International Civil Aviation Organization
North American, Central American and Caribbean Office

WORKING PAPER

NACC/DCA/14 — WP/20
20/05/26

Fourteenth Meeting of the North American, Central American and Caribbean Directors of Civil Aviation (NACC/DCA/14)

St. George's, Antigua and Barbuda, 1 to 5 June 2026

Agenda Item 5: Every Flight is Secure

U.S. TRANSPORTATION SECURITY ADMINISTRATION USE CASES FOR ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING APPLICATIONS

(Presented by United States)

EXECUTIVE SUMMARY

This Working Paper reviews the U.S. Transportation Security Administration (TSA) use cases for artificial intelligence (AI)/machine learning (ML) applications to support aviation security screening, including the use of synthetic imaging to train AI/ML detection algorithms and to augment certification testing.

Action:	a) Encourage NACC Member States to engage their TSA representatives with any questions or concerns related to TSA's synthetic imaging initiative; b) Consider endorsing and adopting a similar aviation security approach to the use of synthetic data to support AI/ML-based threat detection, in line with appropriate national and regional frameworks; and c) Contribute to ongoing efforts within ICAO to address evolving threats, especially within the Aviation Security Panel of Experts and the Cybersecurity Panel as well as its working groups.
Strategic Objectives:	• Every Flight is Safe and Secure
References:	• Annex 17 – Aviation Security

1. Introduction

1.1 This paper provides an overview of U.S. Federal policy and accountability frameworks for the use of artificial intelligence (AI), outlines the U.S. Transportation Security Administration's (TSA) current and planned use of AI and ML in aviation security operations, and describes TSA's efforts to use physics-based synthetic imaging to support algorithm development, testing, and evaluation.

2. Background

2.1 U.S. Government agencies' use of AI is guided by national laws, Presidential executive orders, and relevant policies. Since 2019, several executive orders have been issued and laws have been enacted to promote AI research, encourage trustworthy AI, and set principles for how AI should be used by/in government.[1] These rules require government agencies to be transparent and accountable, and to manage risks when developing and using AI systems. Agencies must also protect privacy and civil rights and monitor how AI systems perform over time. A key part of this process is ensuring the data used for AI are high quality, reliable, properly documented, unbiased, secure and are appropriate for both developing and operating AI systems.

2.2 Organizations using AI should set clear goals and assign specific roles and responsibilities to their teams. They need to promote values and establish principles that build trust and train their staff to be skilled in AI. It is important to include people with different backgrounds and viewpoints to help identify and mitigate risks. Organizations should also have a risk management plan that is tailored for AI. At the system level, they must create technical requirements to make sure the AI works as intended and follows all applicable laws and rules, as well as ensure an oversight mechanism is in place. They should also share information about their AI systems with outside groups to keep things transparent.

2.3 Organizations should regularly evaluate how their AI systems are performing and maintain records of issues identified and corrective actions taken. They need to evaluate and measure whether the AI continues to meet their goals over time. It is important to periodically assess whether the AI system remains effective and fit-for-purpose, and to decide whether to expand its scope, adjust its scale, or discontinue use.

2.4 Organizations should keep track of all the parts that make up their AI system and measure how each part performs. They also need to evaluate the AI system as a whole, document their testing methods, watch for bias, and make sure humans can oversee the system. Using synthetic data and simulations can help organizations test AI performance in rare, unusual, or high-risk scenarios and provide consistent data for validation and ongoing performance monitoring.

2.5 The AI trend is growing quickly at the U.S. Department of Homeland Security (DHS), with current and future uses planned. Within DHS, TSA is using AI/ML to improve security while protecting privacy and civil rights, working closely with other government agencies to make sure these values are central to their efforts. TSA is exploring ways to use AI responsibly to boost security and make travel smoother, while keeping data safe. TSA's aim for AI is to improve the agency's security and business operations, help its workforce, and provide a better experience for travelers. For example, using AI to automatically detect prohibited items in carry-on bags and develop advanced imaging systems. Synthetic data is also being used to help train and test these AI systems.

---

[1] Examples of U.S. Executive Orders and laws issued: In February 2019, Executive Order 13859 established the American AI Initiative, which promoted AI research and development investment and coordination amongst other things (https://www.govinfo.gov/content/pkg/DCPD-201900073/pdf/DCPD-201900073.pdf). In December 2020, Executive Order 13960 promoted the use of trustworthy AI, which focused on operational AI and established a common set of principles for the design, development, acquisition, and use of AI in the federal government (https://www.govinfo.gov/content/pkg/DCPD-202000870/pdf/DCPD-202000870.pdf). In December 2020, the AI in Government Act of 2020 was enacted as part of the Consolidated Appropriations Act, 2021 (https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf). In October 2023, Executive Order 14110 advanced a coordinated, federal government-wide approach to the development and safe and responsible use of AI (https://www.govinfo.gov/content/pkg/DCPD-202300949/pdf/DCPD-202300949.pdf).

3. Discussion

TSA's use of Synthetic Data to support AI/ML efforts

3.1 Synthetic data is increasingly vital for training AI models in aviation security, enabling industry to simulate rare or risky scenarios without relying on extensive real threat data. This approach supports advanced screening and training, improves detection accuracy, and reduces false alarms. There are less labeled threat data, therefore, using synthetic data can help fill gaps and improve detection in underrepresented scenarios.

Synthetic Imaging Solutions

3.2 TSA is exploring alternative approaches to create synthetic images for training and testing screening solutions. They are using platforms that generate artificial data for perception systems and tools that add to real-world images and videos. Some methods create pre-labeled data for supervised learning, while others focus on making synthetic images for stream of commerce baggage. For example, TSA is piloting a system that uses synthetic images of baggage containing various test objects to train AI algorithms. These synthetic images help improve detection accuracy by exposing the algorithms to a wider range of scenarios than would be possible with real-world data alone. By combining these techniques, TSA aims to make synthetic datasets that look real, match actual operations, and can be changed to test for overall performance, consistency, and bias.

Testing AI/ML Solutions

3.3 The U.S. Transportation Security Laboratory is assisting TSA and DHS to validate that ML detection algorithms work correctly and can be trusted when used in real situations. TSA and DHS are developing a strategy to test AI systems by checking if the algorithms focus on actual threats and not irrelevant details. They also confirm the training data covers a wide range of scenarios, materials, and passenger types to avoid bias. Testing for bias ensures the AI works fairly for everyone and does not only perform well for certain groups or situations. To make testing more thorough, they use synthetic and augmented data to simulate diverse threats and conditions, enabling faster, safer, and more controlled testing—especially with physics-based synthetic data that allows precise and repeatable experiments.

Integrating AI/ML

3.4 TSA is investing in comprehensive training programs to upskill current employees in AI operations, data analysis, and system troubleshooting. Through clear communication, hands-on training, and dedicated support resources, TSA helps staff adapt to new technologies and capabilities. While AI can automate routine tasks and streamline operations, human expertise remains essential for complex decision-making and managing exceptions.

AI/ML for Operational Efficiency and Passenger Flow

3.5 TSA leverages AI/ML to analyze passenger volumes and optimize staffing and lane openings in real time, improving both security and efficiency. Automation of screening processes allows officers to focus on higher-risk cases, while AI-driven tools support operational decisions. While AI automates routine tasks, human expertise remains essential for complex decision-making and handling exceptions, ensuring personnel are equipped to oversee and intervene when needed.

3.6 For example, the Automated Passenger Screening Gate System uses AI to guide passengers through queues and initiate screening when they are optimally positioned, managing flow and reducing human interaction. Additionally, the Answer Engine, an AI-powered chatbot, helps frontline personnel quickly access standard operating procedures (SOPs), regulations, and policy information from mobile devices, streamlining decision-making and ensuring consistent, authoritative guidance.

Threat Detection Using AI/ML

3.7 TSA is leveraging AI/ML to enhance checkpoint capabilities and algorithm development, using an open architecture framework to enable data-driven decision making. Key use cases include emerging screening technologies, threat and vulnerability analysis, rapid information sharing, workforce efficiency, and ongoing innovation. TSA is piloting self-service screening and AI-powered kiosks to streamline the process and maintains attentive customer service for complex issues, balancing technology with personal assistance.

3.8 With respect to security and threat detection, AI-trained algorithms can identify prohibited items and suspicious behavior in real time, including through video analytics. For example, the Automated Prohibited Item Detection algorithm, which uses deep learning to automate detection of prohibited items in carry-on property. By working with equipment manufacturers and third-party developers, TSA is expanding detection capabilities and minimizing false alarms, allowing officers to focus on alarmed bags and improving overall security and efficiency.

Challenges with AI/ML

3.9 TSA prioritizes data quality and bias mitigation by training screening personnel to ensure technology outputs are accurate and representative, avoiding bias in threat detection and passenger screening. While AI automates many processes, TSA maintains human oversight for complex or ambiguous situations, ensuring personnel use AI tools to support—not replace—their expertise. This balance provides a safe, trusted customer experience.

3.10 TSA is committed to continuous improvement through ongoing testing, validation, and collaboration with industry and government partners to keep AI solutions secure, effective, and trusted. For example, TSA is developing AI-enhanced millimeter wave detectors (also known as body scanners) as alternatives to traditional Walk-Through Metal Detectors, improving detection of both metallic and non-metallic threats while enhancing the passenger experience. Additionally, Accessible Property Screening uses AI with computed tomography X-ray scanners to identify non-explosive threats and prohibited items in carry-on baggage, delivering consistent and uninterrupted threat detection as an added layer of security.

4. Conclusion

4.1 TSA is committed to the responsible integration of AI/ML into aviation ecosystem operations, using synthetic data to augment testing/evaluation efforts, while preserving human oversight essential to enhance security and regional resilience.

— END —