from the potential for AI systems to reinforce biases, resulting in unfair treatment of certain groups. Addressing these concerns requires AI applications to prioritize equity and fairness while maintaining transparency. Understanding how AI decisions are made is vital for operational stakeholders, necessitating the implementation of safeguards to uphold privacy and civil liberties.

A small hub airport public safety employee expressed concerns about bad actors gaining an edge using AI tools to potentially hurt law enforcement staff.

Developers play a pivotal role in mitigating ethical risks by creating AI solutions that are transparent and comprehensible to all stakeholders. A phased approach to AI deployment, including comprehensive assessments, pilot projects, and partnerships with technology providers, is recommended.

SOCIAL RISKS AND MITIGATION STRATEGIES

AI systems can introduce social risks, including misinformation, social isolation, and erosion of public trust. These risks can fragment communities and undermine confidence in institutions.

- **Hallucinations and deepfakes:** AI-generated outputs can occasionally contain fabricated or contextually inaccurate information, a phenomenon known as hallucination. While typically unintentional, these outputs can erode public trust if not properly flagged and contextualized. In contrast, deepfakes involve the deliberate use of AI to fabricate realistic yet deceptive media. Both challenges underscore the need for rigorous validation protocols, algorithmic transparency, and proactive collaboration with media organizations to maintain information integrity and public confidence.
- **Social isolation:** Over-reliance on AI for customer interactions may reduce human contact. AI solutions should complement, rather than replace, human interactions to maintain a personalized experience.
- **Erosion of trust:** Transparent communication of AI purposes and benefits is crucial to maintaining public confidence. Implementing privacy safeguards and adhering to regulations will further reinforce trust.

A phased approach to AI deployment, including pilot projects and scalable implementation, ensures AI systems are optimized and reliable before full-scale adoption.

4.6 Strategies for Risk Mitigation

Mitigation of risks associated with AI involves a forward-thinking and multi-faceted approach that extends beyond technology to include governance, personnel, and proactive security measures. A foundational element of this strategy is recognizing that AI systems are vulnerable to unique and sophisticated threats. According to DHS's AI roadmap, "Malicious actors can exploit AI not only to develop new cyberattack tools but also to directly compromise security systems by feeding them 'poisoned data.'"[32] Examples could include an attacker subtly manipulating the data fed to a surveillance system over time, teaching it to ignore a specific threat, or causing a critical sensor within an access control system to fail or shut down.

[32] U.S. Department of Homeland Security, *Artificial Intelligence: Roadmap 2024*, 2024, https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf.

Testing and evaluation of AI performance should be performed throughout system deployment and life cycle.

To counter these threats proactively, airport security leadership should adopt a schedule of rigorous and continuous testing, as emphasized in the DHS Roadmap. This involves establishing a robust testing and evaluation framework that validates an AI system's performance and security before its deployment and throughout its life cycle. A key component of such a framework is adversarial testing, where internal or external "red teams" conduct ethical hacking exercises designed to mimic real-world threats. For instance, these teams could attempt to fool facial recognition systems with spoofed credentials or test if surveillance analytics can be misled by manipulated video feeds. Another option may include adopting a model like a bug bounty program—inviting vetted security researchers to find vulnerabilities in the AI-powered system. The findings from these tests or assessments are invaluable for driving critical security enhancements and ensuring AI tools remain effective and resilient against manipulation.

This section outlines a methodology for strategic risk mitigation by categorizing steps within four areas: foundational, operational and procedural enhancements, technical and systematic safeguards, and advanced collaboration and infrastructure.

FOUNDATIONAL STEPS

Adopt a Phased Approach: To mitigate implementation and operational risks, airport personnel should adopt a phased approach to AI deployment, allowing for gradual adoption, thorough testing/assessing and refinement based on real-world feedback.

Engage Stakeholders and Align Goals: Mitigate integration risks and foster broader acceptance by actively engaging all relevant stakeholders and ensuring AI initiatives are closely aligned with overarching airport leadership goals and security objectives.

Conduct Comprehensive Cost-Benefit Analyses: To mitigate financial and operational decision-making risks, conduct comprehensive CBAs that evaluate potential financial impacts and returns, ensuring well-informed strategic investments in AI technology.

OPERATIONAL AND PROCEDURAL ENHANCEMENTS

Incorporate Human Oversight: Mitigate errors and ensure appropriate use of AI outputs by incorporating robust human oversight into AI decision-making processes to maintain human accountability and intervention capabilities.

Stay Informed on Regulations: To mitigate compliance risks, airport personnel must stay informed of evolving legal and regulatory requirements related to AI, ensuring operations remain compliant and adaptable to legislative changes. Section 5 of this guidebook provides an overview of legal and regulatory considerations.

Implement Regular Audits and Testing: Mitigate risks of bias, inaccuracy, and system errors by implementing regular audits and testing protocols for all AI systems and AI integrations.

Provide Continuous Staff Training: To mitigate operational risks arising from a lack of proficiency, provide continuous staff training and capacity-building programs to enhance workforce readiness and optimize AI usage.

TECHNICAL AND SYSTEMIC SAFEGUARDS

Establish Strict Data Privacy and Security Safeguards: Mitigate data privacy and security breach risks by establishing and enforcing strict safeguards that protect sensitive information and ensure regulatory compliance.

Implement Robust Cybersecurity Measures: To mitigate risks from malicious attacks and misuse, implement robust cybersecurity measures specifically designed to protect AI systems and their underlying infrastructure.

Improve Data Quality: Mitigate risks of AI bias and inaccurate performance by actively working to improve the quality of training data, ensuring it is diverse, representative, and free from errors.

ADVANCE COLLABORATION AND INFRASTRUCTURE

Collaborate with Responsible AI Vendors: To mitigate ethical and operational risks stemming from third-party solutions, collaborate exclusively with vendors who clearly prioritize and demonstrate a commitment to responsible AI development, ensuring alignment with ethical AI practices and compliance requirements.

Ensure Vendor Oversight and Accountability: Mitigate risks associated with external dependencies by establishing strong vendor oversight and accountability frameworks, including contractual obligations and performance metrics that ensure transparency, traceability, and enforceable remediation processes. Section 5 of this guidebook provides an overview of legal and regulatory considerations for vendor risk.

Institute a Vendor Feedback Loop: To mitigate persistent anomalies and performance issues, institute a formal feedback loop to vendors, ensuring that anomalies are reported, and they are held accountable for corrective measures via, for example, over-the-air updates, controlled patch implementation, or other suitable measures that reduce or remove the anomaly.

Implement Scalable AI Solutions: Mitigate future operational and adaptability risks by implementing scalable AI solutions specifically tailored to evolving airport operational needs, providing flexibility and ensuring AI can adapt to changing requirements.

SECTION 5: PRIVACY, LEGAL, AND REGULATORY CONSIDERATIONS

As airports consider potential use cases for AI systems, it is critical they also consider applicable legal requirements and guidance. Given the evolving nature of this technology, these requirements and guidance change, so periodic reviews of applicable statutes and regulations are necessary to promote compliance. Airports should involve their legal and compliance teams in proposals as soon as possible to identify potential roadblocks or prohibitions early, thereby helping the operational team design the program with compliance in mind from the start.

CONSIDERATIONS AROUND PRIVACY

At this point, the most significant restrictions and requirements related to the use of AI involve privacy concerns. Specifically, the collection, processing, and potential exposure of sensitive information is addressed in existing law. Each US state has laws covering data breaches affecting Personal Information (PI) or Personal[ly] Identifiable Information (PII).[33] While the specific definitions vary by state, each state's laws address unauthorized access to and/or acquisition of the specified data. Where qualifying information is shared with an AI system, there is a real risk that the information could be exposed or subsequently shared with unauthorized persons. Two primary ways this may occur are through access by the AI system developers or by data/information leakage.[34] While such disclosures may not always be considered a "data breach," use of public AI systems or insecure systems heighten these privacy risks.

In addition to data breach laws, US states and foreign governments are increasingly enacting comprehensive privacy laws. While the EU's GDPR and California's CCPA, as amended by the California Privacy Rights Act, are some of the best-known examples in the US, there are a growing number of these laws. As of early 2025 there were nineteen enacted state comprehensive privacy laws, many of which were already in full effect, and more were under consideration.[35] Other jurisdictions, including the EU, Canada, Brazil, and China, also have comprehensive privacy laws that may apply extraterritorially. For example, both the EU and China apply a "targeting criterion" for data subjects who are in their jurisdictions.[36] The targeting criterion means that if an airport (even one located in the US) offers specific services to people located in the EU or China, or monitors their behavior while they are there, that airport must comply with those foreign privacy laws.

The applicable laws for each airport will depend on their location, activities, and the domicile of those whose personal information is being collected and processed.

As of early 2025, many laws governing the use of AI systems are concerned with employment or general consumer protections.[37] While these laws primarily focus on privacy protections, they also emphasize evaluating and controlling against biases in AI systems. It may appear counterfactual, but

---

[33] See Alabama Legislature, *Alabama Data Breach Notification Act of 2018*, vol. 8-38–1 to 8-38–12, 2018, https://alison.legislature.state.al.us/code-of-alabama?section=8-38-1; see also Wyoming Legislature, *Article 5 - Credit Freeze Reports*, vol. 40-12–501 to 40-12–502, n.d., https://wyoleg.gov/statutes/compress/title40.pdf.

[34] See National Institute of Standards and Technology, "Information Leakage - Glossary | CSRC," *National Institute of Standards and Technology*, n.d., https://csrc.nist.gov/glossary/term/information_leakage.

[35] "US State Privacy Legislation Tracker," *Iapp25*, July 7, 2025, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[36] See, Article 3 of the GDPR available at https://gdpr-info.eu/art-3-gdpr/ and the English translation of China's Personal Information Protection Law, Chapter I, Article 3 available at http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

[37] See The New York City Council, Local Law 144. Available at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&Options=ID|Text|&Search=. See also the National Association of Insurance Commissioners Model Bulletin on the Use of AI by Insurers, available at https://content.naic.org/sites/default/files/inline-files/2023-12-4 Model Bulletin_Adopted_0.pdf.

"bias" in the outputs of an AI system designed for security—specifically statistical bias toward identifying anomalies—is an intended outcome. This is because security operations are designed to look for patterns in behavior that deviate from the norm to identify suspicious and/or potentially malicious activity. However, this must be balanced against discriminatory bias, which is legally and ethically prohibited..

Federal regulatory action in this space has been limited. TSA, and the US Cybersecurity and Infrastructure Security Agency (CISA), are concerned with the security of systems used at or in support of airports. However, at the time of writing, TSA regulations have not been specific to AI. Rather, current regulations focus on physical security as well as information security and privacy.[38] For airports planning to introduce AI systems into their security operations, the primary concerns relate to how the underlying data was collected; whether informed consent was given for the collection and use of the data, including for use with the AI system; how the system and underlying data was created, maintained, and evaluated; and how the data is retained or destroyed as appropriate.

The integration of AI into airport security and law enforcement operations presents significant advantages but also introduces legal challenges. AI systems can be used to enhance security, crime prevention, and operational efficiency. However, its deployment must be carefully managed to uphold ethical standards, protect civil liberties, and comply with applicable legal frameworks. As airports consider these requirements and considerations, legal counsel should be involved in determining applicable laws and regulations. While each airport will be subject to some varying requirements, commonalities do exist. TSA issues guidance, often involving or deferring to CISA where evolving information security technologies are involved. Additionally, the FAA may eventually issue regulations for the use of AI systems when it comes to directing and overseeing air traffic. Local and state laws may also impose requirements and restrictions, as may foreign laws in limited situations. In sum, airports must work with counsel and compliance to create AI-involved programs that consider applicable law from the start.

5.1 Compliance with Privacy Laws

Airports intending to introduce AI systems into their operations must evaluate what laws apply to them and the data they hold. This analysis should be led by legal counsel. Airports may always choose to adhere to heightened protections and limitations, but the applicable law covers the minimum requirements. Table 3 describes some of the most commonly applicable legal frameworks (e.g., laws, regulation, binding guidance), including a high-level description of areas addressed under the law. Importantly, an airport being outside the physical borders of a jurisdiction does not necessarily mean they are exempt from these laws. It is worth reiterating that legal counsel should be involved in determining an airport's legal obligations.

Table 3. Legal Frameworks Applicability to AI

Legal Framework	General Description
US Constitution	Although the US Constitution does not specifically contemplate AI, its text could affect potential uses of AI. For example, the Fourth Amendment generally provides a right for "people to be secure in their persons, houses, papers, and effect, against unreasonable searches and seizures…" While there are exceptions to this rule, these exceptions are most common where a person does not have a reasonable

[38] See "49 CFR 1542 - Airport Security," *National Archives Code of Federal Regulations*, February 22, 2002, https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1542.

Legal Framework	General Description
	expectation of privacy, or the government has a compelling reason for the search. Where AI systems are contemplated by government-operated airports, these requirements, and their exceptions, should be fundamental considerations.
US Federal Law	The US Privacy Act of 1974, as amended, sets limitations on the collection, use, and sharing of personal records by agencies (as that term is defined in the law), and affords individuals certain rights to their data. For airports with access to Criminal Justice Information Services, data must also consider the limitations and security requirements set forth therein. Importantly, the federal government has limited powers that are set forth in law (usually, enabling statutes). To the extent applicable to airport operations, these enabling statutes set boundaries on what is permissible.
Airport-Specific Requirements	Federal agencies derive their regulatory powers from applicable law, including directives from the US Congress to promulgate regulations. As discussed earlier in this section, regulatory action in this space is largely driven by TSA and FAA. In addition to regulations, federal agencies regularly issue frameworks and guidance regarding the use of tools. For example, TSA has set forth guidelines regarding surveillance, screening, and passenger privacy.
US State Privacy Laws	US states have been issuing comprehensive privacy laws. While the laws are usually targeted at operations in the given state, data collection and processing that is targeting or affecting residents of other states may bring an organization within the scope of the law. This depends, however, on a number of factors that are very fact-specific. If applicable, laws like the CCPA, as amended, generally place limitations on data collection and afford individuals enumerated data subject rights. For up-to-date information on US state AI governance legislation, see the International Association of Privacy Professionals (IAPP) legislation tracker: https://iapp.org/resources/article/us-state-ai-governance-legislation-tracker.
US State Biometric Privacy Laws	For airports considering AI systems that use biometric identifiers (e.g., fingerprints, faceprints, iris scans), additional privacy laws could potentially apply. For example, Illinois's Biometric Privacy Act requires covered organizations to develop a publicly available written policy that establishes a retention schedule and guidelines for destroying biometric identifiers and information. AI systems complicate compliance with such requirements as they are trained on and "remember" this data for the life of the system. As the act (and other laws) provide for a private right of action with substantial penalties, these laws create significant legal risk for covered organizations that fail to comply with their requirements.
Canada's Personal Information Protection and Electronic Documents Act and related provincial laws	Canadian privacy laws generally require covered organizations to adhere to fair information principles to protect personal information. These laws also generally cover the transfer of personal information across Canada's borders. The Personal Information Protection and Electronic Documents Act applies to airports that handle Canadian passenger data as part of their commercial activities.
The EU's 2016/679 GDPR and the UK's Data Protection Act 2018	The EU's GDPR set requirements on the collection, processing, and transfer of personal data. Among other things, the regulation prohibits biometric processing except in consented or public interest applications and affords data subjects specific rights, including the rights to access, delete, restrict and seek transparency regarding processing. AI systems trained on or otherwise processing personal data must be able to appropriately action such requests. Moreover, the GDPR sets forth requirements around the transfer and processing of data across borders. GDPR was brought into application in the UK via the Data Protection Act 2018, and the regulation is known as UK GDPR—identical to GDPR—with additional provisions applied via the 2018 act.

Legal Framework	General Description
The EU Artificial Intelligence Act (Regulation (EU) 2024/1689)	The EU AI Act, which entered into force on August 1, 2024, and is directly applicable and effective in all 27 member states, introduced a harmonized framework setting forth requirements and obligations on specific uses of AI. The act implements a risk-based approach that considers the developer (provider) and the value chain through to the user (deployer), and the impact on the health, safety, and fundamental rights of individuals. The act classifies AI systems, sets forth prohibited practices, and requires a risk management system for high-risk AI systems. The act codified the OECD and High-Level Experts Group principles for trustworthy AI, putting them on a statutory footing for high-risk systems.
China's Personal Information Protection Law	China's Personal Information Protection Law covers the handling of personal information of natural persons within the borders of China as well as other circumstances provided in laws or administrative regulations. It requires organizations to follow principles of openness and transparency, including the disclosure of rules for handling personal information in a manner that indicates the purpose, method, and scope of such handling. Similar to other privacy laws, China's law sets forth requirements for cross border transfers and processing of personal information.

5.2 Consent for Data Collection and Processing

Airports, unlike many other organizations, operate with limited exceptions to the general requirement to obtain consent or obtain a warrant before conducting searches. Courts have reasoned that this exception stems from the need to address risks to public safety, including from terrorism (as in United States v. Aukai).[39] Airport screening procedures, which are required by federal law (49 USC 44901), generally qualify as "administrative searches" and, as a result, do not depend on the consent of a potential passenger (see United States v. Biswell).[40] This exception, however, is restricted in that the searches must be conducted for the limited purpose of protecting public safety and be no more extensive nor intensive than necessary.

This, as is the case with almost all legal questions, is a fact-specific analysis. Airport operators should therefore work closely with legal counsel to determine whether the proposed use case of an AI system meets these requirements. Moreover, where the use case is not directly related to public safety (e.g., mass-reviewing employment applications), the exception is unlikely to apply. Additionally, if AI systems are contemplated for clearly non-security related functions such as marketing or advertising, consent for the collection and processing of the individual's personal data would, absent other legal bases, be required.

Where consent is required, there are different methods of consent. For example, some laws and types of processing require express (sometimes written) consent (also called "informed consent"). In sum, this method of consent requires intentionality from the individual in providing their consent. For example, an individual may check a box, sign a form, or orally provide such consent where complete and accurate information regarding the collection and processing of their personal information has been made available to them. The other form of consent is generally referred to as "implied consent." This method of consent involves an individual's actions indicating their consent even where they do not explicitly, in writing, or otherwise, state their consent. A common example is where an individual intentionally enters

[39] United States v. Aukai (United States Court of Appeals, Ninth Circuit 2007).
[40] *Screening Passengers and Property*, *49 USC 44901*, 2001, https://uscode.house.gov/view.xhtml?req=granuleid:USC-2000-title49-section44901&num=0&edition=2000; United States v. Biswell, 406 U.S. 311 (United States Supreme Court 1972).

an area with ongoing audio and video recording and where notice is provided of such recording. Where the individual proceeds to enter the recorded space, their consent is implied.

Where consent is required, express consent, especially express written consent, is the most easily defensible method of evidencing an individual's consent. Airports considering implementing AI systems where consent is required should consider what method of consent is required as well as whether it has sufficiently documented the individual providing their consent to the specific collection, use, and processing. Additionally, airports should consider whether additional limitations are placed on the consent, such as the expiration of an individual's consent or any requirements that prohibit continued retention or use of data after a certain period of time has elapsed.

5.3 Ethical AI Usage

This section has focused on determining an airport's legal *requirements* as they relate to AI usage. In addition to these requirements, airports should be aware of industry best practices, including mitigating potential harm to individuals. These considerations influence an airport's common law responsibilities and mitigate legal risk, including claims by individuals of tortious harms. As AI tools continue to develop and industry practices evolve, airports must continually learn from their peers and thought leaders.

Airports should be prepared to inform individuals when AI is used. However, the actual AI system and its outputs may qualify as SSI or protected critical infrastructure information (PCII) and therefore may not be subject to disclosure.

Airports should also understand the AI system to mitigate risks posed by its limitations, biases, and other potential shortcomings. Failure to understand these issues will not only present potential legal risk to an airport but could potentially allow gaps in the effectiveness of the tool. Ethical usage also requires considerations about what data is entered into the system, how the system maintains such information, and how it is deleted once it is no longer beneficial.

Biases in the data input create a significant risk of skewed and unfair outputs and subsequent actions. For example, if the underlying data involved biased policing, screening, or other actions, the resulting system decisions are also likely to be biased. Past examples of this involved racial profiling, in which organizations disproportionately targeted members of certain classes of persons, resulting in higher stops, arrests, or other findings for those groups. To avoid replicating these dynamics in AI-supported systems, airports should evaluate data inputs and system outputs across all stages of the security workflow, and not solely for end outcomes. This includes examining how frequently individuals are flagged, escalated, searched, or cleared, and whether those actions meaningfully correlate with confirmed security findings. If escalation rates or false positives are not statistically justified, airports can adjust thresholds, operational procedures, or training practices to reduce unnecessary intervention. Focusing on proportionality across the full decision process, rather than outcomes alone, helps mitigate both actual and perceived bias in AI-assisted security operations.

PRIVACY AND DATA PROTECTION

Privacy protections and user rights should be prioritized when deploying AI systems that process personal data, such as surveillance tools or cybersecurity solutions monitoring employee activities. Airports must comply with applicable data protection regulations and implement safeguards to protect passenger and employee data. Passengers should also be informed about AI usage and be provided with avenues to contest AI-driven decisions, such as security screening escalations, wherever possible.

5.4 Compliance

It bears repeating that an essential element of any compliance program is to involve legal counsel and, where available, their compliance team. These teams should be familiar with what laws, regulations, or other requirements apply to the airport. Also crucial to this conversation are personnel who are intimately familiar with the proposed AI system as well as the operations intended to be supplemented by the system. This step allows an airport to make informed decisions about the risks and rewards involved, including helping to identify tools that over promise and under deliver. The compliance analysis should have either an individual or leadership group that has authority within the organization to implement any decision, build buy-in to the project, and make informed decisions based on the input of the subject matter experts involved.

To promote compliance with applicable law, the following factors should be considered when proposing an AI system and periodically thereafter. The period will depend on changes to the system, operations, and other factors, but should be performed at least annually.

- **Accuracy:** Airports should evaluate AI systems to determine how reliable their outputs are in real operational conditions, including how often the system produces inaccurate, incomplete, or misleading results. This assessment should identify when and under what conditions errors occur—such as hallucinated content, misclassification, or false alerts—and whether those errors are detectable before action is taken. For any AI output that may influence security decisions, safety actions, or operational responses, airports should require direct human review and confirmation to ensure outputs are understood, validated, and appropriately applied.
- **Availability:** Airports should evaluate AI systems to understand how the loss, degradation, or malfunction of the system would affect airport operations and safety. This includes assessing whether personnel can continue critical functions if the AI system is unavailable, whether fallback procedures exist, and whether system failures could delay security responses, disrupt passenger flow, or create unsafe conditions. AI systems should therefore be deployed in a manner that supports continuity of operations, rather than becoming a single point of failure.
- **Beneficial Impact:** AI system uses should be evaluated to determine their potential benefit to airport operations, public safety, and/or individuals or groups of individuals who may be affected by the proposed AI system uses, as appropriate.
- **Confidentiality:** AI system inputs should be classified to protect the confidentiality of sensitive information, including but not limited to SSI, PCII, and/or personal information.
- **Contractual Obligations:** Where applicable, AI system uses should be evaluated for compliance with relevant contractual requirements (i.e., if the AI system use affects an airport's ability to perform a contract).
- **Risk Evaluation:** Airports should subject AI systems to ongoing oversight and documented decision-making throughout their operational life, rather than treat them as static tools that are approved at a single point in time. This evaluation should consider how systems are validated before deployment, how updates or changes are reviewed and approved, and how operational risks (such as performance degradation, bias, or security vulnerabilities) are identified and addressed once the system is in use. From a compliance perspective, this ensures the airport can demonstrate that AI-related risks are periodically reassessed, responsibly managed, and escalated or remediated when necessary, including modifying, suspending, or retiring the system if risks can no longer be effectively controlled.

- **Ethical Usage:** AI system uses should be evaluated to ensure compliance with industry best practices as well as applicable ethical principles (described in greater detail throughout this document).
- **Human Impact and Ethical Implications:** AI system uses should be evaluated for fairness and bias, privacy, and safety, including the interests of individuals or groups of individuals who may be affected by the proposed AI system uses.
- **Integrity:** AI system uses should be evaluated to assess the potential for data or system output to be inadvertently or intentionally manipulated.
- **Intellectual Property Protection:** AI system uses should be evaluated for the potential to infringe upon a third-party's intellectual property interests, as applicable.
- **Lawfulness:** AI system uses should be assessed based on applicable or potentially applicable laws. The review of lawfulness must consider whether and to what extent the use of the AI system poses a risk of making a decision that adversely impacts any individual (or class of individuals) in a manner that violates the individual's rights.
- **Reliability:** AI systems should be evaluated for their ability to perform consistently and as intended under real operational conditions. This includes documenting baseline performance expectations, monitoring error rates and system stability, and establishing a process for ongoing reassessment as data inputs, operating environments, technologies, or use cases change. Reliability reviews should ensure that AI outputs remain dependable over time and that degradation, performance drift, or unexpected behavior is identified and addressed before it impacts security, safety, or operations.
- **Remediation Controls:** AI systems should include clear mechanisms to respond when risks are identified—whether anticipated during planning or observed during operations. This includes the ability to adjust system thresholds, modify operational procedures, retrain or recalibrate models, limit system use, or suspend or decommission the AI system or specific use cases when issues such as persistent inaccuracies, bias, security vulnerabilities, or operational disruption cannot be effectively mitigated. Effective remediation controls ensure that AI systems remain aligned with legal, operational, and ethical requirements over time, rather than remaining in use despite known harms.
- **Reputational Impact:** AI system uses should be assessed for their potential to cause reputational harm to the airport.
- **Third-Party and Supply Chain Risk:** Before implementing any third-party AI system, the vendor's ownership, geopolitical location, and potential conflicts of interest must be thoroughly assessed. This review should evaluate any factors that could compromise the confidentiality, integrity, or security of the AI system and its data. As a rule, systems from vendors known or reasonably suspected of violating security and privacy standards should be disqualified from consideration.

A small hub airport operations employee expressed concerns around third-party engineering firms using AI and not disclosing that they're using it (integrity and ethical bias around using tools)

- **Transparency:** First, the airport must have sufficient visibility into how the AI system functions and impacts the operational security environment. Second, a clear strategy must be determined for what information will be disclosed to the public and stakeholders about the use of AI.

5.5 Standards and Frameworks

One additional consideration is the development of standards and best practices that are not strictly required but which may be either implemented later by regulation (as is common with NIST's special publications and frameworks) or established as an industry best practice. For example, NIST published an AI Risk Management Framework describing current best practices for AI system development and implementation. The OECD and United Nations have also published materials encouraging transparency, accountability, and principles of fairness in the development and use of AI systems.[41]

Table 4 identifies non-binding guidance standards and frameworks. Each framework/standard is explored in more detail below the table.

Table 4. Non-binding Guidance Standards and Frameworks

Framework / Standard	Description	Relevance / Application
NIST AI Risk Management Framework (AI RMF)	Voluntary framework from NIST offering best practices for managing AI risks. Promotes trustworthy, fair, and accountable AI.	Critical infrastructure, law enforcement, public sector AI deployments
NIST Generative AI Profile	Companion to AI RMF focused on risks unique to generative AI (e.g., hallucinations, misinformation).	Generative AI use in threat analysis, public communications, airport operations
ISO/IEC 42001: AI Management System	First certifiable international standard for AI governance across the lifecycle. Integrates with ISO/IEC 27001.	Enterprise AI governance, transparency, and oversight
ISO/IEC 5259: Data Quality for AI	Standard series for managing data quality (accuracy, completeness, consistency) in AI systems.	Reliable and unbiased AI, especially in security-critical environments like airports
UN Guiding Principles on Business and Human Rights	Framework asserting organizational responsibility to respect human rights, including in AI use.	Preventing misuse, discrimination, and adverse impacts from AI
General Ethical AI Frameworks (OECD, etc.)	International principles promoting transparency, fairness, and accountability in AI.	Ethical deployment of AI in high-stakes public safety and security contexts
Security Industry Association Principles for Facial Recognition	Voluntary principles for responsible use of facial recognition, emphasizing transparency and oversight.	Building public trust and mitigating risks in facial recognition deployments

ISO IEC 42001: AI MANAGEMENT SYSTEM STANDARD

ISO/IEC 42001:2023 is the world's first certifiable international standard for AI management systems. Developed jointly by ISO and the IEC, the standard provides a structured and auditable framework for organizations to manage the life cycle, risks, and governance of AI systems, which is especially critical in high-stakes environments like airports where safety, privacy, compliance, and public trust intersect.

[41] The OECD maintains a collection of policies, analysis, and general publications on responsible development and use of AI. See "The OECD Artificial Intelligence Policy Observatory," accessed August 4, 2025, https://oecd.ai/en/. See also, United Nations General Assembly, "Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development," March 11, 2024, https://docs.un.org/en/A/78/L.49.

The standard follows the Annex SL high-level structure (a much simpler and more efficient way for an airport to adopt and manage multiple ISO certifications), making it interoperable with other widely adopted management system standards such as ISO/IEC 27001 (information security) and ISO 9001 (quality management).

ISO/IEC 42001 addresses both the technical and organizational dimensions of AI, placing emphasis on transparency, human oversight, ethical use, and robust governance mechanisms. This is particularly relevant in airport security and operations, where AI systems are increasingly used in surveillance, identity verification, baggage screening, threat detection, and passenger flow management. Organizations and AI system providers who are certified to ISO/IEC 42001 signal AI maturity and trustworthiness where the risks of misuse, bias, or system failure can have significant real-world consequences.

NIST GENERATIVE AI

The NIST Generative AI Profile (AI 600-1, 2024) is a companion document to the AI Risk Management Framework (AI RMF 1.0), developed by the NIST to help organizations manage the risks associated with generative AI technologies, including large language models and image-generation systems.[42] This profile is especially relevant to critical infrastructure sectors such as aviation, airport security, and law enforcement, where the deployment of generative AI systems must be carefully managed to protect safety, security, and public trust.

The profile outlines how to apply the AI RMF's four core functions—Govern, Map, Measure, and Manage—to the specific challenges posed by generative AI, such as:

- Hallucinations and misinformation
- Bias and representational harm
- Unauthorized data generation or reproduction (e.g., copyright infringement)
- Misuse or malicious use
- Loss of human oversight and explainability

By identifying these risks across the AI system life cycle, the profile supports decision-makers in implementing appropriate controls, policies, and mitigation strategies. For critical infrastructure operators, this includes ensuring traceability, maintaining human control, securing sensitive data, and addressing emergent risks in both operational and customer-facing applications.

For airport authorities and security contractors, the profile is particularly valuable when evaluating AI-enabled systems used in surveillance, identity verification, threat analysis, and public communication tools. It reinforces the importance of governance, transparency, and preparedness when integrating generative AI into high-assurance environments, aligning with broader federal guidance on trustworthy AI use in safety-critical domains.

SECURITY INDUSTRY ASSOCIATION

The Security Industry Association (SIA) is the leading trade association for global security solution providers, with over 1,500 innovative member companies representing thousands of security leaders and experts who shape the future of the security industry. The SIA protects and advances its members' interests by advocating pro-industry policies and legislation at the federal and state levels, creating open industry standards that enable integration, advancing industry professionalism through education and

[42] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, July 2024, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.

training, opening global market opportunities, and collaborating with other like-minded organizations. The SIA advocates for policies and legislation that drive business opportunities in a wide range of vertical markets, including health care, ports, transit, and education.[43]

The SIA's AI Advisory Board works alongside industry peers comprising developers and integrators of AI technology across the security domain, including the airport security environment. The board created a glossary of terms specifically designed to accommodate the context of the use cases for AI in security. The glossary covers a wide range of terms commonly used in AI discussions, including:

- Core AI concepts (e.g., algorithm, ML, neural network)
- Deployment-related terms (e.g., edge computing, inference, training data)
- Performance and governance concepts (e.g., bias, accuracy, false positive rate)
- Security and privacy-relevant terms (e.g., data minimization, adversarial attack)

It also distinguishes between general AI terminology and its specific interpretations in the context of physical and electronic security, helping reduce confusion when AI terms are adapted for surveillance, facial recognition, object detection, and automated decision systems. The glossary is available as a free download from the SIA website.[44]

FACIAL RECOGNITION

The SIA developed a set of voluntary Principles for the Responsible and Effective Use of Facial Recognition Technology by private security organizations in private and public sector applications, as well as law enforcement use.[45] This was developed following a number of high-profile mistakes and subsequent statewide bans on the use of the technology. The core principles include:

- Transparency
- Clear and defined purpose
- Using accurate technology
- Human oversight
- Nondiscrimination
- Data security
- Privacy by design
- Training and education
- Ethical acquisition
- Targeted public policy

ISO/IEC 5259: DATA QUALITY

The ISO/IEC 5259 standard series provide a crucial framework emphasizing that "high-quality data is critical... throughout the entire AI system life cycle." This concept is foundational to the entire series, particularly covered in ISO/IEC 5259-1 (Overview, terminology, and examples) and ISO/IEC 5259-3

[43] "About SIA," *Security Industry Association*, n.d., https://www.securityindustry.org/about-sia/.
[44] "Glossary," *National Institute of Standards and Technology Computer Security Resource Center*, accessed July 3, 2025, https://csrc.nist.gov/glossary.
[45] Security Industry Association, *SIA Principles for the Responsible and Effective Use of Facial Recognition Technology*, 2020, https://www.securityindustry.org/wp-content/uploads/2020/08/SIA-Principles-Responsible-Ethical-Facial-Recognition-Usage.pdf.

(Data quality management requirements and guidelines).[46] For AI in airport security, this is directly practical, ensuring "the data used to train, test, and operate these AI systems is accurate, complete, consistent, and timely."[47] Adhering to these principles is vital because data quality "directly impacts the system's ability to function effectively and safely," and helps to "minimize errors, biases, and false positives or negatives that could compromise security or inconvenience passengers." These outcomes are the primary goals of implementing data quality management as described in ISO/IEC 5259-3 and are implicitly addressed across the series as the benefits of good data quality for trustworthy AI.[48] This focus on data quality throughout the AI life cycle, as outlined in ISO/IEC 5259, is fundamental to enhancing the dependability and trustworthiness of AI used in security-critical airport operations.

5.6 Future Legal Trends

Regulatory action specific to AI has, through early 2025, been somewhat piecemeal. US federal law has largely failed to address the topic in detail beyond an emphasis on funding development efforts and coordinating research activities. For example, in passing the FAA Reauthorization Act of 2018, Congress noted that its sense was that the FAA:

> "should, in consultation with appropriate Federal agencies and industry stakeholders, periodically review the use or proposed use of artificial intelligence technologies within the aviation system and assess whether the Administration needs a plan regarding artificial intelligence standards and best practices to carry out its mission."[49]

President Biden issued an Executive Order in 2023 that further developed the federal government's approach to AI by requiring certain federal agencies to appoint a chief AI officer and set new standards for AI safety and security.[50] US state laws have also seen some developments,[51] and there have been developments outside of the US.[52]

These trends, however, have come in fits, and tension exists between regulating the risks posed by AI systems and the potential benefits to being a global leader in the space. Moreover, there are divisions

[46] International Organization for Standardization, "ISO/IEC 5259-1:2024 Artificial Intelligence — Data Quality for Analytics and Machine Learning (ML), Part 1: Overview, Terminology, and Examples" (Geneva, Switzerland, July 2024), https://www.iso.org/standard/81088.html; International Organization for Standardization, "ISO/IEC 5259-3:2024 Artificial Intelligence — Data Quality for Analytics and Machine Learning (ML), Part 3: Data Quality Management Requirements and Guidelines" (Geneva, Switzerland, July 2024), https://www.iso.org/standard/81092.html.

[47] International Organization for Standardization, "ISO/IEC 5259-2:2024 Artificial Intelligence — Data Quality for Analytics and Machine Learning (ML), Part 2: Data Quality Measures" (Geneva, Switzerland, November 2024), https://www.iso.org/standard/81860.html; International Organization for Standardization, "ISO/IEC 5259-4:2024 Artificial Intelligence — Data Quality for Analytics and Machine Learning (ML), Part 4: Data Quality Process Framework" (Geneva, Switzerland, July 2024), https://www.iso.org/standard/81093.html.

[48] International Organization for Standardization, "ISO/IEC 5259-3:2024 Artificial Intelligence — Data Quality for Analytics and Machine Learning (ML), Part 3: Data Quality Management Requirements and Guidelines."

[49] *FAA Reauthorization Act of 2018*, *Public Law 115-254*, 2018, https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf.

[50] *Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 2023, https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[51] See, for example, the California AI Transparency Act (California Senate Bill No. 942, September 19, 2024) or Utah's Artificial Intelligence Policy Act (Utah Senate Bill 149,. March 13, 2024).

[52] See, for example, The EU Artificial Intelligence Act (Regulation 2024/1689, June 13, 2024); see also "DeepSeek Rushes to Launch New AI Model as China Goes All in | Reuters," accessed August 4, 2025, https://www.reuters.com/technology/artificial-intelligence/deepseek-rushes-launch-new-ai-model-china-goes-all-2025-02-25/.

between the proponents for heightened protections and those who support increased investment. This creates an impasse that has slowed the development of applicable rules and guidelines.

As developments in AI continue at a rapid pace, governments may be forced to take action.[53] Legal trends are most likely to be influenced by AI's capabilities, its uses, and perhaps most importantly, the perception of those who develop it. If the public and lawmakers trust the developers of AI systems, the tension is more likely to be resolved in favor of increased investment. If, on the other hand, the public loses trusts in AI developers or comes to see the systems themselves as a threat, increased oversight is more likely.

[53] Ezra Klein, "Opinion | The Government Knows A.G.I. Is Coming," *The New York Times*, March 4, 2025, sec. Opinion, https://www.nytimes.com/2025/03/04/opinion/ezra-klein-podcast-ben-buchanan.html.

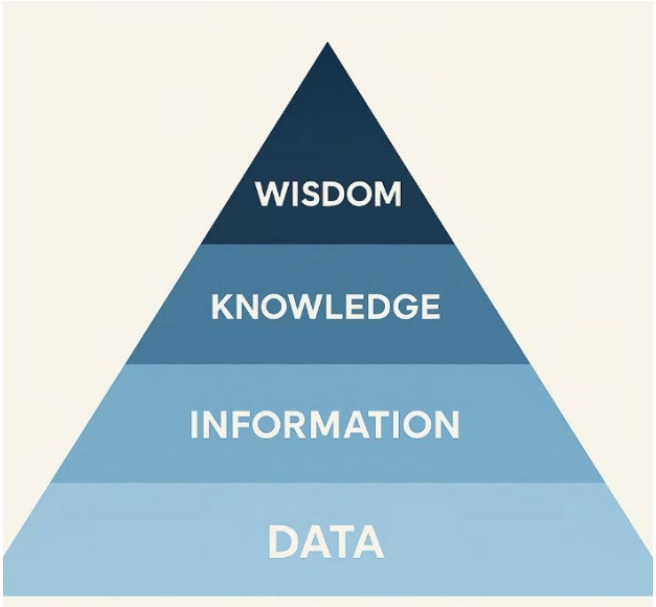
SECTION 6: DATA MANAGEMENT, INTEGRATION, AND INFRASTRUCTURE

Data Management, integration, and infrastructure considerations refer to the essential framework needed to effectively implement AI systems in complex environments such as airports. Data management ensures that information collected from various sources, like biometric systems, surveillance cameras, and Internet of Things (IoT) sensors, is accurate, organized, and secure. Integration focuses on seamlessly connecting AI technologies with existing systems, enabling smooth data flow and interoperability between new and legacy platforms. Lastly, infrastructure considerations involve building the necessary hardware, software, and networks to ensure AI solutions can process large volumes of data efficiently, scale with increasing demand, and maintain operational reliability. Underpinning this entire framework is a comprehensive set of cybersecurity and IT controls designed to protect data integrity, ensure system availability, and defend against malicious actors.

MANAGING AIRPORT DATA THROUGH DIKW

The process of transforming raw data into actionable intelligence involves several stages. Airport security software applications often have large databases with a wealth of information. Generally, it is up to the IT department to assist with accessing this data, which is in its raw/unstructured format, and turning it into actional data.

Figure 5. DIKW Hierarchy



To understand the journey of this data, the DIKW hierarchy (Data → Information → Knowledge → Wisdom; Figure 5), is a common conceptual framework used across knowledge management and decision-making and intelligence communities. Data is aggregated, organized, and interpreted to create information. This information, when paired with insight, becomes knowledge, which in turn, when paired with actionable intelligence and experience, ultimately becomes wisdom. This hierarchical progression is fundamental to effective decision-making in complex operational environments. Table 5 outlines how this process applies to various airport security systems.

The progression from raw data to actionable wisdom is critical for AI to deliver tangible security benefits. Data, as isolated facts (e.g., a surveillance camera feed, an access log entry), gains context to become information (e.g., a person entered a restricted area at a specific time). When this information is accumulated and analyzed over time, it forms knowledge (e.g., patterns of unauthorized access attempts, common tailgating behaviors). Finally, this knowledge, combined with actionable intelligence and human experience, evolves into wisdom, enabling strategic decision-making and proactive security measures.[54]

[54] "What Is the Data, Information, Knowledge, Wisdom (DIKW) Model?," *Weje*, n.d., https://weje.io/blog/data-information-knowledge-wisdom.

Table 5. Transforming Data into Wisdom

System	Data Type/Example	Transformation Description	Information Generated	Knowledge Derived (from)	Wisdom Gained (from)
Secure Access Control / Monitoring Systems	Biometric scans, RFID/NFC taps, PIN entries	Credential authentication, access logging	Access logs, alerts, audit trails	Unauthorized attempts, policy compliance, anomalies	Role-based access tuning, lockdown automation, insider threat detection
Surveillance and CCTV Analytics	Live/recorded CCTV feeds	Object/event detection, recognition	Alerts, heatmaps, zone counts	Incident detection, crowd analysis, tracking	Camera placement optimization, predictive alerts
AI-Driven Radio Communication Transcription	Live radio audio	Speech-to-text, speaker ID	Transcripts, keyword alerts	Communication monitoring, incident documentation	Situational awareness, training enhancement
Cybersecurity AI Systems	Network logs, IDS alerts, threat feeds	Anomaly/malware detection	Threat alerts, risk scores, attack paths	Incident prioritization, threat prediction	Automated response, vulnerability detection
Computer-Aided Dispatch System	Calls, sensor alerts, GPS, resource data	Incident prioritization, responder matching	Incident logs, assignments, status tracking	Resource deployment, response time	Hotspot prediction, escalation automation
License Plate Recognition Systems	Video feeds from entrances, garages	Plate extraction, hotlist comparison	Vehicle ID, timestamps, alerts	Vehicle tracking, access alerts, traffic flow	Suspicious pattern detection, law enforcement integration

6.1 Airport Big Data Concepts and Quality

The concept of Big Data, characterized by the four V's—Volume, Variety, Velocity, and Veracity—is central to modern data analysis. Big Data inherently includes the concept of data mining, a process that leads to knowledge discovery. Through data mining, large volumes of diverse data can be transformed into actionable intelligence, extracting knowledge that can reveal deeper patterns and relationships. For example, analyzing environmental factors can provide knowledge about their effects on various types of machinery used in airport operations, transforming predictive maintenance schedules and enhancing operational security.

The integration of AI into airport security systems necessitates a robust understanding of Big Data principles. Airport environments are inherently high-volume data ecosystems, generating immense quantities of information from diverse sources such as surveillance cameras, biometric systems, and IoT sensors. The sheer volume of data, coupled with its variety (structured and unstructured, from video to access logs), demands sophisticated AI algorithms for effective processing.

For instance, a connected vehicle—a vehicle equipped with onboard sensors, telematics systems, GPS, infotainment platforms, and wireless connectivity—can generate up to 25 GB of data per hour. This data may include location and movement data, engine and diagnostic telemetry, key-fob and access logs, Wi-Fi and Bluetooth connection records, and time-stamped system events. In law-enforcement and public-safety contexts, such data is increasingly used as digital evidence to reconstruct timelines, correlate vehicle movements with incidents, and to link individuals, locations, and devices during investigations. AI-enabled platforms are used to securely ingest, filter, and correlate this high-volume vehicle data with other sources, such as surveillance video, access logs, and incident reports, transforming raw sensor outputs into actionable intelligence while managing privacy, legal, and data-governance constraints. This example illustrates the scale and complexity of data saturation modern security and law-enforcement organizations must manage, and why AI-driven analytics are necessary to extract timely, relevant insights from high-volume, high-velocity data streams.[55]

The velocity of data, particularly in real-time operational security contexts, requires AI systems capable of instantaneous analysis and response.[56] Furthermore, the veracity, or trustworthiness, of this data is paramount, as inaccurate or biased data can lead to flawed insights and compromised security outcomes. AI-driven data mining techniques are crucial for extracting hidden patterns and knowledge from this complex data landscape, transforming raw Big Data into actionable intelligence that informs predictive security measures and optimizes resource allocation.[57] The ability of AI to process and make sense of data at scales and speeds impossible for humans is not merely an enhancement but a fundamental necessity for managing and extracting actionable intelligence from the Big Data generated in airport environments.[58] It overcomes inherent human limitations in processing vast, varied, and high-velocity datasets, thereby enabling effective operational security and law enforcement in complex, dynamic settings.

The effectiveness of AI in airport security hinges on the precision, organization, and accuracy of data. Airports operate as high-volume data ecosystems, collecting information from diverse sources, including surveillance cameras, biometric systems, passenger tracking systems, and IoT sensors. Ensuring high-quality data is critical for AI systems to provide actionable and reliable insights.

A medium-hub airport, when asked about using AI at the airport for security, expressed concerns, particularly regarding data hygiene and security: “Organizations may not be ready for AI due to poor data classification management.”

Incorporating AI into an organizational environment can be significantly more effective when data is well-categorized and classified, for the following reasons:

- **Improved Accuracy:** When data is organized, AI algorithms can process information more accurately, reducing errors and enhancing the reliability of insights.
- **Enhanced Learning:** Structured data provides a solid foundation for AI models to learn from. Organized unstructured data, such as text or images, can be more effectively analyzed using techniques like NLP and image recognition.

[55] Borche Stefanov, “6 Ways AI Is Transforming Data Sharing and Security in Law Enforcement,” *Kaseware*, May 29, 2025, https://www.kaseware.com/post/6-ways-ai-is-transforming-data-sharing-and-security-in-law-enforcement.
[56] “How AI Flight Data Analysis Revolutionizes Aviation Safety and Risk Prediction in 2025 - Axis Intelligence,” accessed August 4, 2025, https://axis-intelligence.com/ai-flight-data-analysis-revolutionizes-2025/.
[57] “Real-World Applications of AI in Airport Operations,” *Copenhagen Optimization*, accessed August 4, 2025, https://copenhagenoptimization.com/blog/the-role-of-ai-and-machine-learning-in-airport-resource-optimization/.
[58] “What Is the Data, Information, Knowledge, Wisdom (DIKW) Model?”

- **Efficient Processing:** Pre-categorized data enables faster processing and analysis, as the AI does not need to spend additional resources on sorting and organizing the data.
- **Better Decision-Making:** Clear data categorization allows AI tools to provide more precise and actionable insights, aiding in strategic decision-making.

KEY AREAS TO CONSIDER

The quality of data—its accuracy, consistency, and completeness—is the bedrock upon which effective AI systems are built in airport security. Flawed or biased data can lead to erroneous AI outputs, resulting in false positives that overwhelm security personnel, or false negatives that allow threats to go undetected. For AI models to learn effectively and provide reliable insights, the underlying data must be meticulously curated and validated.[59]

Data quality also extends to ethical considerations. AI systems, particularly those involving facial recognition or behavioral analysis, can "inherit biases present in training data, leading to unfair targeting of certain groups."[60] For instance, facial recognition technology has shown "higher error rates in identifying women and people of color," which could result in certain demographic groups being "disproportionately flagged for secondary screening or further investigation due to the AI's inherent biases."[61] To mitigate such outcomes, it is imperative to "balance the data set to ensure equal representation of different groups" during AI model training.[62] This transforms data quality from a purely technical concern into a fundamental ethical and social responsibility for airport security, ensuring fairness and maintaining public trust.

- **Data Collection:** Real-time data processing is vital for continuous monitoring and operational decision-making. For example, Heathrow Airport employs real-time passenger monitoring systems to dynamically allocate security staff during peak hours and adjust terminal resources based on passenger flow.
- **Advanced Analytics:** AI relies on sophisticated tools to interpret data and predict patterns. Predictive analytics can forecast passenger traffic and optimize resource allocation, such as efficiently deploying cleaning teams or offering targeted retail promotions during low-traffic periods.
- **Storage Solutions:** Airports must invest in scalable and secure storage solutions:
    - **Cloud Storage:** Offers flexibility and scalability but raises concerns over latency and data sovereignty.
    - **On-Premises Storage:** Provides better control and security but requires higher upfront costs and maintenance.
    - **Hybrid:** A hybrid approach often provides the best balance between these factors.
- **Compliance:** Handling sensitive data demands adherence to regulations like GDPR and CCPA, discussed more in-depth in Section 5 regarding data privacy. Non-compliance risks include reputational damage and financial penalties. Transparency in data governance and obtaining informed passenger consent are essential for building trust.

---

[59] Mariana Coutinho, "#Why Airports Need Strong Data Governance - Ivy Partners," February 12, 2025, https://www.ivy.partners/why-airports-need-strong-data-governance/, https://www.ivy.partners/why-airports-need-strong-data-governance/.
[60] Divyanshu Ranjan Srivastava, "Ethical Concerns in AI-Powered Surveillance Technologies," *Medium*, October 6, 2024, https://divsriv.medium.com/ethical-concerns-in-ai-powered-surveillance-technologies-bdbd67ce6869.
[61] Srivastava, "Ethical Concerns in AI-Powered Surveillance Technologies."
[62] Nitin Vats, "The Ethics of AI in Monitoring and Surveillance," *NICE Systems*, January 1, 2024, https://www.niceactimize.com/blog/fmc-the-ethics-of-ai-in-monitoring-and-surveillance/.

- **Data Encryption:** Involving the airport's IT and/or cyber team is critical for ensuring the implementation of end-to-end encryption for all sensitive data, both at rest (e.g., in databases, storage systems) and in transit across the network. Encrypting data can reduce the likelihood of intercepted or breached data becoming readable or unsecure.
- **Access Control and Identity Management:** Two areas where the airport's IT and/or cyber team can contribute include enforcement of Role-Based Access Control and the Principle of Least Privilege for all data repositories, applications and AI models.[63] This can reduce the risk of personnel and systems being accessed through unauthorized means.

By ensuring data is well-structured, AI tools become more knowledgeable and effective in delivering valuable insights and solutions. This approach not only optimizes AI performance but also enhances overall efficiency and decision-making capabilities within an organization.

6.2 Integration with Existing Infrastructure

Integrating AI systems into existing airport technologies presents a critical challenge, especially given the legacy systems many airports rely on. Seamless integration ensures AI-driven insights can be effectively leveraged to enhance operations and security.

> One medium hub airport stated, "while various AI-powered security solutions exist (e.g., cam-based, readers, tamper detection), integrating them seamlessly into existing airport systems (like video surveillance) requires significant effort in building out capabilities and licensing."

KEY AREAS TO ADDRESS

- **System Interoperability:** Legacy systems often lack compatibility with modern AI platforms. Standardized communication protocols, such as Application Programming Interfaces (API), enable efficient data sharing and collaboration between systems.
- **Secure Integration Points:** All APIs and data integration points must be secured using authentication tokens, API gateways, and traffic encryption. This reduces the risk of unauthorized data access and/or system manipulation.
- **Real-Time Data Processing:** AI integration facilitates real-time responses to operational challenges. For instance, integrating weather data with flight schedules allows AI systems to predict delays and suggest gate changes, minimizing disruptions.
- **Centralized Platforms:** Consolidating data management through centralized platforms enhances operational efficiency by reducing departmental silos. These platforms integrate airport security information and customer information management with business intelligence tools for better forecasting and coordination.[64]

INFRASTRUCTURE SECURITY AND IT CONTROLS

While AI can enhance security, the AI systems themselves, along with the data they rely on, must be rigorously protected. The airport's IT and/or cyber team should deploy a multi-layered security strategy that is essential for the underlying IT infrastructure.

---

[63] **Role-Based Access Control:** A method of restricting system access to authorized users based on their specific job function rather than individual identity.
Principle of Least Privilege: The practice of limiting access rights for users and systems to the bare minimum permissions they need to perform their specific work.
[64] Alwyn Joy, "Redefining Airports with Advanced Technological Infrastructure," *Rezcomm*, August 24, 2023, https://www.rezcomm.com/resources/blog/ai/redefining-technological-infrastructure.

KEY CONTROLS TO IMPLEMENT

- **Network Security and Segmentation:** Isolate AI systems and sensitive data repositories on segmented network zones protected by firewalls. Employ Intrusion Detection and Prevention Systems (IDS/IPS) to monitor network traffic for malicious activity and block potential threats in real time.
- **System Hardening:** All servers, applications, and network devices must be securely configured according to industry best practices. This includes disabling unnecessary ports and services, changing default credentials, and applying security configuration templates.
- **Vulnerability and Patch Management:** Establish a formal process for regularly scanning all systems for security vulnerabilities and applying security patches. This proactive approach prevents attackers from exploiting known weaknesses in software and operating systems.
- **Centralized Logging and Monitoring:** Aggregate security logs from all systems (networks, servers, applications) into a Security Information and Event Management solution. This enables centralized monitoring, threat hunting, and faster incident investigation by providing a comprehensive view of all activity across the environment.
- **Incident Response and Recovery Plan:** Develop and regularly test a formal incident response plan that outlines the specific steps to take in the event of a cyberattack. This plan should include procedures for containment, eradication, and recovery to ensure operational resilience and minimize the impact of a security breach.

A checklist of technical security controls is provided in Appendix B to assist in evaluating a vendor's AI solution prior to implementation.

6.3 Scalability

In a dynamic airport environment, the successful deployment of AI hinges on strategic infrastructure scalability. The architecture must be designed to accommodate the ever-increasing data volumes generated by security systems without compromising performance. While managing scalability is a foundational responsibility for airport IT teams, its importance is significantly amplified in AI-driven operations. These teams are expected to have established strategies for the key priorities detailed below.

KEY AREAS TO PRIORITIZE

- **Infrastructure Investments:** AI systems require high-performance hardware, such as Graphics Processing Units, and scalable software to process complex algorithms and large datasets.
- **Cloud vs. On-Premises Solutions:**
  - **Cloud Solutions:** Ideal for scalability and cost-effectiveness across multiple locations but may face latency and security challenges.
  - **On-Premises Solutions:** Offer robust data control and reliability, though they demand greater initial investment.
- **Network Reliability:** AI-driven systems depend on uninterrupted connectivity. Airports must ensure sufficient bandwidth, low latency, and redundancy to handle surges in data traffic, especially during high-security scenarios like emergency evacuations or cyber incidents.
- **Proactive Cybersecurity Measures:** As systems scale, the risk of cyberattacks increases. Continuous monitoring, regular updates, and penetration testing are essential for maintaining security and operational integrity.

SECTION 7: DEVELOPING A BUSINESS CASE FOR AI IN AIRPORT SECURITY

Airports worldwide are rapidly adopting AI to enhance security, streamline operations, and improve passenger experience. Developing a robust business case for AI in airport security is essential to ensure that investments deliver measurable value. According to industry technology leaders, it is important to have a business strategy with a clear set of business objectives for AI, with prioritized use cases, to ensure success.[65]

This section provides guidance for building a compelling business case for AI in airport security. The section first establishes the strategic context by reviewing worldwide AI adoption trends and real-world outreach findings. From there, a detailed framework for financial analysis is provided, including practical examples of Cost-Benefit Analysis (CBA), Net Present Value (NPV), and Return on Investment (ROI) to help airports make informed investment decisions.

WORLDWIDE ADOPTION RATE OF AI

The OECD is an international organization made up of 38 member countries that promotes policies to improve the economic and social well-being of people around the world. The OECD is a key source for benchmarking AI readiness and adoption trends and principles for trustworthy AI, and encouraging inclusive innovation policies across public and private sectors.

A non-aviation (Train/ Transportation System) executive commented during the outreach that AI is widely used in security operations, such as law enforcement with predictive analytics, metadata, and video surveillance analytics. They also leverage AI to automate incident responses.

The OECD taxonomy identifies four dimensions of AI intensity that are critical for assessing readiness and impact in airport environments:

- **AI Human Capital:** The availability of skilled professionals needed to develop, deploy, and manage AI systems.
- **AI Innovation:** The sector's contribution to advancing AI through research, patents, and new applications.
- **AI Exposure:** The degree to which AI can transform tasks, processes, or business models within a sector.
- **AI Use:** The actual adoption and integration of AI tools into operational activities.

Together, these dimensions provide a framework for evaluating where airports stand on the AI adoption curve and guide strategic decisions for workforce development, technology investment, and operational integration.

As shown in Figure 6, certain sectors such as IT services, media, and telecommunications rank highly across all dimensions of AI intensity. Airports are included in the "transportation and storage" sector.

[65] Susan Etlinger, "Building a Foundation for AI Success," *The Microsoft Cloud Blog*, October 12, 2023, https://www.microsoft.com/en-us/microsoft-cloud/blog/2023/10/12/building-a-foundation-for-ai-success-a-six-part-series-on-ai-leadership/.

Figure 6. Sectoral Taxonomy of AI Intensity, by Indicator[66]

Distribution of AI intensity across industries considered, by indicator

Bottom quartile | 2nd quartile | 3rd quartile | Top quartile

Industry (A38)	AI human capital	AI innovation	AI exposure (barrier-adjusted)	AI use
10-12 Food products				
13-15 Textiles & apparel				
16-18 Wood & paper				
20 Chemicals				
21 Pharmaceuticals				
22-23 Rubber, plastics, minerals				
24-25 Metal products				
26 Computer & electronics				
27 Electrical equipment				
28 Machinery & equipment				
29-30 Transport equipment				
31-33 Other manufactures				
41-43 Construction				
45-47 Wholesale & retail				
49-53 Transportation & storage				
55-56 Hotels & food services				
58-60 Media				
61 Telecommunications				
62-63 IT services				
64-66 Finance & insurance				
68 Real estate				
69-71 Legal & accounting				
72 Scientific R&D				
73-75 Other business services				
77-82 Admin. & support services				

Note: The Figure reports the AI intensity of each sector according to each AI indicator (AI human capital, AI innovation, barrier-adjusted AI exposure, and AI use). All underlying indicators are expressed as sectoral intensities, where sectoral values represent averages across countries and years. The colour of the cells in the table corresponds to the quartile of the sectoral distribution to which the sector belongs. Sectors considered are manufacturing (excluding coke & petroleum), construction and business services.
Source: authors' elaboration based on Lightcast, STI Micro-data Lab: Intellectual Property Database, BTOS data, Felten, Raj, and Seamans (2021[41]), Eurostat and OECD Digital Economy Outlook 2024 (OECD, 2024[43]).

HOW CBA, NPV, AND ROI CALCULATIONS IMPROVE A BUSINESS CASE

With global and industry-specific context in mind, the next step is to build the financial foundation of the business case using three proven analytical methods. The steps for using CBA, NPV, and ROI calculations to improve a business case for AI in airport security are shown in Table 7. The following sections describe each of these concepts in more detail.

[66] Calvino, F. et al. (2024), "A Sectoral Taxonomy of AI Intensity," *OECD Artificial Intelligence Papers* 30, No. OECD Publishing, Paris, https://doi.org/10.1787/1f6377b5-en.

Figure 7. Steps for Improving an AI Business Case using CBA, NPV, and ROI

Step	Method	Purpose	Output
1	**CBA**	Identify all costs and benefits This is the foundational step. The purpose of a CBA is to identify and list all potential costs and benefits associated with the project, including both tangible (quantitative) and intangible (qualitative) factors. This provides a comprehensive inventory of all variables that will inform the subsequent financial calculations.	A comprehensive list of all financial variables / Input for NPV/ROI
2	**NPV**	Assess value over time Once the costs and benefits have been identified and quantified in the CBA, the NPV calculation is used to determine the project's value over time. It accounts for the time value of money by translating future cash flows into today's dollars, providing a clear figure of the net value the project is expected to create.	Net dollar value
3	**ROI**	Measure efficiency of investment After establishing the project's net value via NPV, the ROI is calculated. ROI is a performance metric that expresses the efficiency of the investment as a percentage. Its primary utility is comparing the AI project against other potential investments or organizational benchmarks.	Percentage return

7.1 Cost-Benefit Analysis

Incorporating AI into airport security is a strategic move that aims to enhance efficiency, bolster security, and streamline operations. As airports face increasing challenges from rising passenger volumes, evolving security threats, and the need for seamless operations, AI offers innovative solutions that can address these complexities. However, before embarking on this technological transformation, it is crucial to conduct a thorough CBA to ensure the investment in AI delivers tangible value and aligns with the airport's strategic goals. By examining both the costs and benefits associated with AI implementation, airport authorities can make informed decisions that balance technological advancements with fiscal responsibility.

The financial figures presented in this section are for illustrative purposes only. This section provides a detailed guide on how to perform a CBA for AI in airport security, complete with practical examples to illustrate the potential impact and value of this investment.

DEFINING THE SCOPE AND OBJECTIVES

To start, it is essential to clearly define the scope of the AI implementation. The example project describes the integration of an AI analytical layer into the airport's access control monitoring system. The primary objectives are to improve the efficiency of security personnel, enhance threat detection at secure access points, and reduce operational costs associated with false alarms and incident investigations.

IDENTIFYING COSTS

When considering the costs, it is necessary to account for the initial investment and ongoing expenses.

- **Capital Expenses (CAPEX):** These are one-time, upfront expenditures. For this project, they include the AI software licenses, server hardware, system integration with the existing access control infrastructure, and initial staff training.
- **Operational Expenses (OPEX):** These are recurring expenses required to maintain the system. They include annual software maintenance contracts, technical support, data storage/cloud fees, and any marginal increase in network bandwidth or electricity consumption.

IDENTIFYING BENEFITS

The benefits of incorporating AI can be categorized into tangible and intangible benefits.

- **Tangible Benefits:** These benefits can be directly measured in monetary terms. For instance, AI can significantly improve operational efficiency by automating manual monitoring tasks, allowing for the strategic reallocation of personnel. It also reduces the time and labor costs associated with investigating security alerts and responding to false alarms.
- **Intangible Benefits:** These benefits, while not directly measurable in monetary terms, are equally valuable. An improved security posture enhances the airport's reputation, and faster, more accurate security processes can lead to higher satisfaction among staff who rely on the system.

QUANTIFYING COSTS AND BENEFITS

To make an informed decision, monetary values need to be assigned to the identified costs and benefits. Table 6 provides key information to get started building a CBA.

Project Costs
CAPEX: $100,000
This one-time, upfront cost in Year 0 covers the AI software, integration, necessary hardware upgrades, and initial training for security and IT staff.

OPEX: $20,000 Annually
This recurring annual cost covers software maintenance, technical support, and data storage fees.

Tangible Benefits (Estimated Annual Savings)
By analyzing common operational inefficiencies, we can project the following annual savings:

- **Reduced Labor Costs via Personnel Optimization, $40,000.** The AI system can monitor hundreds of access points simultaneously and intelligently flag only true anomalies. This automates the need for constant human monitoring of live feeds, allowing for the reallocation of one security officer's time from passive monitoring to active patrol for 4 hours per shift.
- **Increased Efficiency in Incident Investigation, $9,600.** When an alert occurs, AI can instantly retrieve and collate relevant video clips from multiple angles, cutting investigation time dramatically. We estimate this saves 20 hours of investigative work per month.
- **Reduced Costs from False Alarm Responses, $6,000.** AI is significantly better at distinguishing between genuine threats (e.g., forced entry) and false alarms (e.g., environmental factors). We project a 75% reduction in false alarms, saving approximately 150 person-hours annually.

Based on this breakdown, the Total Estimated Tangible Annual Benefit is $55,600. For simplicity in our CBA, this will be rounded to $56,000.

Intangible Benefits

- **Enhanced Security Posture:** AI's ability to detect sophisticated threats like piggybacking or loitering near restricted areas provides a proactive security layer that is nearly impossible to achieve with human monitoring alone.
- **Improved Safety:** By ensuring only authorized personnel are in secure areas, the system directly reduces the risk of accidents, sabotage, or other safety incidents.
- **Data-Driven Decision-Making:** The system will generate a wealth of data on access patterns and failed entry attempts. This data is invaluable for optimizing security staffing and making informed strategic decisions.
- **Improved Reputation:** An airport that invests in cutting-edge security technology builds a reputation for being safe, modern, and innovative, which can attract airlines and increase passenger confidence.

Table 6. Cost-Benefit Analysis Summary

Metric	Description	Value
Initial Investment (CAPEX)	One-time cost in Year 0	($100,000)
Annual Operating Cost (OPEX)	Recurring annual cost	($20,000)
Annual Tangible Benefit	Projected annual savings	$56,000
Annual Net Cash Flow (Yrs 1-5)	Benefits minus ongoing costs	$36,000

Table 7. Five-Year Cash Flow Projection

Category	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Total Annual Benefits	$0	$56,000	$56,000	$56,000	$56,000	$56,000	$280,000
Total Annual Costs	($100,000)	($20,000)	($20,000)	($20,000)	($20,000)	($20,000)	($200,000)
Net Cash Flow	($100,000)	$36,000	$36,000	$36,000	$36,000	$36,000	$80,000
Cumulative Cash Flow	($100,000)	($64,000)	($28,000)	$8,000	$44,000	$80,000	

As the cash flow projection demonstrates, the key financial metrics for this project are a Payback Period of 2.78 years and a 5-Year ROI of 40%.

7.2 Net Present Value

To understand if an AI project for airport security is truly worth the investment, NPV is used. It helps compare the value of the money to be saved or gained in the future, like improved efficiency and lower labor costs, with what is available to spend today. Since money loses value over time, NPV gives a clearer picture of whether the long-term benefits of adding AI (e.g., faster threat detection, improved operational personnel efficiencies, better flow management) outweigh the upfront costs. The NPV formula is shown in Figure 8.

Figure 8. Net Present Value Formula

$$\text{NPV} = \sum_{t=0}^{n} \frac{\text{Net Cash Flow}_t}{(1+r)^t}$$

The NPV formula has the following components:

- **n (Number of periods):** This represents the total number of periods (usually years) in the analysis. For example, in a 5-year analysis, 'n' would be 5.
- **Σ (Sigma):** This is a mathematical symbol that means "summation." It indicates that you need to perform the calculation for each year of the project and then add all the results together.
- **t (Time Period):** This represents the specific year of the project you are calculating for (e.g., Year 0, Year 1, Year 2, etc.).
- **r (Discount Rate):** This is the rate used to adjust future cash flows to their present value. It represents the time value of money and typically reflects the organization's cost of capital or a target rate of return (e.g., 12%).

Using the corrected cash flow projections from the CBA (Table 4), an initial outlay of ($100,000) and an annual net cash flow of $36,000 for five years, the following NPV is calculated in Table 8.

Table 8. NPV for Each Year

Year	Net Cash Flow	Present Value Calculation	Present Value
0	($100,000)	-$100,000 / (1 + 0.12)^0	($100,000.00)
1	$36,000	$36,000 / (1 + 0.12)^1	$32,142.86
2	$36,000	$36,000 / (1 + 0.12)^2	$28,702.55
3	$36,000	$36,000 / (1 + 0.12)^3	$25,627.28
4	$36,000	$36,000 / (1 + 0.12)^4	$22,872.57
5	$36,000	$36,000 / (1 + 0.12)^5	$20,427.29
		Total NPV:	**$29,772.55**

Based on the tangible financial figures, this project is highly recommended. The NPV is positive at $29,772.55, and the 5-year Return on Investment (ROI) is 40%.

This indicates that even after accounting for the time value of money with a significant 12% discount rate, the quantifiable financial benefits still outweigh the costs. When the considerable intangible benefits—such as enhanced security posture and improved operational intelligence—are also considered, the business case for this investment becomes exceptionally strong.

7.3 Return on Investment and Strategic Considerations

While NPV provides a clear dollar value for a project's profitability, ROI offers a powerful percentage-based metric for comparing its efficiency against other potential capital projects. A project's ROI is calculated by dividing the net profit by the total cost of the investment.

The formula for ROI is provided in Figure 9.

Figure 9. Return on Investment Formula

$$\text{ROI} = \left(\frac{\text{Net Profit (from NPV)}}{\text{Total Investment Cost}}\right) \times 100\%$$

For this project, the 5-year net profit is $80,000 and the total cost is $200,000. The ROI calculation is as follows in Figure 10:

Figure 10. ROI for Access Control System AI Integration

$$ROI = \frac{\text{Net Profit}}{\text{Total Cost}} \times 100\% = \frac{\$80{,}000}{\$200{,}000} \times 100\% = 40\%$$

The calculated ROI should not be viewed as a static, guaranteed figure. It is based on a series of assumptions about future costs and benefits. This is why performing a sensitivity analysis is a critical step in the decision-making process. A sensitivity analysis helps in understanding how changes in key assumptions, such as a higher-than-expected maintenance cost or lower-than-projected labor savings, affect the final NPV and ROI. This step is crucial for assessing the robustness of the financial case and ensuring the conclusions remain valid under different scenarios, providing a clearer picture of the project's potential risks and rewards.

Ultimately, the decision to proceed with an AI project is based on a holistic evaluation of this financial analysis. A positive NPV and a strong ROI indicate that the investment is financially sound and worthwhile to pursue from a quantitative perspective. However, the final decision must also incorporate the significant intangible benefits outlined in the CBA. The enhanced security, improved safety, and better passenger experience may hold strategic value that far exceeds the calculated financial return. Therefore, the final determination should balance the quantitative analysis (NPV and ROI) with a qualitative assessment of how the project aligns with the airport's core mission and long-term strategic goals.

SECTION 8: DEPLOYMENT CONSIDERATIONS

Deploying AI in an airport security environment is more than a technical upgrade; it is a strategic business decision that requires a structured, top-down approach. For AI to be a force multiplier for security, operations, and law enforcement, leaders must guide the process through a deliberate life cycle. This guide distills the complex landscape of AI deployment into five phases that integrate the foundational knowledge provided throughout this document.

8.1 Phase 1: Establish the Foundation (Strategy and Governance)

Before evaluating any technology, the “rules of the runway” must be defined. This foundational work ensures that any AI system deployed aligns with the airport’s strategic goals, ethical standards, and risk tolerance.

- **Form an AI Governance Committee:** Assemble a cross-functional team of leaders from Security, Operations, IT, Legal, and HR. This body is accountable for the entire AI strategy, ensuring all members have a shared understanding of the core concepts presented in Section 2: Understanding AI. The committee’s primary role is to oversee the entire life cycle and mitigate the full spectrum of potential issues, from technical failures to ethical missteps, as detailed in Section 4: Potential Risks of AI Use.
- **Define the "Why" with Specific Outcomes:** Move beyond vague goals. Leveraging the examples of AI capabilities outlined in Section 3: AI Applications in Airport Security, the committee’s first task is to define success in measurable terms. Each potential case should be supported by a robust financial justification, using the CBA and ROI models described in Section 7: Developing a Business Case.
- **Set Clear Ethical Guardrails:** Proactively address the risks of bias, fairness, and privacy. The governance framework must be built on the legal and regulatory requirements discussed in Section 5: Privacy, Legal, and Regulatory Considerations. This includes establishing clear policies on data use and transparency to build and maintain public trust, directly addressing the concerns raised in Section 4.5: Bias, Fairness, and Ethical Risks.
- **Adopt a Full Life Cycle Mindset:** Plan for the AI system from procurement to decommissioning. This includes budgeting for ongoing maintenance, model updates, and eventual replacement.

8.2 Phase 2: Choose the Right Partner and Technology

The success of an AI initiative heavily depends on the technology that is chosen and the partner vendor. Airport security teams must look past the sales pitch and conduct rigorous due diligence informed by technical, operational, and ethical knowledge.

- **Scrutinize the Vendor, Not Just the Algorithm:** Prioritize vendors with proven experience in aviation or similarly complex environments. Use the terminology from Section 2 to ask tough questions about their technology (e.g., “Is this a CV model based on a CNN?”). Require them to explain how they mitigate the risks of data poisoning and adversarial attacks discussed in Section 4: Potential Risks of AI Use. Ensure their practices align with the voluntary frameworks, such as the NIST AI RMF, outlined in Section 5.5: Standards and Framework.

- **Demand Actionable Service Level Agreements:** The binding contract must clearly define vendor commitments for what truly matters:
    - **Availability:** Ask what the guaranteed system uptime is (e.g., 99.9%)?
    - **Performance:** Ask what the promised accuracy rate is and what the penalties for underperformance are.
    - **Support:** How quickly will they resolve critical issues?
- **Require Secure and Open Systems:** Any new AI system must integrate safely with existing infrastructure. This requires vendors to provide secure, well-documented APIs that meet the technical IT controls detailed in Section 6: Data Management, Integration, and Infrastructure Considerations.

CONSIDERATIONS FOR DEVELOPING TECHNICAL REQUIREMENTS AND SPECIFICATIONS

Implementing AI in airport security requires more than just technical specifications—it demands a holistic approach that addresses operational, regulatory, and risk factors. [67] While AI applications such as deep learning and neural networks require substantial computational power, high-performance GPUs, and robust data storage solutions, airports must also consider the following:

Key Technical and Operational Considerations:

- **Cybersecurity and Data Privacy:** AI systems process sensitive passenger and operational data. Requirements should mandate encryption standards, secure data transmission protocols, and compliance with privacy regulations.
- **Interoperability:** AI solutions must integrate seamlessly with existing airport systems, including surveillance, access control, and baggage handling. Define API standards and data exchange formats early to avoid costly retrofits.
- **Scalability:** Design requirements to accommodate future growth in passenger volume and evolving threat landscapes. Modular architectures and cloud-based solutions can support incremental upgrades.
- **Reliability and Redundancy:** Ensure continuous operation during outages by including failover mechanisms, backup servers, and offline operational modes in technical specifications.
- **Performance Benchmarks:** Establish measurable KPIs such as detection accuracy, false positive rates, and latency thresholds for real-time processing. These benchmarks should be validated during pilot testing.
- **Environmental Constraints:** Hardware deployed in terminals or outdoor areas must withstand temperature fluctuations, humidity, and dust. Include environmental durability in procurement specifications.
- **Compliance and Certification:** Align requirements with FAA, TSA, and ICAO standards. Include certification processes for AI algorithms and hardware to ensure regulatory approval.

Practical Guidance for Airports

- **Engage Subject Matter Experts:** Collaborate with AI and cybersecurity professionals during requirements development to avoid gaps and ensure best practices.
- **Conduct a Risk Assessment:** Identify operational, financial, and reputational risks associated with AI deployment and incorporate mitigation strategies into requirements.

[67] "AI Advancements in Airport Security: Transforming Safety and Efficiency."

- **Pilot Programs:** Implement small-scale pilots to validate technical assumptions and performance benchmarks before full-scale deployment.
- **Vendor Evaluation Framework:** Develop criteria for selecting vendors, including aviation experience, compliance history, and ability to provide ongoing support.
- **Training and Change Management:** Include requirements for staff training and operational readiness to ensure smooth adoption and minimize resistance.
- **Life Cycle Management:** Plan for updates, patches, and end-of-life replacement during the requirements phase to maintain system integrity over time.

8.3 Phase 3: Ensure a Successful Go-Live (Implementation and Testing)

A deliberate and phased implementation is critical to managing risk, demonstrating value, and ensuring the technology works in the airport's unique environment.

- **Start Small with a "Crawl, Walk, Run" Approach:** Begin with a pilot project. Use this "crawl" phase to test the technology against specific goals from the business case (Section 7) and uncover any unforeseen challenges before a full airport-wide deployment.
- **Test for Failure, Not Just Success:** Go beyond standard performance testing. As recommended in Section 4.6: Strategies for Risk Mitigation, task teams with actively trying to fool or break the AI system (i.e., "red teaming"). This process must validate the system against the full range of potential risks, from cybersecurity threats to biased outputs.
- **Validate for Bias and Data Quality:** Rigorously test the system against diverse demographic data to ensure it does not produce the discriminatory outcomes detailed in Section 4.5. This requires a foundation of high-quality, representative data, underscoring the principles of data management laid out in Section 6.1: Airport Big Data Concepts and Quality.

8.4 Phase 4: Prepare People for Change (The Human Element)

The most sophisticated AI is useless if staff do not trust it, understand it, or know how to use it. The human element is the most critical component of a successful AI deployment.

- **Invest in Role-Specific Training:** Cybersecurity analysts and frontline security officers require different training. Education must cover the specific AI types (see Section 2), their operational applications (see Section 3), and crucially, the risks of automation bias—the tendency to over-rely on the machine—as detailed in Section 4.
- **Manage the Change Proactively:** Communicate the "why" behind the AI implementation openly and frequently. Address concerns and fears head-on, emphasizing that the goal is to augment human expertise, not replace it.
- **Reinforce Human-in-the-Loop Authority:** As defined in Section 4, HITL is non-negotiable for critical security decisions. Trained personnel are the final authority. The AI provides recommendations, but human oversight and judgment are paramount.
- **Training Staff for AI Deployment:** Effective training is the bridge between technology and trust. It ensures that the investments in role-specific education, proactive change management, and HITL authority translate into operational success. Training programs should begin with foundational AI literacy so staff understand system capabilities and limitations, and then progress to scenario-based exercises that demonstrate real-world applications and highlight the risks of automation bias. Hands-on modules tailored to cybersecurity analysts, frontline security officers, and supervisors will build confidence in interpreting alerts and applying escalation

protocols. Ethical and compliance considerations must be embedded throughout, reinforcing privacy and regulatory obligations. Finally, continuous learning opportunities, updates, and feedback loops will sustain competence and accountability as AI systems evolve. This holistic approach prepares personnel not only to use AI effectively but to remain the ultimate decision-makers in critical security operations.

8.5 Phase 5: Sustain Performance and Trust (Ongoing Management)

Deployment is the beginning, not the end. AI systems require continuous oversight to ensure they remain effective, secure, and trustworthy over time.

- **Monitor for "Model Drift":** An AI model's performance can degrade as real-world conditions change. Implement the continuous performance monitoring discussed in Section 6 to track accuracy and work with vendors on a schedule for retraining the model.
- **Plan for AI-Specific Incidents:** The standard incident response plan is not enough. Using the risks identified in Section 4, develop playbooks for AI-specific failures, such as what to do if the system is compromised or produces mass false alarms. The response plan should be integrated with the technical monitoring controls (e.g., Security Information and Event Management) described in Section 6.
- **Conduct Regular Audits:** Periodically audit the AI system's performance, fairness, and security posture. This process demonstrates accountability and ensures ongoing compliance with the legal, regulatory, and ethical frameworks detailed in Section 5.

SECTION 9: RECOMMENDATIONS FOR FUTURE RESEARCH

As AI becomes more deeply integrated into airport security, the pace of technological and societal change requires a forward-looking research agenda. The dual-use nature of AI—serving as both a powerful security tool and a potential vector for new threats—necessitates continuous inquiry.[68] To ensure future AI systems are secure, effective, and trustworthy, research should focus on several key areas. These recommendations are designed to guide airport security leaders, technology partners, and policymakers in anticipating challenges and shaping the next generation of AI-driven security.

9.1 Emerging AI Terminology (The Near Future)

Airport leaders should be aware of the next wave of concepts, such as the following:

XAI: Moving beyond "black box" systems, XAI focuses on developing models that can provide clear, human-understandable justifications for their decisions. This is becoming a requirement for trust, accountability, and debugging in high-stakes environments.

Digital Twins: Already a reality in some airports, the digital twin is a virtual, real-time replica of an airport's physical assets and operational systems. This technology will be used to simulate potential security threats, test AI responses, and optimize resource allocation without impacting live operations.

Federated Learning: This is a privacy-preserving ML technique where the AI model is brought to the data, rather than the data being brought to a central model. This allows multiple airports to collaboratively train a more effective model without sharing sensitive, proprietary, or passenger data.

Neuro-Symbolic AI: This is an advanced approach that combines the pattern-matching strengths of neural networks with the logical reasoning of symbolic AI. The goal is to create systems that are able to recognize a threat as well as "reason" about the context, intent, and causality behind it.

Artificial General Intelligence (AGI): AGI is a hypothetical future form of AI with the capacity to understand or learn any intellectual task that a human can. While not yet a reality, understanding the concept is crucial for long-term strategic planning and risk assessment.

9.2 Preparing for Next-Generation AI Applications

The capabilities of AI are expanding beyond pattern recognition into autonomous action and advanced reasoning. Airports must begin researching the implications of these next-generation technologies to prepare for their eventual integration.

Autonomous Systems and AI-Powered Virtual Employees. As AI capabilities grow, the concept of "fully AI employees" for tasks like security monitoring, dispatch, or administrative processing is becoming a near-term possibility. Research is needed to establish governance frameworks for these autonomous agents to ensure they operate safely and ethically, and align with human command intent. This includes understanding how to best automate tasks currently performed by law enforcement and security personnel to enhance, not just replace, human roles.[69]

[68] Conceal.io, "AI in Cybersecurity: Navigating the Digital Frontier," February 1, 2024, White Paper.
[69] Veritone, Inc., "Comprehensive Guide to AI in Law Enforcement - Veritone," February 1, 2024, https://www.veritone.com/blog/ai-in-law-enforcement/.

The Impact of AGI. The potential emergence of AGI—AI with human-like general intelligence—demands strategic foresight. As noted by government advisors and industry leaders, the rapid progress in foundation models tracked by the Stanford AI Index suggests that research into the profound security and societal implications of AGI for critical infrastructure is no longer premature.[70]

9.3 Enhancing AI Trustworthiness and Reliability

A primary barrier to the adoption of advanced AI is a lack of trust in its decision-making processes. Future research must prioritize making AI systems more transparent, reliable, and accountable, especially in high-stakes airport environments.

XAI and "Glass Box" Models: Research should accelerate the shift from opaque, black box systems toward inherently interpretable "glass box" models.[71] XAI provides transparent justifications for its decisions, which is crucial for operator trust, accountability, and regulatory compliance.[72] For example, research building on the successful implementation of explainable passenger flow algorithms at airports like Cincinnati/Northern Kentucky International can provide a roadmap for other high-stakes applications.[73]

Validating the Scientific Basis of AI Applications: A critical area for research involves scrutinizing the underlying scientific validity of AI-driven security applications. For instance, research has questioned the reliability of using AI to detect deception from micro-expressions, arguing that the psychological science itself lacks definitive support. Future research must rigorously validate that the premises upon which security AI is built are sound before such systems are deployed at scale.[74]

Continuous Learning in Secure Environments: Future systems will need to learn and adapt to new threats in real time. Research is needed to develop safe and secure continuous learning frameworks that allow AI models to be updated with new data without being taken offline or becoming vulnerable to data poisoning attacks during the learning process.

9.4 Securing AI Systems Against Novel Threats

As airports adopt more AI, these systems become attractive targets for adversaries. The security of the AI itself is a critical and evolving research domain that requires urgent attention. While cybersecurity was not the focus of this guidance, including future recommendations on cybersecurity is key in maintaining an eye on future airport controls around the digital space at airports.

Proactive Cybersecurity for AI: Adversaries are already using AI "to launch complex, sophisticated, and frequent cyberattacks on US critical infrastructure."[75] Future research must focus on developing AI-specific defense mechanisms. This includes creating countermeasures for emerging threats like prompt injection and data poisoning targeting Retrieval-Augmented Generation systems. The "ConfusedPilot"

[70] Klein, "Opinion | The Government Knows A.G.I. Is Coming"; Maslej et al., *The AI Index 2024 Annual Report*.
[71] Brandon L. Garrett and Cynthia Rudin, "The Right to a Glass Box - Rethinking the Use of Artificial Intelligence in Criminal Justice," *Cornell University Law Review* 109 (2024): 561–627.
[72] Pik, "Airport Security: The Impact of AI on Safety, Efficiency, and the Passenger Experience."
[73] Viaña et al., "Explainable Algorithm to Predict Passenger Flow at Cincinnati/Northern Kentucky International Airport."
[74] Louise Marie Jupe and David Adam Keatley, "Airport Artificial Intelligence Can Detect Deception: Or Am I Lying?," *Security Journal* 33, no. 4 (December 1, 2020): 622–35, doi:10.1057/s41284-019-00204-7.
[75] U.S. Department of Homeland Security, *Artificial Intelligence: Roadmap 2024*.

hack, which demonstrated how to manipulate knowledge bases that feed LLMs, highlights the urgent need for research into securing these systems to prevent data corruption and operational sabotage.[76]

Advanced Threat Simulation and Digital Twins: Research should explore using digital twins—virtual replicas of an airport's entire operational and IT environment—to enhance cybersecurity. By integrating AI with a digital twin, security teams can simulate complex cyberattack scenarios, test defenses against threats like those targeting 5G aviation networks, and identify vulnerabilities without risking the live operational network.[77]

9.5 Navigating the Evolving Legal, Ethical, and Human Landscape

The most significant challenges for future AI adoption may be human-centric. Research must address the legal, ethical, and workforce dimensions of this technological shift.

As discussed in Section 5.6, regulatory action on AI remains fragmented, with US federal efforts to date focused primarily on funding and research coordination rather than comprehensive legal frameworks. For aviation, the FAA Reauthorization Act of 2018 expressed Congress's intent for the FAA to periodically review AI applications and consider standards and best practices. More recently, a 2023 Executive Order required federal agencies to appoint chief AI officers and establish safety and security standards, signaling a gradual shift toward structured oversight. Similar developments are emerging at the state level and internationally, although progress remains uneven.

Looking ahead, legal trends will likely be shaped by the rapid evolution of AI capabilities and public perception of AI technology and its developers. As noted in Section 5.6, if trust in AI systems and their creators remains strong, regulatory approaches may favor innovation and investment. Conversely, diminished trust or heightened concerns about risk could accelerate calls for stricter oversight. This dynamically underscores the uncertainty and complexity of the regulatory landscape as governments seek to balance risk mitigation with the strategic benefits of AI leadership.

Future of AI Regulation: As noted in the FAA Reauthorization Act of 2018 and Executive Order 14110, US regulatory action has been preliminary. Future research should analyze emerging comprehensive legal frameworks, like the EU AI Act, to develop best practices for US airports. This includes anticipating regulations around biometric data privacy, algorithmic bias, and mandatory risk assessments for high-risk AI systems.[78]

AI Literacy and Human-AI Teaming: Widespread AI deployment requires an AI-literate workforce. Research should focus on developing effective training programs that build practical skills and address the psychological factors of working alongside AI.[79] A critical area of study is mitigating automation

[76] Ayush RoyChowdhury et al., "ConfusedPilot: Confused Deputy Risks in RAG-Based LLMs," 2024, https://arxiv.org/pdf/2408.04870; Pauline Norstrom and Anekanta Consulting; SIA Cybersecurity Advisory Board, "The ConfusedPilot Hack: A Wake-Up Call for Identity and Access Management and Physical Access Control," *Security Industry Association*, October 23, 2024, https://www.securityindustry.org/2024/10/23/the-confusedpilot-hack-a-wake-up-call-for-identity-and-access-management-and-physical-access-control/.

[77] Abraham Itzhak Weinberg, "The Role and Applications of Airport Digital Twin in Cyberattack Protection during the Generative AI Era," August 13, 2024, https://arxiv.org/pdf/2408.05248; Huw Whitworth et al., "5G Aviation Networks Using Novel AI Approach for DDoS Detection," July 2023, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10185042&isnumber=10005208.

[78] Kyriazanos, Thanos, and Thomopoulos, "Automated Decision Making in Airport Checkpoints: Bias Detection Toward Smarter Security and Fairness."

[79] U.S. Department of Labor, Employment and Training Administration, Artificial Intelligence Literacy Framework: A Guide for Workforce and Education Systems, February 13, 2026, 14, https://www.dol.gov/sites/dolgov/files/ETA/advisories/TEN/2025/TEN%2007-25/TEN%2007-25.pdf.

bias, where personnel may over-rely on an AI's recommendation. Understanding how to design systems and training that keep a human meaningfully in the loop is essential for safety and accountability.[80]

Collaboration and Best Practice Sharing: No airport can address these challenges alone. Research is needed to create effective frameworks for collaboration between airports, government agencies, and international law enforcement bodies.[81] This includes developing standardized methods for sharing threat intelligence and performance data, and best practices to collectively improve security across the entire aviation ecosystem.[82]

[80] Kahn, Probasco, and Kinoshita, *AI Safety and Automation Bias: The Downside of Human-in-the-Loop*.
[81] U.S. Department of Homeland Security, *Artificial Intelligence: Roadmap 2024*; "Artificial Intelligence Toolkit," accessed August 4, 2025, https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit.
[82] Amiri and Kuşakcı, "A Scoping Review of Artificial Intelligence Applications in Airports."

SECTION 10: CONCLUSION

The integration of AI into airport security represents a transformative shift in how airports manage safety, efficiency, and passenger experience. This guidebook explores the multifaceted dimensions of AI deployment, from foundational concepts and technical applications to legal, ethical, and operational considerations. As airports face increasing demands for security and service excellence, AI offers a powerful toolkit to enhance threat detection, streamline operations, and support informed decision-making. However, realizing these benefits requires a deliberate, risk-informed approach that balances innovation with accountability.

This report emphasizes that AI is not a one-size-fits-all solution, but rather a dynamic set of tools—such as ML, CV, NLP, and generative AI—that offer unique strengths and limitations. For airport security professionals, the value of AI lies in its ability to enhance real-time situational awareness, automate threat detection, and support smarter decision-making at every checkpoint and access point. Successful implementation depends on thoughtful integration with existing security infrastructure, clear operational objectives, and a practical understanding of how AI can complement human judgment. Real-world examples show that, when deployed strategically, AI can significantly improve outcomes such as identifying anomalies, streamlining screening processes, and optimizing the use of security personnel.

Equally important are the risks and challenges associated with adoption of AI. Issues such as algorithmic bias, automation bias, lack of explainability, and cybersecurity vulnerabilities must be proactively addressed. The report outlines comprehensive mitigation strategies, including HITL oversight, vendor accountability, and adherence to international standards such as ISO/IEC 4200 and the NIST AI Risk Management Framework. These frameworks provide a foundation for trustworthy AI deployment that respects privacy, civil liberties, and regulatory obligations.

The guidebook also underscores the importance of organizational readiness. Successful AI implementation hinges on cross-functional collaboration, continuous staff training, and a culture that embraces responsible innovation. Airports must invest in scalable infrastructure, establish clear governance structures, and engage stakeholders early in the process. A phased deployment strategy, supported by rigorous testing and validation, ensures that AI systems are both effective and adaptable to evolving threats and operational needs.

Looking ahead, the future of AI in airport security will be shaped by continued advancements in technology, evolving regulatory frameworks, and lessons learned from real-world deployments. For physical security practitioners, this means staying attuned to developments in XAI, automated threat detection, and AI-assisted surveillance tools that enhance situational awareness and response times. As AI becomes more integrated into perimeter monitoring, access control, and passenger screening, airports that adopt a proactive, well-governed approach grounded in operational needs and ethical considerations will be best positioned to strengthen their security posture and adapt to emerging challenges.

In conclusion, AI holds immense promise for enhancing airport security, but its deployment must be guided by strategic foresight, operational discipline, and a commitment to public trust. This guidebook provides a roadmap for navigating this complex terrain, empowering airport leaders to harness AI’s potential while safeguarding the values and responsibilities that underpin aviation security.

REFERENCES

"49 CFR 1542 - Airport Security." *National Archives Code of Federal Regulations*, February 22, 2002. https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1542.

"About SIA." *Security Industry Association*, n.d. https://www.securityindustry.org/about-sia/.

"AI Principles Overview." *Organisation for Economic Co-Operation and Development*, updated 2024 2019. https://oecd.ai/en/principles.

Alabama Legislature. *Alabama Data Breach Notification Act of 2018*. Vol. 8-38–1 to 8-38–12, 2018. https://alison.legislature.state.al.us/code-of-alabama?section=8-38-1.

AlSeddiqi, Mahmood. "The Power of AI and Machine Learning for Airport Operations." *International Airport Review*, September 18, 2024. https://www.internationalairportreview.com/article/222537/the-power-of-ai-and-machine-learning-for-airport-operations/.

Amiri, Misagh Haji, and Ali Osman Kuşakcı. "A Scoping Review of Artificial Intelligence Applications in Airports." *CRPASE: Transactions of Industrial Engineering* 10, no. 2 (June 2024): 1–12.

"Artificial Intelligence Toolkit." Accessed August 4, 2025. https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit.

Brown, Tom B., Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelekantan, et al. "Language Models Are Few-Shot Learners," July 22, 2020. https://arxiv.org/pdf/2005.14165.

Brownlee, Jason. *Deep Learning for Time Series Forecasting: Predict the Future with MLPs, CNNs and LSTMs in Python*. Machine Learning Mastery, 2018.

Calvino, F. et al. "A Sectoral Taxonomy of AI Intensity." *OECD Artificial Intelligence Papers* 30, no. OECD Publishing, Paris (2024). https://doi.org/10.1787/1f6377b5-en.

Conceal.io. "AI in Cybersecurity: Navigating the Digital Frontier," February 1, 2024. White Paper.

Coutinho, Mariana. "#Why Airports Need Strong Data Governance - Ivy Partners," February 12, 2025. https://www.ivy.partners/why-airports-need-strong-data-governance/, https://www.ivy.partners/why-airports-need-strong-data-governance/.

"DeepSeek Rushes to Launch New AI Model as China Goes All in | Reuters." Accessed August 4, 2025. https://www.reuters.com/technology/artificial-intelligence/deepseek-rushes-launch-new-ai-model-china-goes-all-2025-02-25/.

"Enhancing Airport Security: Transformative Role of AI Across the Industry." *Airport Cooperative Research Program | Applied Technology in Airports*, June 17, 2024. https://crp.trb.org/acrptransformativetech/applied-technology-in-airports/enhancing-airport-security-transformative-role-of-ai-across-the-industry/.

Etlinger, Susan. "Building a Foundation for AI Success." *The Microsoft Cloud Blog*, October 12, 2023. https://www.microsoft.com/en-us/microsoft-cloud/blog/2023/10/12/building-a-foundation-for-ai-success-a-six-part-series-on-ai-leadership/.

Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 2023. https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

FAA Reauthorization Act of 2018. *Public Law 115-254*, 2018. https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf.

Federal Trade Commission v. Rite Aid Corporation, (Eastern District of Pennsylvania Federal Court Pending).

Garrett, Brandon L., and Cynthia Rudin. "The Right to a Glass Box - Rethinking the Use of Artificial Intelligence in Criminal Justice." *Cornell University Law Review* 109 (2024): 561–627.

———. "The Right to a Glass Box: Rethinking the Use of Artificial Intelligence in Criminal Justice." *Cornell Law Review* 109 (2024): 561–627.

"Glossary." *National Institute of Standards and Technology Computer Security Resource Center*. Accessed July 3, 2025. https://csrc.nist.gov/glossary.

Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. *Deep Learning*. Cambridge, Mass.: MIT Press, 2016.

Grammarly. *How an AI-Literate Workforce Is the New Competitive Advantage*. ebook, 2024. https://www.grammarly.com/business/events-resources/ebook/new-language-of-business.

"How AI Flight Data Analysis Revolutionizes Aviation Safety and Risk Prediction in 2025 - Axis Intelligence." Accessed August 4, 2025. https://axis-intelligence.com/ai-flight-data-analysis-revolutionizes-2025/.

International Organization for Standardization. "ISO/IEC 5259-1:2024 Artificial Intelligence — Data Quality for Analytics and Machine Learning (ML), Part 1: Overview, Terminology, and Examples." Geneva, Switzerland, July 2024. https://www.iso.org/standard/81088.html.

———. "ISO/IEC 5259-2:2024 Artificial Intelligence — Data Quality for Analytics and Machine Learning (ML), Part 2: Data Quality Measures." Geneva, Switzerland, November 2024. https://www.iso.org/standard/81860.html.

———. "ISO/IEC 5259-3:2024 Artificial Intelligence — Data Quality for Analytics and Machine Learning (ML), Part 3: Data Quality Management Requirements and Guidelines." Geneva, Switzerland, July 2024. https://www.iso.org/standard/81092.html.

———. "ISO/IEC 5259-4:2024 Artificial Intelligence — Data Quality for Analytics and Machine Learning (ML), Part 4: Data Quality Process Framework." Geneva, Switzerland, July 2024. https://www.iso.org/standard/81093.html.

———. "ISO/IEC 22989:2022 Information Technology - Artificial Intelligence - Artificial Intelligence Concepts and Terminology." Geneva, Switzerland, July 2022. https://www.iso.org/standard/74296.html.

———. "ISO/IEC 38507:2022 Governance Implications of the Use of Artificial Intelligence by Organizations." Geneva, Switzerland, 2022. https://www.iso.org/standard/56641.html.

Joy, Alwyn. "Redefining Airports with Advanced Technological Infrastructure." *Rezcomm*, August 24, 2023. https://www.rezcomm.com/resources/blog/ai/redefining-technological-infrastructure.

Jupe, Louise Marie, and David Adam Keatley. "Airport Artificial Intelligence Can Detect Deception: Or Am I Lying?" *Security Journal* 33, no. 4 (December 1, 2020): 622–35. doi:10.1057/s41284-019-00204-7.

Kahn, Lauren, Emelia S. Probasco, and Ronnie Kinoshita. *AI Safety and Automation Bias: The Downside of Human-in-the-Loop*. Center for Security and Emerging Technology, November 2024. https://cset.georgetown.edu/wp-content/uploads/CSET-AI-Safety-and-Automation-Bias.pdf.

Klein, Ezra. "Opinion | The Government Knows A.G.I. Is Coming." *The New York Times*, March 4, 2025, sec. Opinion. https://www.nytimes.com/2025/03/04/opinion/ezra-klein-podcast-ben-buchanan.html.

Kyriazanos, D. M., K. G. Thanos, and S. C. A. Thomopoulos. "Automated Decision Making in Airport Checkpoints: Bias Detection Toward Smarter Security and Fairness." *IEEE Security & Privacy* 17, no. 2 (April 2019): 8–16. doi:10.1109/MSEC.2018.2888777.

Lloyd's Futureset. *Generative AI: Transforming the Cyber Landscape*, March 2024. https://assets.lloyds.com/media/439566f8-e042-4f98-83e5-b430d358f297/Lloyds_Futureset_GenAI_Transforming_the_cyber_landscape.pdf.

Maslej, Nestor, Loredana Fattorini, Raymond Perrault, Vanessa Parli, Anka Reuel, Erik Brynjolfsson, John Etchemendy, et al. *The AI Index 2024 Annual Report*. Stanford University, Stanford, Calif.: AI Index Steering Committee, Institute for Human-Centered AI, 2024. https://hai.stanford.edu/assets/files/hai_ai-index-report-2024-smaller2.pdf.

National Institute of Standards and Technology. *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, July 2024. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.

———. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, January 2023. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

———. "Information Leakage - Glossary | CSRC." *National Institute of Standards and Technology*, n.d. https://csrc.nist.gov/glossary/term/information_leakage.

———. *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, March 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

Norstrom, Pauline and Anekanta Consulting; SIA Cybersecurity Advisory Board. "The ConfusedPilot Hack: A Wake-Up Call for Identity and Access Management and Physical Access Control." *Security Industry Association*, October 23, 2024. https://www.securityindustry.org/2024/10/23/the-confusedpilot-hack-a-wake-up-call-for-identity-and-access-management-and-physical-access-control/.

Pik, Eugene. "Airport Security: The Impact of AI on Safety, Efficiency, and the Passenger Experience." *Journal of Transportation Security* 17, no. 1 (April 8, 2024): 9. doi:10.1007/s12198-024-00276-6.

"Protected Critical Infrastructure Information (PCII) Program." *Cybersecurity & Infrastructure Security Agency*, n.d. https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program.

"Real-World Applications of AI in Airport Operations." *Copenhagen Optimization*. Accessed August 4, 2025. https://copenhagenoptimization.com/blog/the-role-of-ai-and-machine-learning-in-airport-resource-optimization/.

"Regulation - EU - 2024/1689 - EN - EUR-Lex." *European Union*, 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

RoyChowdhury, Ayush, Mulong Luo, Prateek Sahu, Sarbartha Banerjee, and Mohit Tiwari. "ConfusedPilot: Confused Deputy Risks in RAG-Based LLMs," 2024. https://arxiv.org/pdf/2408.04870.

Screening Passengers and Property. *49 USC 44901*, 2001. https://uscode.house.gov/view.xhtml?req=granuleid:USC-2000-title49-section44901&num=0&edition=2000.

Security Industry Association. *SIA Principles for the Responsible and Effective Use of Facial Recognition Technology*, 2020. https://www.securityindustry.org/wp-content/uploads/2020/08/SIA-Principles-Responsible-Ethical-Facial-Recognition-Usage.pdf.

"Sensitive Security Information." *U.S. Department of Homeland Security Transportation Security Administration*, n.d. https://www.tsa.gov/for-industry/sensitive-security-information.

Simeonova, Antoaneta, and Angel Krumov. "AI Integration in Airport Security: A Case Study of Sofia Airport within Bulgaria's Critical Infrastructure Framework." *International Scientific Journal "Security & Future"* VIII, no. 3 (2024): 76–78.

Srivastava, Divyanshu Ranjan. "Ethical Concerns in AI-Powered Surveillance Technologies." *Medium*, October 6, 2024. https://divsriv.medium.com/ethical-concerns-in-ai-powered-surveillance-technologies-bdbd67ce6869.

Stefanov, Borche. "6 Ways AI Is Transforming Data Sharing and Security in Law Enforcement." *Kaseware*, May 29, 2025. https://www.kaseware.com/post/6-ways-ai-is-transforming-data-sharing-and-security-in-law-enforcement.

"The OECD Artificial Intelligence Policy Observatory." Accessed August 4, 2025. https://oecd.ai/en/.

"Types of Machine Learning." *IBM*, December 20, 2023. https://www.ibm.com/think/topics/machine-learning-types.

"Understanding the Scope of the Council of Europe Framework Convention on AI." *Opinio Juris*, November 5, 2024. https://opiniojuris.org/2024/11/05/understanding-the-scope-of-the-council-of-europe-framework-convention-on-ai/.

United Nations General Assembly. "Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development," March 11, 2024. https://docs.un.org/en/A/78/L.49.

United States v. Aukai, (United States Court of Appeals, Ninth Circuit 2007).

United States v. Biswell, 406 U.S. 311, (United States Supreme Court 1972).

U.S. Department of Homeland Security. *Artificial Intelligence: Roadmap 2024*, 2024. https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf.

———. "Screening at Speed," March 2024. https://www.dhs.gov/sites/default/files/2024-03/24_0304_st_ScreeningatSpeed_March2024.pdf.

"US State Privacy Legislation Tracker." *Iapp25*, July 7, 2025. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, and Illia Polosukhin. "Attention Is All You Need," August 2, 2023. https://arxiv.org/pdf/1706.03762.

Vats, Nitin. "The Ethics of AI in Monitoring and Surveillance." *NICE Systems*, January 1, 2024. https://www.niceactimize.com/blog/fmc-the-ethics-of-ai-in-monitoring-and-surveillance/.

Veritone, Inc. "Comprehensive Guide to AI in Law Enforcement - Veritone," February 1, 2024. https://www.veritone.com/blog/ai-in-law-enforcement/.

Viaña, Javier, Kelly Cohen, Stephen Saunders, Marx Naashom, and Brian Cobb. "Explainable Algorithm to Predict Passenger Flow at Cincinnati/Northern Kentucky International Airport." *Transportation Research Record* 2678(2) (2023): 839–62.

Weinberg, Abraham Itzhak. "The Role and Applications of Airport Digital Twin in Cyberattack Protection during the Generative AI Era," August 13, 2024. https://arxiv.org/pdf/2408.05248.

"What Is the Data, Information, Knowledge, Wisdom (DIKW) Model?" *Weje*, n.d. https://weje.io/blog/data-information-knowledge-wisdom.

Whitworth, Huw, Saba Al-Rubaye, Antonios Tsourdos, and Julia Jiggins. "5G Aviation Networks Using Novel AI Approach for DDoS Detection," July 2023. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10185042&isnumber=10005208.

Williams, Wyn. *Post Office Horizon IT Inquiry Report: Volume 1*. London: United Kingdom Government, 2025. https://www.postofficehorizoninquiry.org.uk/sites/default/files/2025-07/Post%20Office%20Horizon%20IT%20Inquiry%20Final%20Report%20Volume%201_0.pdf.

Wyoming Legislature. *Article 5 - Credit Freeze Reports*. Vol. 40-12–501 to 40-12–502, n.d. https://wyoleg.gov/statutes/compress/title40.pdf.

APPENDIX A: AIRPORT USE CASES

MEDIUM HUB AIRPORT #1 – PROJECT 1: AI FOR RADIO TRANSCRIPTION

This airport deployed an AI-based speech-to-text platform (referred to in outreach as *Voice Brain*) to continuously transcribe airport radio communications in the Airport Operations Center. The operational problem was that radio traffic was high-volume, jargon-heavy, and historically difficult to search or reconstruct during after-action reviews or investigations. The AI system captured radio traffic, generated searchable transcripts, enabled keyword alerts, and auto-generated daily communication logs.

Over time, the AI model improved transcription accuracy as it learned airport-specific phraseology and jargon. Airport staff stated that daily AI-generated logs were "surprisingly accurate," estimating 75% accuracy solely from transcription output, before any human correction.

Lessons Learned

Data Hygiene: During use, airport personnel discovered that transcripts and related artifacts were being stored in shared environments without consistent data classification. Outreach commentary explicitly notes that documents were being marked "public" when they should have been marked as non-public or sensitive. This raised concern that AI-generated content derived from radio traffic could be discoverable or misused if data hygiene and classification were not corrected.

SSI Concerns with Vendors: While radio frequencies themselves are public, airport leadership became concerned once AI transformed ephemeral radio chatter into persistent, searchable, vendor-processed records. Outreach respondents explicitly stated reluctance to allow vendors access to security data and clips, particularly where vendors might retain data or use it for training purposes.

These concerns were related to governance and data control, not AI transcription accuracy.

Investment Decision

After piloting the system, the airport decided to limit expansion and take a cautious approach to further use.

- The airport did not expand transcription to additional radio or phone lines
- Existing transcription was retained, but expansion was paused
- Future expansion was explicitly tied to deployment of a new Motorola Avtec Scout radio/phone system that may simplify integration and recording

The two explicit drivers for these decisions were:

1. **Cost structure:** The vendor charges per recorded (transcribed) line per month, meaning expansion increases recurring operational expenditures rather than a one-time capital expenditure
2. **Integration constraints:** The existing phone system created technical friction; leadership chose to wait for infrastructure modernization before expanding the AI system's scope

This was not a rejection of the use case; it was a scope containment decision driven by cost and legacy integration.

CBA / NPV / ROI

The airport did not measure costs and benefits for this project, and no sanitized or range-based figures were made available.

MEDIUM HUB AIRPORT #1 – PROJECT 2: AI FOR REAL-TIME ALERTS

The airport applied AI analytics to operational and security data streams to generate real-time alerts for anomalies.

Lessons Learned

While alerts improved awareness, the airport encountered challenges related to alert validation and integration complexity. In practice, not all alerts had sufficient contextual confidence, reinforcing the need for human validation and careful thresholding. This was not fully a technical failure, but a confidence and governance maturation issue.

Investment Decision

What was decided:

- Leadership chose a phased rollout
- Alerting remained limited to select use cases
- Widespread automation was deferred pending confidence in alert quality

Why:

- To avoid nuisance alerts
- To avoid operator desensitization
- To ensure false positives did not undermine trust in the system

CBA / NPV / ROI

The airport did not measure costs and benefits for this project, and no quantitative labor or response-time savings were captured.

MEDIUM HUB AIRPORT #2: VIDEO ANALYTICS FOR PERIMETER SECURITY

This airport deployed AI video analytics to reduce nuisance alarms generated by perimeter intrusion detection systems.

Lessons Learned

The airport described AI improving classification (human vs. animal), but only after extensive model training. False positives remained in edge cases (e.g., crawling humans vs. wildlife). The airport also observed that camera condition (e.g., dirty lenses) directly degraded AI performance.

Investment Decision

What was decided:

- Leadership adopted a phased rollout
- Some perimeter areas retained manual monitoring
- Expansion was limited by staff capacity to train and maintain models

Why:

- Training effort was non-trivial
- AI maturity did not yet justify full reliance
- Cost-benefit versus staffing remained marginal in some zones

CBA / NPV / ROI

The airport did not measure costs and benefits for this project.

LARGE HUB AIRPORT – PROJECT 1: QUEUE MONITORING / DYNAMIC RESOURCE ALLOCATION

This airport deployed AI queue analytics to monitor passenger flow at checkpoints, toll plazas, and concessions.

Lessons Learned

After early integration challenges with legacy systems, adoption expanded rapidly beyond the original security scope into operational and financial use cases. The lessons learned emphasize integration effort and continuous tuning, not feasibility failure.

Investment Decision

What was decided:

- The project transitioned from pilot to ongoing enterprise program
- AI analytics became embedded in day-to-day operations

Why:

- Leadership identified sustained operational value
- AI reduced blind spots in staffing and contract enforcement
- The organization accepted iterative tuning as a normal cost of ownership

CBA / NPV / ROI

The airport did not measure costs and benefits for this project.

LARGE HUB AIRPORT – PROJECT 2: CYBERSECURITY ANOMALY DETECTION

AI was deployed to learn baseline network and user behavior and flag anomalies.

Lessons Learned

The airport confirmed improvement in threat detection and incident prioritization but also emphasized human-in-the-loop review and governance.

Investment Decision

What was decided:

- Sustained adoption
- Continuous tuning
- Integration into cybersecurity operations

Why:

- Leadership assessed the risk of inaction as greater than tool cost
- AI enabled continued operations without adding staff

CBA / NPV / ROI

The airport cited qualitative benefits but no quantitative financial benefits. The system enabled the airport to avoid hiring one analyst.

NON-AVIATION SECTOR - PROJECT 1: PREDICTIVE MAINTENANCE

AI analyzed IoT and operational data from escalators, HVAC systems, and other infrastructure to enable predictive maintenance and reduce downtime.

Lessons Learned

The primary lesson learned was that governance and AI policy maturity lagged implementation, rather than technical limitations of the AI tools.

Investment Decision

- Outreach responses indicate continued deployment rather than pilot abandonment
- Operational efficiency and reduced reactive maintenance were cited as value drivers

CBA / NPV / ROI

The organization did not measure costs and benefits for this project.

NON-AVIATION SECTOR – PROJECT 2: CYBERSECURITY AUTOMATION

AI-enabled cybersecurity platforms, including SIEM and security automation tools, were used to ingest large volumes of logs and security telemetry, correlate events, and automate portions of alert triage and incident response. Outreach participants reported that these capabilities reduced the amount of manual analysis required by security staff and functioned as a force multiplier, allowing existing teams to focus on higher-value investigative and response activities rather than routine log review.

Lessons Learned

The primary lessons learned were governance-related rather than technical. Outreach responses noted concerns around acceptable AI use, control over AI-driven decision support, and the need to clearly define guardrails for how AI tools could access, process, and act on security data. These governance gaps highlighted the importance of formal policies, oversight mechanisms, and clear human-in-the-loop expectations to prevent over-reliance on automation and to ensure accountability for AI-assisted security decisions.

Investment Decision

Outreach responses indicate that AI-enabled cybersecurity automation remained in ongoing operational use, rather than being limited to a short-term pilot. Key investment-related outcomes derived from outreach include:

- AI-enabled SIEM and automation tools continued to be used in day-to-day cybersecurity operations
- Operational efficiency gains supported continued deployment without proportional increases in cybersecurity staffing
- Identified governance and acceptable-use gaps were addressed through policy development and clarification of oversight and control mechanisms, rather than discontinuing or rolling back AI capabilities

These responses suggest an investment posture focused on refining governance and controls while retaining the operational benefits of AI-assisted cybersecurity tools.

CBA / NPV / ROI

- Staffing efficiency and workload reduction were cited as key qualitative benefits
- Outreach participants noted the ability to remain lean or avoid adding additional cybersecurity personnel
- No quantitative financial metrics (e.g., cost savings, avoided headcount costs, ROI, or NPV) were provided or calculated

APPENDIX B: TECHNICAL SECURITY CONTROLS CHECKLIST

Category	Control Item / Requirement	Status (Y/N/NA)	Verification Method / Notes
Data Security & Privacy	**Encryption:** Is all data (video, logs, biometrics) protected with strong, modern Quantum-Resistant (or TLS 1.3+) encryption both at rest and in transit?	☐	
Data Security & Privacy	**Data Anonymization/Masking:** For training AI models, does the solution support using anonymized or synthetic data? Can the system mask sensitive PII in its operational outputs to protect privacy?	☐	
Data Security & Privacy	**Data Lineage and Provenance:** Can the system track the origin, transformations, and access history of data from source to decision?	☐	
Application & Model Security	**Secure SDLC:** Does the vendor follow and provide evidence of secure coding practices (e.g., OWASP Top 10) in the application's development?	☐	
Application & Model Security	**Model Integrity & Anti-Tampering:** How is the AI model protected from unauthorized modification or data poisoning? Are mechanisms like digital signatures or checksums used?	☐	
Application & Model Security	**Explainability and Interpretability (XAI):** Can the AI system provide an auditable reason for critical decisions (e.g., access denial, flagging)?	☐	
AI Bill of Materials (AI-BOM)	**AI-BOM:** Does the vendor provide a manifest of all base models, fine-tuning sets, and third-party AI libraries used?	☐	
Infrastructure & Operational Security	**Network Segmentation:** Will the AI system and its data repositories be deployed in a dedicated, isolated Zero-Trust network segment with strict firewall rules?	☐	
Infrastructure & Operational Security	**Principle of Least Privilege:** Are service accounts configured with the absolute minimum permissions required?	☐	
Infrastructure & Operational Security	**Robust and Correlated Logging:** Does the system generate detailed logs (including AI confidence scores) formatted for ingestion into central Security Information and Event Management?	☐	
Infrastructure & Operational Security	**Incident Response Playbooks:** Have specific incident response plans been developed and tested for AI system compromise or malfunction scenarios?	☐	
Human-in-the-Loop (HITL)	**HITL Override:** Is there a verified manual override (kill-switch) for security personnel if the AI produces "hallucinations" or system-wide errors?	☐	

APPENDIX C: FUNDING RESOURCES BY STATE

Category	Program	Focus	AI/Cybersecurity Relevance	URL / Search Strategy
Federal	Airport Improvement Program (AIP)	Infrastructure, Safety, Security	AI-enabled surveillance, access control	https://www.faa.gov/airports/aip/
Federal	Airport Infrastructure Grants – IIJA	Major infrastructure and security upgrades	Modernizing terminals with integrated AI and biometric systems	https://www.faa.gov/iija/airport-infrastructure
Federal	SMART Grants Program	Advanced Tech, Efficiency, Safety	AI for security and transportation	https://www.transportation.gov/grants/SMART
Federal	Homeland Security Grant Program (HSGP)	Preparedness, Protection	Cybersecurity measures for airports	Search: 'HSGP site:dhs.gov'
Federal	TSA AI Modernization Initiative	AI, Biometrics, Threat Detection	AI-driven screening, biometric ID, threat detection	Search: 'TSA AI Modernization Initiative'
Federal	Transit Security Grant Program (TSGP)	Critical Infrastructure Protection	AI-enabled surveillance and anomaly detection	Search: 'TSGP site:dhs.gov'
Federal	State & Local Cybersecurity Grant Program (SLCGP)	Cyber Risk Reduction	Cybersecurity resilience for airport IT systems	Search: 'SLCGP site:cisa.gov'
Federal	Targeted Violence & Terrorism Prevention (TVTP)	Threat Prevention, Intelligence Sharing	AI analytics for threat detection	Search: 'TVTP site:dhs.gov'
Law Enforcement	COPS Technology & Equipment Program (TEP)	Tech Acquisition, Interoperability	AI-based surveillance and analytics	Search: 'COPS TEP site:justice.gov'
Law Enforcement	Operation Stonegarden (OPSG)	Border & Aviation Security	AI surveillance and drones for border airports	Search: 'OPSG site:fema.gov'
Cybersecurity	CISA Financial Assistance Programs	Cybersecurity Risk Mitigation	Cybersecurity for aviation infrastructure	Search: 'CISA cybersecurity grants'
Cybersecurity	TSA Cybersecurity Requirements Compliance	Cyber Resilience for Airports	Projects may qualify for DHS funding	Search: 'TSA cybersecurity requirements'
State	California Airport Security Technology Grant	Security, Technology	AI-based surveillance and access control	Search: 'CALTRANS airport security grant'

Category	Program	Focus	AI/Cybersecurity Relevance	URL / Search Strategy
State	Florida State Public Transportation Grant Program	Infrastructure, Capital Improvements	AI/cybersecurity in screening and defense systems	Search: 'Florida Department of Transportation Aviation Grants'
State	North Carolina SCIF	Infrastructure	AI for operational efficiency and security	Search: 'North Carolina SCIF airport grants'
State	Texas TxDOT Aviation Grants	Improvement, Maintenance	AI for predictive maintenance and security	Search: 'Texas Department of Transportation Aviation Grants'
Federal	FAA State Block Grant Program	Infrastructure	State-managed airport improvement projects	https://www.faa.gov/airports/aip/state_block
State	Alabama Aviation Grants	Infrastructure	Potential AI integration	Search: 'Alabama Department of Transportation Aviation Grants'
State	Alaska Aviation Grants	Infrastructure	Potential AI integration	Search: 'Alaska Department of Transportation Aviation Grants'
State	Arizona Aeronautics Division Grants	Infrastructure	Potential AI integration	Search: 'Arizona Department of Transportation Aeronautics Division Grants'
State	Arkansas Aviation Grants	Infrastructure	Potential AI integration	Search: 'Arkansas Department of Transportation Aviation Grants'
State	Colorado Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Colorado Department of Transportation Aeronautics Grants'
State	Connecticut Aviation Grants	Infrastructure	Potential AI integration	Search: 'Connecticut Department of Transportation Aviation Grants'
State	Delaware Aviation Grants	Infrastructure	Potential AI integration	Search: 'Delaware Department of Transportation Aviation Grants'

Category	Program	Focus	AI/Cybersecurity Relevance	URL / Search Strategy
State	Hawaii Airports Division Grants	Infrastructure	Potential AI integration	Search: 'Hawaii Department of Transportation Airports Division Grants'
State	Idaho Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Idaho Transportation Department Aeronautics Grants'
State	Illinois Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Illinois Department of Transportation Aeronautics Grants'
State	Indiana Aviation Grants	Infrastructure	Potential AI integration	Search: 'Indiana Department of Transportation Aviation Grants'
State	Iowa Aviation Grants	Infrastructure	Potential AI integration	Search: 'Iowa Department of Transportation Aviation Grants'
State	Kansas Aviation Grants	Infrastructure	Potential AI integration	Search: 'Kansas Department of Transportation Aviation Grants'
State	Kentucky Airport Grants	Infrastructure	Potential AI integration	Search: 'Kentucky Transportation Cabinet Airport Grants'
State	Louisiana Aviation Grants	Infrastructure	Potential AI integration	Search: 'Louisiana Department of Transportation and Development Aviation Grants'
State	Maine Aviation Grants	Infrastructure	Potential AI integration	Search: 'Maine Department of Transportation Aviation Grants'
State	Maryland Aviation Grants	Infrastructure	Potential AI integration	Search: 'Maryland Department of Transportation Aviation Grants'
State	Massachusetts Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Massachusetts Department of

Category	Program	Focus	AI/Cybersecurity Relevance	URL / Search Strategy
				Transportation Aeronautics Grants'
State	Michigan Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Michigan Department of Transportation Aeronautics Grants'
State	Minnesota Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Minnesota Department of Transportation Aeronautics Grants'
State	Mississippi Aviation Grants	Infrastructure	Potential AI integration	Search: 'Mississippi Department of Transportation Aviation Grants'
State	Montana Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Montana Department of Transportation Aeronautics Grants'
State	Nebraska Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Nebraska Department of Transportation Aeronautics Grants'
State	Nevada Aviation Grants	Infrastructure	Potential AI integration	Search: 'Nevada Department of Transportation Aviation Grants'
State	New Hampshire Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'New Hampshire Department of Transportation Bureau of Aeronautics Grants'
State	New Jersey Aviation Grants	Infrastructure	Potential AI integration	Search: 'New Jersey Department of Transportation Aviation Grants'
State	New Mexico Aviation Grants	Infrastructure	Potential AI integration	Search: 'New Mexico Department of Transportation Aviation Grants'
State	New York Aviation Grants	Infrastructure	Potential AI integration	Search: 'New York State Department of Transportation Aviation Grants'

Category	Program	Focus	AI/Cybersecurity Relevance	URL / Search Strategy
State	North Dakota Aeronautics Commission Grants	Infrastructure	Potential AI integration	Search: 'North Dakota Aeronautics Commission Grants'
State	Ohio Aviation Grants	Infrastructure	Potential AI integration	Search: 'Ohio Department of Transportation Aviation Grants'
State	Oklahoma Aeronautics Commission Grants	Infrastructure	Potential AI integration	Search: 'Oklahoma Aeronautics Commission Grants'
State	Oregon Aviation Grants	Infrastructure	Potential AI integration	Search: 'Oregon Department of Transportation Aviation Grants'
State	Pennsylvania Aviation Grants	Infrastructure	Potential AI integration	Search: 'Pennsylvania Department of Transportation Aviation Grants'
State	Rhode Island Airport Corporation Grants	Infrastructure	Potential AI integration	Search: 'Rhode Island Airport Corporation Grants'
State	South Carolina Aeronautics Commission Grants	Infrastructure	Potential AI integration	Search: 'South Carolina Aeronautics Commission Grants'
State	South Dakota Aeronautics Commission Grants	Infrastructure	Potential AI integration	Search: 'South Dakota Aeronautics Commission Grants'
State	Tennessee Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Tennessee Department of Transportation Aeronautics Grants'
State	Utah Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Utah Department of Transportation Aeronautics Grants'
State	Vermont Aviation Grants	Infrastructure	Potential AI integration	Search: 'Vermont Agency of Transportation Aviation Grants'
State	Virginia Aviation Grants	Infrastructure	Potential AI integration	Search: 'Virginia Department of Aviation Grants'

Category	Program	Focus	AI/Cybersecurity Relevance	URL / Search Strategy
State	Washington Aviation Grants	Infrastructure	Potential AI integration	Search: 'Washington State Department of Transportation Aviation Grants'
State	West Virginia Aviation Grants	Infrastructure	Potential AI integration	Search: 'West Virginia Department of Transportation Aviation Grants'
State	Wisconsin Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Wisconsin Department of Transportation Aeronautics Grants'
State	Wyoming Aeronautics Grants	Infrastructure	Potential AI integration	Search: 'Wyoming Department of Transportation Aeronautics Grants'