

# BORDER MANAGEMENT TODAY

Issue 014 | FEBRUARY 2026

## MIDDLE EAST SUMMIT 2025 BAHRAIN REPORT

### SCAN APP:

DIGITISING FREIGHT CLEARANCE AT THE UK BORDER

### BORDER TECHNOLOGY:

NO SILVER BULLETS

### FUTURE BORDERS:

OFFICERS OR TECHNOLOGY?

### AMERICAS SUMMIT 2026

MEXICO HERE WE COME



JOIN THE GROWING IBMATA FAMILY: [WWW.IBMATA.ORG/JOIN-IBMATA](http://WWW.IBMATA.ORG/JOIN-IBMATA)

**PUBLISHER****IBMATA**

International Border  
Management and Technologies  
Association Ltd

E: [info@ibmata.org](mailto:info@ibmata.org)

W: [www.ibmata.org](http://www.ibmata.org)

[linkedin.com/company/ibmata/](https://www.linkedin.com/company/ibmata/)

[twitter.com/border\\_mgmt](https://twitter.com/border_mgmt)

**EDITORIAL &  
ADVERTISING**

Enquiries to:

Sharon Ayley

E: [info@ibmata.org](mailto:info@ibmata.org)

**DESIGN**

LimeChilli Design

**COPYRIGHT**

All material appearing in Border Management Today is copyright unless otherwise stated or it may rest with the provider of the supplied material. Border Management Today takes all care to ensure information is correct at time of publishing, but the publisher accepts no responsibility or liability for the accuracy of any information contained in the text or advertisements. Views expressed are not necessarily endorsed by the publisher or editor.

# Contents...

- 4** IBMATA Middle East Summit 2025 – Bahrain
- 10** CBP and PHL Airport launch Enhanced Passenger Processing for U.S. travelers returning from overseas
- 12** Digitising the front line: How ScanApp is delivering a frictionless UK border
- 15** Dominican Republic Launches New E-Passport
- 18** From space to AI: Minimising risk at Britain's border
- 20** Border Management, Security and Technology: Strengthening Fiji's Borders in a Rapidly Changing World
- 22** Leveraging Visual Behavioural Analytics to Secure Borders and Protect Public Spaces
- 26** Eyes on the Coast – How Maritime Loopholes Must Be Closed
- 29** Unlocking the economic power of borders through digital identity
- 33** No silver bullets: secure borders demand successful integration of multiple technologies
- 36** Future Borders: Officers or Technology



## Message from the Chairman

**W**elcome to our 14th edition of “Border Management Today” – the online magazine written by border experts for border experts.

In this edition we take a look back to our recent Middle East Summit, kindly hosted by the Ministry of the Interior in Bahrain in November 2025. I am grateful to Lt General (Retired) Stuart Skeates CB CBE for stepping up to chair this event in my absence, and for his comprehensive report. Which appears in this edition.

The event was very well attended by government representatives from across the region, as well as from further afield including the UK and the USA. Like many countries in the region, Bahrain is forging ahead with new technologies to build the next generation of border controls. Our members were treated to a “behind the scenes” visit to the King Fahd Causeway linking Bahrain to Saudi Arabia, where technology is assisting vehicle flows across the second busiest vehicle crossing point in the world.

In this edition we also have reports of how digital technology is being deployed at borders in the UK, Fiji, and the Dominican Republic – demonstrating that IBMATA continues to search the world for new innovation. In particular it was heartening to see the roll out of e passports in the Dominican Republic, which shows us that the number of countries without e passport technology continues to decrease around the world – thus facilitating the increased roll out of biometric visas, electronic travel authorities, and automated border controls globally.

Kevin Foster – a former immigration minister at the UK Home Office and good friend to IBMATA – reminds us that the threat to border security is not confined to passengers. The maritime threat is real – and if left unchecked could cause significant damage to national security by relying upon outdated processes for controlling the entry of seafarers.

Having spent over half a century working in this industry I have added an epilogue about the ongoing battle between organised crime and law enforcement, reviewing the perennial question as to whether technology can ever be a real substitute for officer presence at the border. Is there really a technological substitute for human intuition?

As we enter 2026, we look forward to continuing our global borders journey, with upcoming events in Mexico City (10 – 12 March) and Lisbon, Portugal (22 – 24 June). Thank you all for your continued support to IBMATA’s mission – and I hope to see many of you there.

**Tony Smith CBE,**

CHAIRPERSON *at* INTERNATIONAL BORDER  
MANAGEMENT AND TECHNOLOGIES ASSOCIATION



By Lieutenant General (Retired)  
Stuart Skeates CB CBE

# IBMATA Middle East Summit 2025 – Bahrain

**F**or our first conference in the GCC Region since 2023, we chose the Kingdom of Bahrain who were highly engaged and enthusiastic hosts. It gave us an excellent opportunity to visit the King Fahd Causeway, the road link between the Eastern District of Saudi Arabia and Bahrain. This vital land border has become the second busiest vehicle crossing point in the World, with 33M vehicles using it in 2024 taking an average of 20 mins to pass including customs and immigration clearance, which is remarkable considering that it was originally designed for only 1800 vehicles per day.

The event was opened by the minister himself, His Excellency Lieutenant General Sheikh Rasid Bin Mohammed Al-Khalifa. He set the theme for the conference, emphasising the new threats to border security particularly cyber,





disinformation and AI which were also vectors that could undermine societies, national security and the economy. The need for new legislation and the development of new partnerships with joint operational procedures was clear.

### **FACILITATION AT THE BORDER**

In the first session of day one we heard imaginative and thoughtful interventions by the Vice President for External Affairs from the Naif Arab University for Security Sciences, HE Dr Khaled Al-Harfash, who commended Bahrain for the forward leaning posture that they have taken within the region and

how they have set the pace for the facilitation of rapid transit across borders. Ihma Shareef from the IOM gave a really thoughtful intervention where she also singled out Bahrain for the Kingdom's excellent example in facilitating border movement, its regional lead role on migration legislation and their measures against human trafficking.

We were privileged to have the President of Interpol, Major General Dr Ahmed Naser al-Raisi who focused on a more modern approach towards tackling Serious and Organised Crime (SOC). He saw technology, particularly AI, playing a key role in the assembly and analysis of databases of threats. He

encouraged Interpol member nations to increase and strengthen their efforts to share intelligence as those threats became more complex and SOC adapts to exploit new technology and expose new weaknesses within borders. This is not something which countries can do alone but must be done in partnership, a sentiment we all support.

HE Sheikh Hisham bin Abdulrahman al Khalifa the Under Secretary for KoB MOI Nationality, Passports and Residence Affairs (NPRA) gave an overview of the many reforms and innovations that the Kingdom was taking to strengthen security and facilitation through improvements



to documentation and identity. The majority of Immigration Services were digital reducing the need for in person visits for travel documentation and visas. The collaboration between the MOI and industry to develop the NPRA app was highly effective and had taken much of the routine process for immigration and travel on-line. His ambition was to digitise the whole travel experience.

Myriam Pellerin, Senior Business Development Manager SITA focused on the importance of data for balancing security and facilitation. In a wide-ranging and fascinating presentation, she highlighted the critical requirements for building a digital travel and borders experience. She emphasised the essential need for high quality data that was flexible enough for many uses, particularly its translation into intelligence for law enforcement. In that respect, there were high value-added tasks for data, particularly intelligence-led policing and targeting which would inform a proactive policy and posture for border officials.

Throughout this section we heard first-hand accounts



from Lebanon and Jordan who face some of the most complex and difficult border challenges in the Region. Fascinating insights and the need for close multi agency



cooperation particularly between law enforcement, military forces, UN agencies and NGOs came across strongly. So too did the need for thorough risk assessments to identify the most serious threats to their domestic populations, and how border operations could mitigate them through targeted policies and operations. The need for integrated border management was absolute, starting at the source of the threat, whether people or weapons and drugs. Serious stuff.

By serendipity, we had a political scientist at hand. Dr Hesham al Ghanam, Director of the Security Research Centre and the Head of the National Security Department at

NAUSS expanded on these themes, discussing other challenging threats the Region faced, particularly non-state actors (proscribed terrorist groups such as Hezbollah in the Lebanon and the Al-Houthi in Yemen) who had become de facto state representatives. In such cases, border management must develop hard security solutions to counter the threats posed.

The first panel session allowed us to look in more detail at the King Fahd Causeway between Saudi Arabia and Bahrain. As a border crossing, the Causeway has been a global success story, and in 2024 was the second busiest crossing point in the world for vehicle

traffic. Opened in 1986 its current capacity and flow rate far exceeded its original design parameters. Over the course of the past 10 years, the deployment of technology, infrastructure improvements, staff enhancements and training and the closer cooperation between the two governments had been key features of its success. The commitment to excellence and continuous improvement of the passenger experience came across very strongly from the panel members, HE Sheikh Ahmed bin Hamad al Khalifa the President of Customs and Mr Rami bin Khalid al-Turki, a Saudi Arabian businessman and a member of the King Fahd Causeway

Authority Board. The panel was an excellent way to showcase the balance between border facilitation, security and customs enforcement. The laser-like focus of the Board, the Authority and the MOI on improving the traveller experience, had become the culture of the Authority but public safety enhanced by AI was not being compromised. They explained that their ambition for the Causeway was to increase its capacity further, particularly the capacity of goods and to explore further integration between the Kingdoms of Saudi Arabia and Bahraini customs.

### **CUSTOMS ENFORCEMENT**

The second section on customs enforcement opened with a video message from the Secretary General of the World Customs Organisation, Ian Saunders. Very helpfully, he emphasised the need for standardisation of high-quality data to deliver the right speed of custom services and encouraged delegates to help achieve this goal. The other side of that coin is cyber security and the risk of over-reliance on AI without firstly understanding the capability. These issues were picked up by Shaikha Munera, the Director General of Clearance and Customs Services who majored on how Bahrain was embracing technology to produce a seamless customs experience within the context of the KoB Economic Vision 2013.

The Director General of Omani Customs, Brigadier Dr Syed bin Hamas al-Egati picked up similar themes in a short history of the Omani Customs Department to its modern, innovative form. Their most recent innovation, the Customs Targeting Centre, used a bespoke data system to assess shipment risk which had drastically reduced clearance times, in some case down to an hour. His closing point, that this success was enabled by a

strong partnership with industry was developed further by S2 Global where Mr Tom Bommell and Novel Daniyela described how AI, when applied intelligently, can drive down clearance times and identify risks. If anyone thought customs officials will be out of a job in the future, he dispelled those thoughts, emphasising the continued importance of the human expert in the loop to make the decisions.

And bravo to Michael Barrie, CEO of e-BIM Solutions, for nailing the point home by talking about why we would want to use AI rather than just how. His most telling point was to encourage customers to consider whether AI would be a good investment to solve their customs problem in the first place and that if it was, to collaborate with the appropriate agencies and industry partners from the outset.

Very fittingly, the last regional speaker of the day was Doctor Salman bin Masud al Ghafari, the President of the GCC Customs Organisation who brought all these points together in mapping out his vision for the future of a GCC trading region. Progress so far has been significant and the potential for improving customs clearances could be economically game-changing. Finally, Alioune Cisse from Web Fontaine left us with much to ponder during the evening's entertainment. His cautionary words on the challenges to AI adoption were key conference take-aways: information data quality or gaps; integration with legacy systems; trust in AI recommendations; the need for skilled personnel; and AI transparency and explanatory concerns.

So, there was a great deal to reflect at SITA's Arabian Nights hosted event where we were royally entertained by the Royal Bahraini Police Band and some exceptional Bahraini

Kawha and eats.

### **THE SEAMLESS BORDER EXPERIENCE**

We were therefore in great shape for Day Two which started with the Deputy Chief of Public Security of the KoB Major General Sheikh bin Hamid Mohammed al Khalifa who reflected on the changing nature of travel and border threats over the past generation. He explained Bahrain's security strategy and the lines of operation which have successfully led to the integration of border policing with internal policing and a reduction of 30% in crime over the past five years.

The next panel, chaired expertly by Chris Rous of Amadeus, set us up brilliantly for the rest of the day. Patrick Cuschieri (Vice-President Aviation Security at Bahrain Airport Company), Major General (Retired) Sameh Mohammed Fawzy Elsayed Hegab (Vice-President Egyptian Aviation Authority) and Joe Burley (Border Force Relationship Manager at Heathrow Airport) gave some fascinating national comparisons, not least the impact on their daily lives of respective national legislative and regulatory regimes. Although this made for significantly different ways of making improvements to the passenger experience, there was unanimous agreement that demonstrating the value of technology required early and consistent engagement with airport authorities so that they understood the need to implement and test it in place.

We then received an outstanding visualisation from Makram Al Banna from Idemia Public Security of what an end-to-end transformed border model might look. The 'Border Ecosystem' took the desired border capability into a concept of operations through to its integration and interface with national

authorities and, finally, to the coordination and corporation at an international level. As a summary of our discussions over the Conference how a modernised, digitised and technology-enabled border management system might look like, it was hard to better...

...Until Phil Douglas, Director General UK Border Force took the floor to cover how he was introducing such a system at UK Airports. The successful trial for biometrically enabled and seamless borders at Manchester Airport had allowed UK and Republic of Ireland citizens to be able to travel through borders without documentation, so plans for expand to other nationalities and airports were already underway. The introduction of ETA for travel to the UK from February 2026 was part of an overall initiative to maximise pre-clearance checks and advanced travelling data as possible. His proposal to make more use of scanning and AI to create of a global image database to improve clearance of goods really hit the mark.

The final panel, which was expertly chaired by Ahmed Kayali from SITA, allowed a more in-depth discussion about the challenges that Serious and Organised Crime (SOC) represented for seamless passenger travel. We could not have done better with our two panelists, Colonel Ahmed Saad Al-Runaihi (Director General Anti-Corruption, Economic and Electronic Security at the Bahraini MOI) and Motaz

Al-Rababah from UNOCT. Regional collaboration across the GCC was strong and turning information into intelligence to allow the more accurate targeting of criminals reassured governments that border management was robust. Although not a panacea, governments needed to understand the benefits of technology in law enforcement although the increased use of AI required greater attention to human rights and data protection regulations.

So, a highly successful return to the GCC for the IBMATA Conference which could not have been hosted better by the Bahrain MOI and had better speakers. Striking a balance between seamless facilitation and security would still be a significant challenge even with the enabling technology that we discussed and was exhibited. There was a commendably pragmatic approach to how AI might help, and it was heartening to hear all industry speakers encouraging potential users to start with the business need not the technology, to get their data in order, to think in systems terms not about the technology, and to prototype fast and measure performance relentlessly. Most importantly, it was about learning from the problems and frictions that need to be overcome. And the Conference was a great step along that path.

The day after the Conference, we were generously hosted at the King Fahd Causeway by the CEO. Superbly

hosted, we were treated to a bird-eye view of a slick and professional road border operation. We experienced at first hand the ability to regulate flow in peak hours and the way in which technology was being used to meet the varying demands of customs clearance, border security and a quite exceptional passenger experience.

---

Lieutenant General (Retired) Stuart Skeates CB CBE

Stuart Skeates served in the Army for 34 years, retiring as a lieutenant general, before becoming a Senior Civil Servant in the Home Office.

Educated at the Judd School Tonbridge, King's College London, and the Royal Military Academy Sandhurst, he was commissioned into the Royal Regiment of Artillery in 1988. During his career, he served in the United Kingdom, Germany, Saudi Arabia, Kuwait, Northern Ireland, the Balkans, Cyprus, Afghanistan, and Iraq.

He has extensive leadership experience on military operations and spent the latter 20 years of his career in joint operations, with coalitions, with the US Marine Corps and with NATO. He was also Commandant of the Royal Military Academy Sandhurst.

He holds degrees from Kings College London, the Cranfield University Management School, he completed the advanced and Higher Command and Staff Course, the NATO Pinnacle Course and the Major Projects Leadership Academy.

After leaving the Army, he worked on small boats and illegal migration initially in the Cabinet and subsequently in the Home Office. He is now a defence and security consultant.

---

# CBP and PHL Airport launch Enhanced Passenger Processing for U.S. travelers returning from overseas

U.S. Customs and Border Protection and Philadelphia International Airport announced today the launch of Enhanced Passenger Processing technology at Philadelphia International Airport.

[Enhanced Passenger Processing](#) utilizes advanced facial comparison technology and biometric software to provide U.S. citizens with a touchless, seamless, and secure international arrivals experience. U.S. citizens experience the same high level of security assurance with fewer steps and reduced processing times.

CBP and Philadelphia International Airport announced the January 2026 launch of Enhanced Passenger Processing. EPP provides U.S. citizens with a touchless, seamless, and secure international arrivals experience.

The technology allows CBP officers to focus on traveler interaction and higher-risk travelers while automating routine processing for eligible U.S. citizens with no enforcement concerns.

EPP is available at 15 U.S. airports, six CBP Preclearance airports in



Aruba, Canada, and Ireland, five seaport ports of entry, and one land border crossing. Since launching EPP nationally in August 2025, CBP officials have observed a 25% reduction in wait times for U.S. citizens.

When a U.S. citizen arrives at the inspection area, auto-capture cameras operated by CBP officers capture their photo using biometric facial comparison technology. Within

seconds, the system compares the live image to photos already in CBP's holdings, such as a passport photo, verifies the traveler's identity and citizenship status, runs law enforcement vetting, and creates a crossing record.

While the process is rapid and touchless, CBP officers are still on hand to instruct passengers on the process and assist them during screening.

## ENHANCED PASSENGER PROCESSING FOR U.S. TRAVELERS RETURNING FROM OVERSEAS

Any passenger wishing to not participate in the EPP process will need to notify an officer and they will then go through the standard international arrivals process.

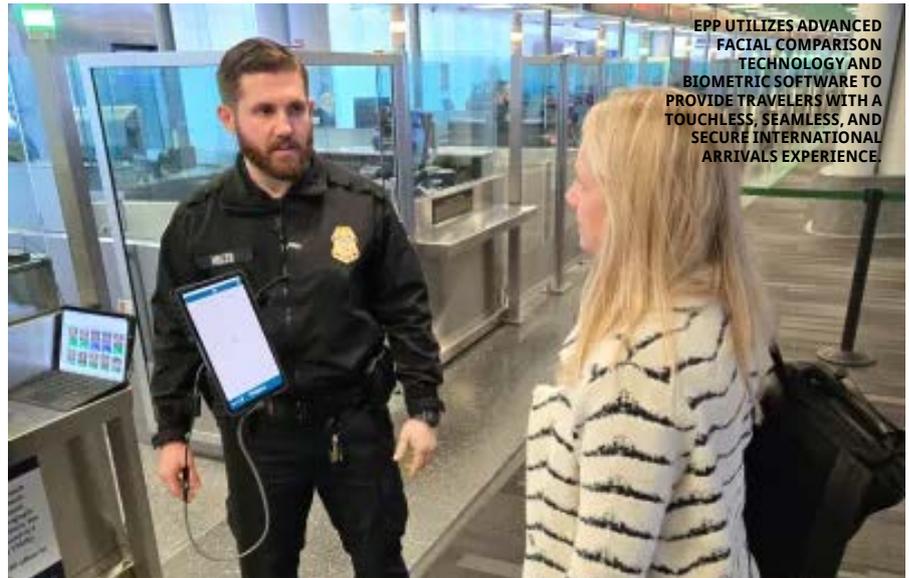
“EPP is an innovative, secure, biometric solution designed to streamline the international arrivals experience for U.S. citizens while enhancing Customs and Border Protection’s national security mission and enforcement capabilities,” said Cleatus P. Hunt, Jr., CBP’s Area Port Director for the Area Port of Philadelphia. “PHL Airport is a major transatlantic hub. Travelers arriving at PHL Airport will feel the benefits of this new technology in shorter wait times, faster processing through CBP arrivals inspection, and the improved ability to make their connecting flights.”

CBP and Philadelphia International Airport announced the January 2026 launch of Enhanced Passenger Processing. EPP provides U.S. citizens with a touchless, seamless, and secure international arrivals experience.

PHL’s IT Department worked with CBP to implement EPP. The airport has a number of Wi-Fi and networking infrastructure upgrades underway to support new technology such as the EPP.

“PHL is proud to be one of the airports selected to offer EPP for the millions of US citizens that arrive on international flights. As a major transatlantic hub, being able to quickly process through customs and head home or to a connecting flight is one of the best guest experiences we can offer travelers. Thank you to CBP for training our Customer Care Team on the new process so that we can support passengers who have questions and continue to provide exceptional service to our guests.”

In fiscal year 2024, CBP processed over 420 million travelers at ports of entry — a 6.6% increase from the previous year. CBP continues to roll out airport modernization



enhancements to support the expected increase in international travel. Enhanced technology ensures better allocation of resources, allowing officers to focus on higher-risk travelers, which aligns with CBP’s national security mission.

CBP also provides a suite of mobile applications to help travelers streamline their entry into the U.S. All CBP mobile apps are free and available through the Google Play Store and Apple App Store, or by visiting the [CBP Mobile Apps Directory](#).

- CBP’s Global Entry mobile app, available to use at [78 locations](#), allows pre-approved members to complete their entry processing on their phones before leaving the aircraft.
- CBP’s Mobile Passport Control app, available to use at [53 ports of entry](#), including 14 Preclearance locations and four seaports, is a free, fast, and secure way to submit their passport and travel information before arriving at a CBP inspection station. The app is available to U.S. citizens, lawful permanent residents, certain Canadian citizens, and Visa Waiver Program travelers.
- CBP’s Electronic System for Travel Authorization (ESTA Mobile) app enables travelers potentially eligible to enter the United States

under the Visa Waiver Program to [submit ESTA applications](#) online or in app easily and quickly from their smartphones, mobile devices or tablets.

Travelers are still required to meet legal requirements and have proper documents for entry, are subject to inspection, and must adhere to visa terms or risk detention and removal. A visa is a privilege, not a right, and only those who respect our laws and follow the proper procedures will be welcomed.

For more information on visas and passports, please visit [travel.state.gov](#). Travelers may also visit the [Know Before You Go](#) page.

Follow the Director of CBP’s Baltimore Field Office on [X @ DFOBaltimore](#) for breaking news, current events, human interest stories and photos, and CBP’s Office of Field Operations on [Instagram @ cbpfieldops](#).

---

U.S. Customs and Border Protection (CBP) is America’s frontline: the nation’s largest law enforcement organization and the world’s first unified border management agency. The 67,000+ men and women of CBP protect America on the ground, in the air, and on the seas. We enforce safe, lawful travel and trade and ensure our country’s economic prosperity. We enhance the nation’s security through innovation, intelligence, collaboration, and trust.

---



By Darren Hart MBE  
Programme Director,  
SCAN AI and MEP Programme,  
Border Strategy and Transformation Directorate,  
Border Force

# Digitising the front line: How ScanApp is delivering a frictionless UK border

**W**ith cargo volumes increasing through borders and global threats becoming more complex and dangerous, the use of technology to make goods flow quicker, easier and safer is more important than ever before.

For those of us responsible for customs and border operations, the goal is not just to stop threats but to keep trade moving efficiently.

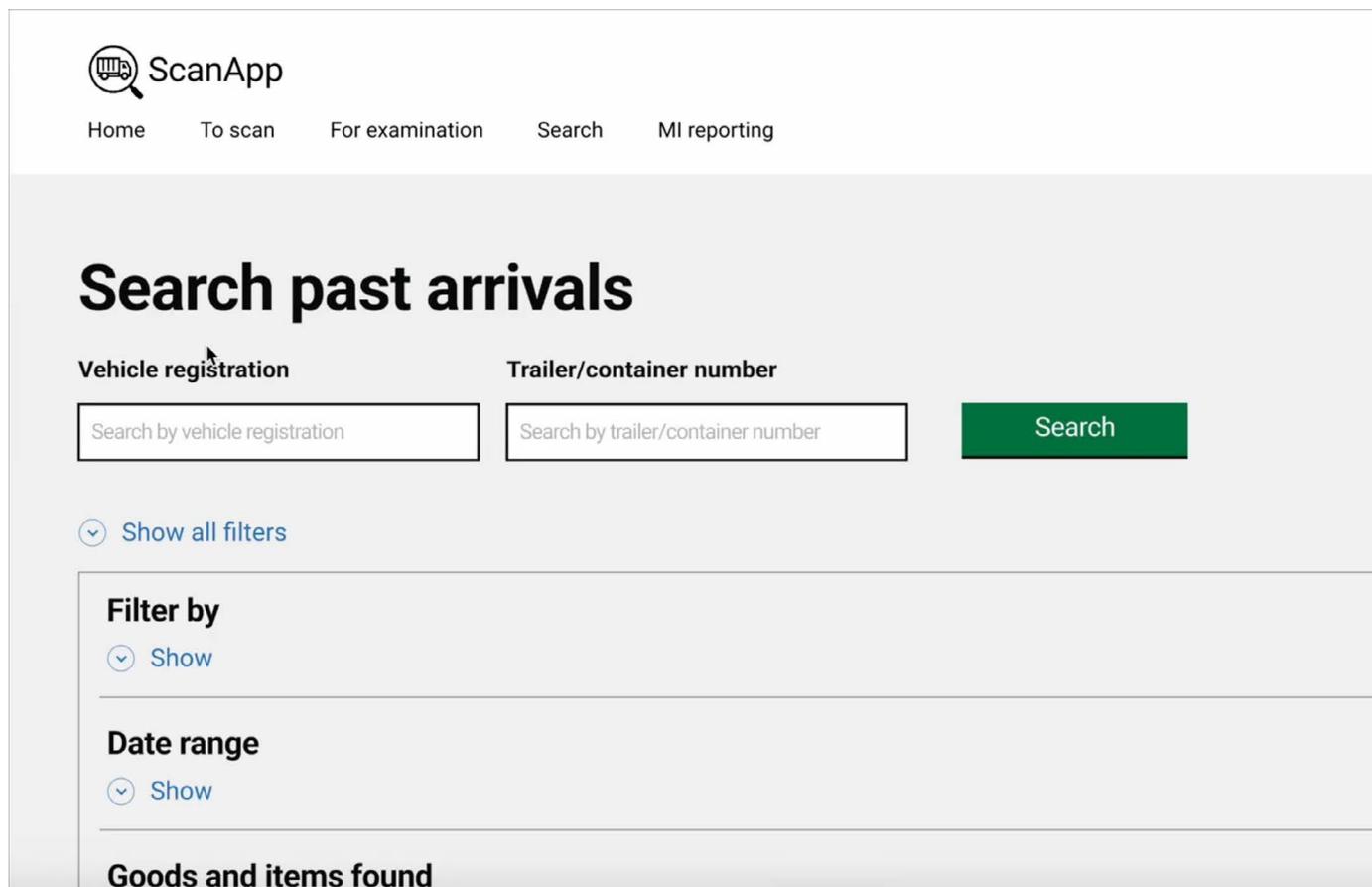
Higher volumes of goods crossing borders place pressure on public resources, making it essential to find ways to do more with less. After all, an inefficient border is an expensive border.

Add to that the increasingly uncertain world, where criminal and terrorist threats are rising, and the challenge becomes even greater.

At Border Force, we've been focusing on how to tackle this challenge; how to keep goods moving quickly while maintaining robust security.

Simple technology and reimagining how we operate can make a real difference in managing growing volumes, reducing friction, and strengthening security.





## HERE'S WHAT WE DID WITH SCANAPP

Border Force teamed up with Zaizi and Symetrica to build a solution that [digitised and automated freight scanning](#) to reduce friction at the UK border.

ScanApp replaced manual, paper-based work to help officers process freight quicker and improve the detection of illicit goods.

It serves as a “single point of truth” for officers, simplifying how scan images and freight data are viewed, analysed and shared.

Key operational benefits include:

- Increased efficiency: Eliminates manual data entry and double handling, freeing officers to focus on high-value operational duties.
- Faster processing: Automates scanning and examination processes with a comprehensive audit trail
- Real-time collaboration: Enables remote access to real-time scan

data, shareable across ports

- Better security: Implements secure, role-based identity and access management, ensuring Border Force has full ownership and control of critical data.
- Data-driven insights: Allows senior stakeholders to monitor throughput and efficiency, and use the data for wider reporting

## DESIGNING AROUND THE FRONTLINE

The solution has been well received by frontline staff because it was built around their needs.

Zaizi embedded user-centred design specialists and [engaged end-users throughout the process](#). The human-centric research ensured a smooth rollout and helped identify essential operational needs — for example, a robust offline mode in port areas with no internet connectivity.

A Border Force team now operates ScanApp internally. Having helped

build the product, Zaizi completed a robust handover and upskilled our staff to run the solution independently.

At the start of the year, ScanApp won the [prestigious PEN-CP Global Customs Innovation Award](#). The award highlights cutting-edge solutions and forward-thinking innovations that address the evolving challenges faced by customs administrations worldwide.

## MAXIMALIST SCREENING — SCANNING WITHIN THE FLOW OF GOODS

As mentioned, customs agencies have a dual focus on security and keeping goods moving efficiently.

ScanApp removes the need to make a trade-off between the two. It helps achieve “maximalist screening” — screening as much as possible without disrupting trade.

Traditional methods of diverting vehicles from the normal flow of

goods for X-ray examinations disrupt the supply chain, are labour-intensive, and result in a low volume of scans.

ScanApp supports bringing x-ray machines to the cargo, rather than taking the cargo to scanners. It means less disruption and more cargo scans, strengthening border security without slowing the flow of goods.

### **QUICKER DECISION-MAKING — INTEGRATING AI**

Today, every government department is talking about AI. But AI is only as good as the data it's trained on — inconsistent and siloed information is not a solid foundation for machine learning.

By digitising our processes and capturing data in a uniform format, ScanApp has laid the foundations to incorporate AI capabilities.

Along with Zaizi, we're exploring how AI can help officers make faster, more accurate decisions using ScanApp. For example, if a manifest states "fruit and vegetables" but the X-ray and algorithm suggest "steel bars," the AI can flag the discrepancy for investigation by a human.

We're developing these capabilities using three main AI approaches: computer vision, large language models, and, in the future, AI agents.

### **CREATING A SCALABLE SYSTEM**

By building internally, we developed a reliable, robust product at a fraction of the cost of a proprietary system.

It was one of the first projects to establish development environments and pipelines on the Home Office's in-house infrastructure. Although integrating with government infrastructure can be complex, it delivers greater control along with strict data security and ownership.

ScanApp is also system-agnostic, integrating seamlessly with various suppliers and scanners. With



government agencies needing to prioritise cost savings, this flexible approach provides a robust, scalable solution without the eye-watering costs of closed-loop products.

The future of ScanApp involves embedding AI, focusing on maximalist screening without disrupting trade, and scaling across domains. Currently, we're addressing the maritime sector but we plan to expand into aviation and parcel/postal operations.

### **A ROADMAP FOR BORDER MODERNISATION**

For organisations considering a similar modernisation project:

- **Start small and specific:** Ensure any solution addresses your use cases and strategy. Don't try to solve every problem at once. Like ScanApp, the most effective solutions are agile and innovative, without being unnecessarily expensive or complex.
- **Put users first:** Move away from manual, paper-based processes by building digital tools that meet the officer's day-to-day reality. Crucially, involve them in the process to secure buy-in. When you design with users, you ensure your solution helps, not hinders them.
- **Build for reuse and interoperability:** Design services to last. One of the benefits of building a system in-house is the ability to reuse the same core platform and

adapt it to different operational scenarios. For example, ScanApp can be applied across a range of border control, security, and inspection settings, both in the UK and internationally. Being supplier-agnostic also ensures better integration with other hardware and future innovations.

With government resources declining but demand on the border increasing, digitisation, automation, and AI are essential tools for delivering secure, efficient services — and for doing more with less.

---

Darren Hart MBE is currently a Programme Director with the United Kingdom Border Force Border Strategy and Transformation Directorate. He focuses on designing and delivering Border Force's future goods operations, creating a secure, facilitative frontier through advanced technologies and modern processes. Darren has more than 30 years of experience across immigration, customs, intelligence, and border security, and is a World Customs Organisation Recognised Expert. In 2020, he was awarded an MBE (Member of the British Empire) for his contribution to the post-BREXIT security and trade facilitation arrangements.

---



By Jon Payne,  
Director Government Relations, &  
Jyotsna Pantula, Director Government  
Solutions Marketing, Entrust

# Dominican Republic Launches New E-Passport



**I**n the march towards global digital borders, perhaps the single most important innovation has been the issuance of chipped electronic passports compliant with International Civil

Aviation Organization (ICAO) standards. e-passports not only enable faster and more secure checks at border points, but have also paved the way for many of the other innovations now emerging in this

space, including digital travel credentials and walk-through biometric corridors.

With 170 countries now issuing e-passports worldwide, the Americas region takes a step closer to total coverage

in early 2026 with the issuance of the first ever chip-enabled passports in the Dominican Republic. This leaves just a handful of countries in the region still to take this step, namely Cuba, El Salvador, Guatemala and Nicaragua.

Towards the end of 2025, the Dominican General Directorate of Passports (DGP) announced that the first ever Dominican Republic e-passport would be issued to President Luis Abinader in a launch ceremony in Santo Domingo on January 14, 2026. Soon after, the general public, including diplomats posted abroad, will be able to request the updated passport.

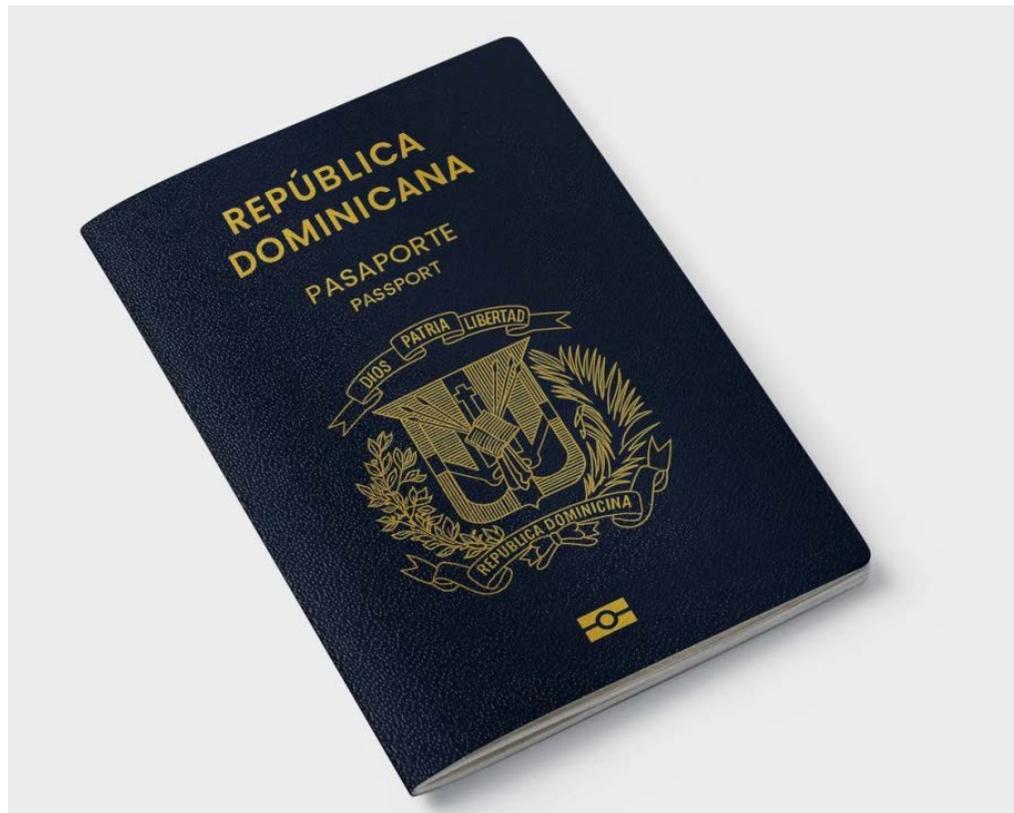
The DGP also announced that the new Dominican e-passport has been admitted into the ICAO Public Key Directory (PKD), allowing the new passports to be verified internationally when holders are traveling overseas.

### POWERING DIGITAL TRANSFORMATION WITH PUBLIC-PRIVATE PARTNERSHIP

Entrust is delighted to collaborate with MIDAS Dominicana and Thales, working in partnership with the DGP to bring this project to life.

The Dominican Republic government tasked the three companies to develop a sustainable strategy for implementing the new passport system. In response, a Public Private Partnership (PPP) between the government and its technology partners was established.

Under this framework, the Directorate General of Passports maintains complete authority and oversight over the entire system, ensuring that national interests and regulatory requirements are upheld. Meanwhile, the companies contribute their specialized technical knowledge, handling the personalization and issuance of



e-passports as well as providing integration support. Through this expertise and collaborative effort, the companies deliver a comprehensive, high-security electronic passport system and security infrastructure for the Dominican Republic, designed to meet international standards and future-proof the country's digital identity infrastructure.

MIDAS Dominicana is a Dominican company with a strong track record delivering technology solutions and information security for government agencies and the private sector. MIDAS acts as the primary integrator and project leader working with the DGP and is responsible for the overall development, implementation, and maintenance of the electronic passport system. Together with the DGP, MIDAS ensures the system's security, efficiency, and compliance with international standards.

Thales is responsible for providing the passport books, including the design, production, and personalization of the chip. It is also responsible for the biometric enrollment system.

Entrust provides industrial-scale printing and secure engraving of the electronic chip in the passport at the time of personalization, with its Datacard PB8500 Compact passport issuance systems. Entrust also deployed the PKI (Public Key Infrastructure) securing the data infrastructure for the DGP. With over 50 years of expertise in developing highly secure printing systems and the integration of advanced digital identity features, Entrust technology ensures the secure issuance of electronic passports.

CECOMSA (Dominican Republic) provides technological support and manages local data centers, ensuring the system's reliability and local operational continuity.

The new e-passport features an integrated chip containing encrypted biometric information, along with a digital photo and electronic signature. The passport book also features more than 70 security elements—including holograms and secure inks—and a durable polycarbonate data page to mitigate against fraud and tampering. The

internal pages highlight key aspects of Dominican history and culture.

The integration of both local and international partners ensures a passport solution that is not only recognized and certified on a global scale, but also specifically adapted to the unique requirements of the Dominican Republic. It ensures the highest standards of security, protects the privacy of the Dominican citizens, and ensures operational excellence at every stage.

The transition to biometric passports will help reduce document fraud, enhance international confidence in the identity of Dominican citizens, and ensure compliance with global security standards and migration interoperability.

The Dominican Republic's successful implementation of a comprehensive and secure electronic passport system serves as a blueprint for countries considering the transition to biometric passports in alignment with the ICAO's requirement to implement ISO/IEC 39794-5 standards for eMRTDs by January 1, 2030. The collaborative framework, which brings together both domestic and international expertise, highlights the effectiveness of public-private partnerships in delivering digital transformation that satisfies international security requirements while being responsive to national priorities.

## DIGITAL PUBLIC INFRASTRUCTURE

In a press conference in September 2025, President Luis Abinader put the new e-passport project in the context of a wider initiative by his government to build Digital Public Infrastructure (DPI).

The Dominican Republic was one of the first countries to join the 50-in-5 campaign promoted by the United Nations Development Program

(UNDP). The aim of the campaign is to support fifty developing countries to establish secure, interoperable DPI systems over a period of five years. The new e-passport and related improvements in border security are an important aspect of this wider effort.

"The country has achieved significant progress in operational safety, modernization of airports, digitalization of processes, and expansion of international connectivity," said the president. "The electronic passport coming soon will have biometric data aligned with international standards, which will strengthen security and travel speed."

The president went on to emphasize wider developments in border security. "In terms of digitalization, we also have Global Entry which has been a great agreement. Since 2023, the country became the first in the Caribbean, and the sixth in Latin America, to join in. We also have e-ticket for digital migration declarations, and auto gates to speed up transit."

## THE NEXT WAVE OF DIGITAL BORDER TRANSFORMATION

We are approaching complete global coverage in terms of ICAO-compliant e-passports. That will be an important step in terms of making digital border security available to all. In order to achieve this, however, some of the remaining countries are likely to need support from the international community, including in the form of developmental aid. Those of us in the industry can contribute to the effort by working creatively to form partnerships and developing commercial models to ensure that no countries are left behind.

---

Jon Payne is Director, Government Relations

at Entrust, where he focuses on digital identity, biometrics and citizen services. He joined Entrust in 2021 via the acquisition of WorldReach Software. Jon has more than 25 years' experience in immigration policy and operations, having served at the UK Home Office as Regional Director, Americas (UKvisas) and Chief of Staff (UK Border Agency). He also served as Deputy Head of Mission at the British Embassy in Kabul, Afghanistan, and as Director of CSC's Global Citizen Services Center of Excellence.

Jyotsna Pantula serves as Director, Government Solutions Marketing, at Entrust, where she spearheads technical marketing initiatives for Entrust Identity solutions that span physical and digital identity issuance programs, fortify identity security, and advance cryptographic infrastructure projects for governments globally.

Prior to joining Entrust, Jyotsna was responsible for leading technical product marketing in the domains of critical infrastructure cybersecurity and Zero Trust at Siemens AG. With more than 15 years of expertise spanning product management, marketing, and business development, she has made significant contributions across key sectors such as cybersecurity for utilities and defense, Industrial IoT, and telecommunications.

Jyotsna holds an MBA with dual specializations in Marketing and Finance and has done her bachelor's in mechanical engineering and is certified in Industrial Network Automation from Siemens.



achieved this by evolving its IT infrastructure to be able to manage hundreds of millions of journeys at UK borders and at least three million tourist visas per year – working with industry partners to enhance efficiency and add new capabilities.

Indeed, while the UK has achieved a lot to modernise its borders, as threats continue to evolve and become more complex, new capabilities are essential to understand and counter the intricate challenges we face.

The subsea element of border protection is a case in point. This is a domain that has become increasingly contested, congested and complex over recent years – with threats increasing both in terms of frequency and severity. As such, the demand for information and intelligence to inform timely decision-making to counter the subsea threat to the UK is growing dramatically.

This highlights a need for networks of sensors and uncrewed underwater vehicles that can communicate data in real time – acting as our eyes and ears underwater as part of a broader border protection strategy.

The challenge of addressing new, complex threats is also where data, machine learning and artificial intelligence (AI) have key roles to play. For example, at BAE Systems Digital Intelligence, we're leveraging these capabilities to build mission-critical systems via the Crossing the Border product family, which has replaced legacy infrastructure that has been in operation since 1994. We also have a team working on Cerberus, a project to replace multiple existing systems with one that is capable of analysing data across different transport modes to create a fully unified picture of risk.

It's these types of initiatives that will enable the UK to keep pace

with the challenges of today and tomorrow, transforming our ability to recognise and assess threats across the UK's border.

### **A MULTI-DOMAIN APPROACH**

Amidst today's landscape, it's increasingly important to consider how different domains and assets can be integrated into one cohesive border control operation. This could include, for instance, observation data from low Earth orbit satellites, leveraging Synthetic Aperture Radar technology that can penetrate clouds to provide real-time intelligence. This cutting-edge approach could maintain a constant and comprehensive view of our borders, no matter the weather or time of day.

Advancements in AI are equally transformative, such as through novel uncrewed vehicles which can be complemented by sophisticated data capture and analysis tools. Harnessing AI such as computer vision for object detection and recognition in this way means we can monitor threats in real time.

And there are plenty more opportunities on the horizon. In the future, autonomous vehicles could be deployed to calculate their own optimised routes to the located threat and enhance our ability to rapidly react to new threats.

Indeed, when it comes to AI, there's virtually no limit to what's possible. Consider predictive maintenance functionality to address potential equipment failures before they occur, ensuring critical assets are always mission ready. Or using AI to help position operational teams in areas where risks are most likely to emerge, enhancing our ability to respond proactively – allowing us to go beyond responding reactively to threats at the border.

It's not a stretch to envisage a future where new data, sensors and

capabilities will combine to form a rich picture of risk. This fusion of historical records and real-time data could empower the UK's Border Force teams with the perspective they need to make decisions that ensure the right resources are deployed where they're needed most to keep our border secure.

As a result, international business travellers and everyday citizens coming to the UK alike will feel even safer. People can travel in confidence knowing that the government is working in conjunction with the UK technology ecosystem to develop and deploy reliable systems that are designed to enhance the security of the UK border, while also making journeys smooth and hassle-free.

Ultimately, the UK has to stay ahead of the curve, maximising opportunities from upcoming technological advancements such as space, sensors or AI. This is what will help achieve the goal of making the UK border the easiest to interact with in the world, while ensuring the country stays secure.

---

Dil Begum is an Account Manager at BAE Systems Digital Intelligence, turning complex digital and security challenges into impactful outcomes. She bridges cutting-edge technology with real-world needs, collaborating across teams to deliver high-stakes solutions that protect critical infrastructure and drive meaningful change.

---



By Mohammed Shameem,  
Chief Customs Officer – Revenue, Fiji  
Revenue & Customs Service (FRCS)

# Border Management, Security and Technology: Strengthening Fiji's Borders in a Rapidly Changing World

**B**order management across the world is undergoing rapid transformation, and Fiji is no exception. As an island nation strategically positioned in the Pacific, Fiji's borders are critical gateways for aviation, maritime travel, international trade, and economic growth. At the same time, they represent frontline protection against illicit activity, transnational crime, biosecurity risks, and emerging threats.

In this evolving environment, technology has become central to strengthening Fiji's border systems. It enables greater efficiency, enhances security, and supports the national vision of a modern, trusted, and resilient border environment. The Fiji Revenue & Customs Service (FRCS)

continues to invest in smarter, data-driven models of border control that ensure both facilitation and security are achieved in balance.

## **THE MODERN BORDER ENVIRONMENT IN FIJI**

Fiji's border environment is shaped by several key pressures that require continuous adaptation and strong inter-agency coordination.

### **Growing Passenger Movements**

International airports, particularly Nadi International Airport, continue to experience strong rebound and growth in travel. Tourism recovery has placed additional pressure on manual clearance systems, making investment in automation and digital identity solutions essential.

Increasing passenger flows require faster processing to maintain Fiji's competitive tourism advantage.

### **Expanding Trade and E-commerce**

Fiji's trade volumes, especially small consignments and courier shipments, continue to grow. With the rise of e-commerce, FRCS must process higher volumes of declarations, often with incomplete or inaccurate documentation. This makes data analytics, cargo profiling, and stronger supply chain visibility crucial to safeguarding revenue and preventing illicit goods from entering Fiji.

### **Evolving Transnational Threats**

Threats such as drug trafficking, human trafficking, currency

smuggling, cyber-enabled fraud, and misuse of travel systems are becoming more sophisticated. These threats increasingly bypass traditional checkpoints, emphasising the need for intelligence-led operations and technology-enabled risk management systems.

## **TECHNOLOGY TRANSFORMING FIJI'S BORDERS**

### **Digital Identity and Biometrics**

Modernising Fiji's air border operations requires advanced identity verification systems. Biometrics such as facial recognition, e-gates, and digital travel credentials improve the accuracy and speed of passenger clearance. As Fiji moves towards alignment with international border standards, integrating biometrics will enhance both traveller experience and national security.

### **Risk Management and Data Analytics**

Risk-based border management is central to FRCS's service delivery model. Through Advance Passenger Information (API), Passenger Name Record (PNR) analysis (access for which (PNR) is very minimal), and data-driven targeting tools, Fiji can detect anomalies early and direct resources toward high-risk travellers and consignments. Analytics also strengthen revenue protection by identifying undervaluation, misclassification, and fraudulent trade behaviours.

### **Strengthening the Cargo Supply Chain**

Cargo security in Fiji is being modernised through Non-Intrusive Inspection (NII) scanners, smart seals, and digital cargo documentation. These systems provide better transparency and reduce the

likelihood of tampering, diversion, or concealment. Faster clearance of compliant traders also supports Fiji's role as a regional transshipment hub.

### **Integrated Border Systems**

Integrated border management is key to improving coordinated decision-making across Fiji's border agencies. Systems such as ASYCUDA World, the Fiji National Single Window, and emerging inter-agency digital platforms improve information sharing, reduce duplication, and ensure aligned enforcement. Integration supports both facilitation and compliance by creating a single view of travellers, cargo, and vessels.

### **Automation, AI, and Surveillance**

Emerging technologies are beginning to shape Fiji's future border capability. Robotic Process Automation (RPA) can handle repetitive tasks such as data validation. AI-driven document verification enhances detection of forged invoices, permits, and IDs. Enhanced maritime surveillance, including drones and remote sensor networks, will strengthen monitoring of Fiji's vast maritime domain.

## **BALANCING FACILITATION AND SECURITY**

Maintaining Fiji's reputation as a welcoming tourism and trade destination requires strong balance between facilitation and border protection. Trusted trader programs, pre-arrival processing, simplified procedures, and digital lodgment platforms all contribute to faster processing for compliant clients. At the same time, improved risk tools ensure high-risk cases receive targeted attention. This balance is essential for both economic growth and national security.

## **THE HUMAN FACTOR: BUILDING SKILLS AND CAPABILITY**

Technology strengthens border management only when supported by skilled and capable officers. FRCS continues to invest in training programs focused on digital skills, intelligence analysis, enforcement, leadership development, and integrity. Officers must understand both the technology and the operational context to make informed, risk-based decisions that uphold national laws and service standards.

## **FIJI'S PATH FORWARD**

To continue modernising its border environment, Fiji's priorities would be:

- Introducing biometric and digital identity systems
- Strengthening cyber security across border platforms
- Deepening data integration with partner agencies
- Expanding maritime surveillance capabilities
- Enhancing industry partnerships across aviation, shipping, and e-commerce sectors
- Building a digitally capable workforce equipped for next-generation border operations.

---

Mohammed Shameem is the Chief Customs Officer – Revenue at the Fiji Revenue & Customs Service (FRCS). With extensive experience in border management, enforcement, revenue administration, and risk assessment, he has led strategic initiatives focused on modernisation, technology adoption, and strengthening Fiji's compliance systems. He is committed to advancing Fiji's border capability through innovation, integrity, and collaborative partnership.

---



By Peter Sutcliffe,  
Borders Technology Lead,  
Fujitsu

# Leveraging Visual Behavioural Analytics to Secure Borders and Protect Public Spaces



## DIGITAL REVOLUTION

Right now, we are experiencing a digital revolution. And it affects every aspect of how we work, live, and interact with the wider world. This revolution has fundamentally changed our reliance upon and relationship with technology. It has created new capabilities that were inconceivable only a few years ago.

Artificial intelligence, quantum computing, large language models, machine learning, predictive analytics, and the real-time analysis of massive,

complex data sets have become mainstream, no longer confined to academia or research laboratories.

In our work in border and public security, we foresee continued advances in real-time video analytics capabilities (analysing video feeds as they are captured) and predictive analytics (initiating actions based on predictions)—underpinned by behavioural science. These capabilities can identify people, understand context, predict potential outcomes, and support decision-making,

advancing how governments secure their borders.

## TRANSFORMING BORDER SECURITY

The security of a country's borders continues to dominate political thinking and public opinion. While much of the debate of recent years has focused on a government's ability to detect and deter illegal immigration—and the policies in place to manage borders more effectively—the reality is that many borders already utilise

robust data-driven systems and advanced technology to reduce risk and help detect and prevent inadmissible passengers and persons of interest from entering the country.

Our work helping governments secure their borders has shaped our approach to applying intelligence, performing risk assessments, determining eligibility, detecting intent, informing decision-making, and ensuring operational integrity.

We understand the value of ‘foresight’ to maximise upstream opportunities to drive down risk before crossing a border. Continuous analysis of border operations creates ‘insight’ by applying existing—and generating new—intelligence to deliver comprehensive situational awareness. And ‘oversight’ ensures that operations improve; people, technology, and processes evolve; and security outcomes increase.

### **HARNESSING THE POWER OF BIOGRAPHIC DATA**

Today, travellers are well aware of the need to share their passport information (i.e., API) when traveling internationally. They are equally adept at scanning their passports and having their identity verified by e-gates and kiosks when crossing borders.

However, as some governments propose new rules that could require travellers to provide details of their social media accounts, previous phone numbers and e-mail addresses (and potentially DNA and other biometrics), an examination of alternative, more balanced approaches is needed. From a societal perspective, a deeper conversation about how much data is enough (or too much) to cross a border will need to consider the broader implications on travel and tourism-based prosperity, and public trust. Some travellers may perceive a destination as unwelcoming, administrative barriers too high, or presenting too great a risk to their right to privacy.

The goal in examining alternative



approaches should be to build government confidence in adopting innovations like Visual Behavioural Analytics, which can reduce risk and deliver equal or better security—without requiring more biographic data.

### **INCREASING AUTOMATION**

The deployment of e-gates, kiosks, totems, contactless corridors, and mobile digital identity solutions continues to gather momentum worldwide. Yet the drive to adopt faster, more seamless border crossing systems has created unintentional capability gaps. Despite many benefits, automation has reduced border officers’ time and opportunity to assess risks, ask questions, intervene, and ensure there is no erosion of security. Without additional measures, increased automation will only further diminish an officer’s ability to perform vital risk assessments and detect anomalous behaviour.

### **CAPABILITY GAPS: THE ROLE OF TECHNOLOGY**

What capabilities are in place to prevent the misuse of e-gates or identify suspicious or anomalous behaviours in the arrivals hall? How can we reliably expect even the most attentive officers to continuously monitor an array of CCTV displays in the Security Operations Centre (SOC)—or monitor a constant stream of people’s faces as they proceed through a bank of multiple e-gates in just a few seconds while maintaining the highest levels of attention throughout their entire shift?

These questions lead us to see the value of ‘enhanced automation’, including the deployment of Visual Behavioural Analytics—and systems of action that detect, alarm, respond,

and report incidents in real-time. This enables continuous improvement in security performance through a joined-up approach that ensures mitigation and response measures are deployed instantly.

What’s more, by ensuring algorithms continually ‘learn’, the capability improves over time, and applies each learning across all operations. For example, a behavioural indicator analysed after an event in one location can—when reviewed and approved by a border officer—be codified to automatically alarm (and generate responses to) a comparable behavioural indicator detected in all other locations.

This would be a significant mitigation for risk displacement, where, for example, human traffickers and migrant smugglers who, perceiving controls to be more rigorous at one location—thereby increasing the probability of detection—shift their operation to a location where they believe controls are less stringent, and their chances of success greater.

Encouragingly, these capabilities not only exist but are also relatively simple to deploy. Once we integrate our product’s algorithms and systems of action into the video surveillance system, it harnesses all cameras connected to it.

The more complex aspect is designing rules and operational processes and building robust systems of action on the back-end. These will determine what type(s) of behaviours should be detected, how alarms should be raised (and cleared), and how mitigation and response measures are deployed.

It’s vitally important to make a clear distinction between automated rules and those that require

human authorisation. With the right approach, these solutions can be responsibly deployed to close capability gaps, strengthen border security, and leverage border officers' skills to assess risk and detect anomalous and suspicious behaviour.

### **LEVERAGING TECHNOLOGY TO SECURE THE BORDER**

Much of our work in border security has been behind the scenes, delivering secure, resilient and mission-critical systems to inform front-line operations. Distilling this deep operational insight, combined with our leadership in complex, high-volume environments, we invested in R&D to evaluate how new seamless journeys and contactless corridors could be enhanced by video analytics underpinned by behavioural science.

Together with Cranfield University, we implemented a Contactless Corridor trial that was presented to UK government stakeholders responsible for transport and borders. To participate, travellers needed to create a Digital Travel Credential (DTC) prior to arriving at the border. The border system then built an 'expected arrivals gallery'. Upon arrival, cameras matched faces against the gallery to identify each person and tracked their movements from the aircraft throughout the airport into the arrivals hall.

The Visual Behavioural Analytics software detected a range of behaviours, including loitering in restricted zones, suspicious activity, medical events, unattended baggage, and overcrowding. It 'tagged' travellers exhibiting suspicious behaviour and continuously tracked their identity throughout the process. Consequently, identity verification was no longer confined to the time-sensitive and complex environment of the actual border crossing.

In future scenarios, officers in control rooms can be freed up to

prioritise intelligence, coordinate interventions for persons of interest (and analyse their relationships with others, objects, and situations), and direct roving officers equipped with mobile or wearable Augmented Reality (AR) displays to intervene when required. This will drive further efficiency gains in operational monitoring, clearance, and intervention and maintain the highest levels of throughput at the border.

The results of the trial have increased our confidence in the value of Artificial Intelligence (AI) in forecasting human behaviour, leveraging real-time video analysis, facial recognition, and person-sensing technologies to understand, predict, and make action recommendations.

### **THE VALUE OF HUMAN OPERATIONS**

An officer's valuable observation and detection skills, when combined with technology, serve as a robust defence against human trafficking, document fraud, smuggling, illegal immigration, and terrorism. And in-person interviews establish the purpose and duration of stay and determine whether the person should be granted permission to enter or subjected to further scrutiny.

With the advent of automated border control, Concepts of Operations (CONOPS) have evolved. Many officers now perform crucial operational monitoring roles. They monitor the use of multiple e-gates simultaneously and coordinate interventions when alerts are triggered or when manual inspections and referrals are needed.

With high workforce costs, the compelling argument is to leverage technology to enhance border operations. Integrating new solutions should lead to revisiting operational models to increase both efficiency and security—fulfilling the promise of technology-led border transformation.

This enables officers to be deployed

in other areas of operation, apply intelligence, perform more in-depth investigations of specific events, and train future cohorts of staff to develop their skills and acquire the knowledge needed to improve the quality and accuracy of the technology solutions that support them.

### **THE ROAD AHEAD**

We are seeing a continuing global drive towards automation and the adoption of digital identity solutions to accelerate border crossings. The next evolution of border security will be driven by advances in real-time and predictive video analytics, with attention-focusing technologies and systems of action, integrated with applications operated by governments and regulated agencies.

The ability of Visual Behavioural Analytics solutions to learn and adapt in real time will ensure that operations improve, people, technology, and processes evolve, and security outcomes increase.

In terms of social acceptability, the deployment of Visual Behavioural Analytics solutions should provide governments with confidence that risks can be effectively managed without requiring travellers to submit ever-increasing amounts of personal data and sensitive information.

---

Peter Sutcliffe has worked across the security industry for more than 25 years. He is the Borders Technology Lead at Fujitsu, having previously held senior technology leadership roles at world-renown organisations, including BAE Systems, Raytheon, SITA and Roke. He holds a Masters in Engineering (MEng Hons) from Loughborough University. Throughout his career, Peter has had a singular mission to support governments in their examination of national security risks and develop advanced technology solutions to address them.

---



**IBMATA**  
INTERNATIONAL BORDER MANAGEMENT  
AND TECHNOLOGIES ASSOCIATION

# **BORDER MANAGEMENT & TECHNOLOGIES SUMMIT**

## **AMERICAS 2026**

**10–12 March 2026**  
**Mexico City, Mexico**

**[WWW.IBMATA.ORG](http://WWW.IBMATA.ORG)**



By Kevin Foster,  
former UK Immigration Minister  
and Member of IBMATA

# Eyes on the Coast – How Maritime Loopholes Must Be Closed



**W**hen writing about Border Management issues some subjects can seem far away, yet this one comes very close to home.

Torquay is known in the UK for Palm Trees, holidays and our most infamous hotelier Basil Fawlty! For me it is home.

Torquay Harbour is a place where visitors stop for a photo with Dame Agatha Christie’s statue, yet it’s a recent visitor with more sinister intentions which saw it hit the national headlines.

## TO TORQUAY WITH INTENT

A suspected Russian intelligence operative entered the UK via Torquay Harbour earlier this year.

He did not sneak in having been dropped off by a submarine as a spy movie might suggest he would, instead

he openly entered the UK as a crew member on a Finnish cargo ship.

Once ashore, he reportedly travelled to Dorset, near Lulworth Cove, where Ukrainian troops have been training with UK forces. It is not clear if he managed to get any intelligence beyond what someone walking past may see, yet the Kremlin's message was clear: It can get to places which are key to Ukraine's defence, including on the British Isles.

This incident was also a worrying reminder of the Salisbury Incident of 2018, when Russian former double agent Sergei Skripal and his daughter Yulia were poisoned using Novichok. Two Russian agents entered the UK with murderous intent. Their excuses about wanting to see the spire of Salisbury Cathedral being plainly ridiculous, in the same way any suggestions the recent visitor wanted simply to see the Jurassic Coast. Yet these ridiculous denials help make the message from the Kremlin clear about its intentions to those it wished to intimidate.

I was banned from Russia three years ago, due to my vocal support of Ukraine. Knowing a suspected Russian agent entered the UK through my local harbour, which has no scheduled international routes or passenger terminal, was a reminder of how nowhere is safe from the growing threat posed by hostile states.

### **NOT A NEW PROBLEM**

Devon and Cornwall has always been a challenge for border security.

The area's rugged coastline provided ideal hideouts for the smugglers of the past. The historic ancestors to today's Border Force, revenue men, were a force established to chase down those involved. This work included the establishment of England's first Preventive boat in Polperro in 1801, which patrolled the coast and enforced the law against smugglers.

Today law enforcement agencies keep watch on the South West's coast and maritime traffic to intercept modern-day threats such as illegal migration, firearms, drugs and explosives. Yet as already mentioned the recent incident was not connected to a boat sneaking into a cove at the dead of night: the person concerned arrived on a large ship, disembarked at a port and is understood to have entered the UK via the rules for Seafarers.

This aspect is what those responsible for managing border security need to focus on.

### **PRACTICAL STEPS**

There is no realistic prospect of having the type of border infrastructure found at airports or major seaports at every small or medium sized coastal port.

Yet doing nothing will see this backdoor into the UK and other western countries be exploited further by not just hostile state intelligence agencies, but others keen to circumvent border controls. There needs to be work to both improve awareness on the ground and to take policy decisions to amend rules which are being abused.

Solutions which balance security with the weight of trade done via maritime shipping and maintaining flow of legitimate crews will be needed.

### **LOCAL HARBOUR AUTHORITIES**

Many smaller harbours are the responsibility of local government, so ensuring effective collaboration between national agencies and local workers will be an essential role for government.

Understandably most harbour authority workers will not be familiar with counter-espionage techniques but are aware of the need to be naturally curious in their job. Coverage of potential use of small vessels for illegal migration and drugs importation has raised awareness.

Information sharing with front

line employees on the ground in local communities can deliver results. In 2013 a council refuse collector in Torquay uncovered a far-right terror plot, because he was curious as to why a house only occupied by men was throwing out so many empty hair dye bottles.

Regular engagement between agencies and the local government leaders who oversee local harbour operations is vital to ensure it's an embedded part of policy decisions, with all understanding their role in this.

### **REVIEWING MIGRATION RULES**

Seafarers arriving on a ship are usually covered by section 8(1) of the 1971 Immigration Act rather than the Immigration Rules, because they are part of the crew.

Being part of a ship's crew provides a simple route into the UK for visa nationals, they do not need to seek specific entry clearance, just hold the relevant documentation for seafarers.

The UK Government website confirms this position by stating:

Seafarers travelling under contract to join a ship in the UK need entry clearance (if they are visa nationals), unless they hold a document issued by a country which has ratified the 1958 International Labour Organisation (ILO) Seafarers Identity Documents Convention No. 108 (see below).

It goes on to state:

*The UK agreed a new convention ILO185 in 2003 and intends to ratify if an effective method of implementation can be identified. To date, the UK has not ratified ILO185. A number of countries, whose seafarers previously qualified for visa exemption under ILO108, have ratified ILO185 (see below). As a result of ratifying ILO185 these countries have denounced ILO108. However, holders of documents issued by these countries do not require entry clearance to join a ship in the UK.*



### **(SEAFARERS - GOV.UK)**

Why is this key? One of the countries to have ratified ILO 185 is the Russian Federation.

**This means citizens of Russia can travel into and out of the UK provided they hold the relevant ILO Seafarers documents. As shown by recent incidents this is open to abuse.**

It's this backdoor the UK needs to close.

### **CHANGE**

Few border authorities would wish to implement visa processing for all who arrive as seafarers.

The overall principle of the dedicated system for seafarers makes sense and avoids them having to hold multiple visas for individual

nations to work on a single ship. Yet maintaining this position for Russian Nationals is odd at a time when the UK and others have applied extensive economic sanctions following the war in Ukraine. It creates an opportunity for a backdoor entry without a visa for someone whom intelligence services may be very interested in, but do not wishing to share information more widely to those issuing seafarer's identification documents.

Recent events are also a reminder of how treaties signed decades ago are now struggling in a very different era of border security requirements.

Whilst Russia continues to send people with intent, not love, on their agenda there is a need to close this backdoor to the west and

implement stronger vetting. This includes reviewing maritime laws where the need to move freely as part of legitimate trade is providing opportunities for intelligence operatives whose aim is to undermine international law, not respect it.

---

Kevin Foster is a former UK Immigration Minister and Member of IBMATA. Kevin regularly appears in UK media commenting on Immigration, Border Security and Law Enforcement. Alongside his media work he acts as a consultant advising clients on a range of public affairs and media issues.

---



By Pedro Alves,  
Senior Vice President  
of SITA Borders

# Unlocking the economic power of borders through digital identity

Borders are rarely seen as economic infrastructure. For most travelers, they are simply the moment a journey slows down. But for governments, borders play a much bigger role. They influence tourism, trade, investment and how a country connects with the world.

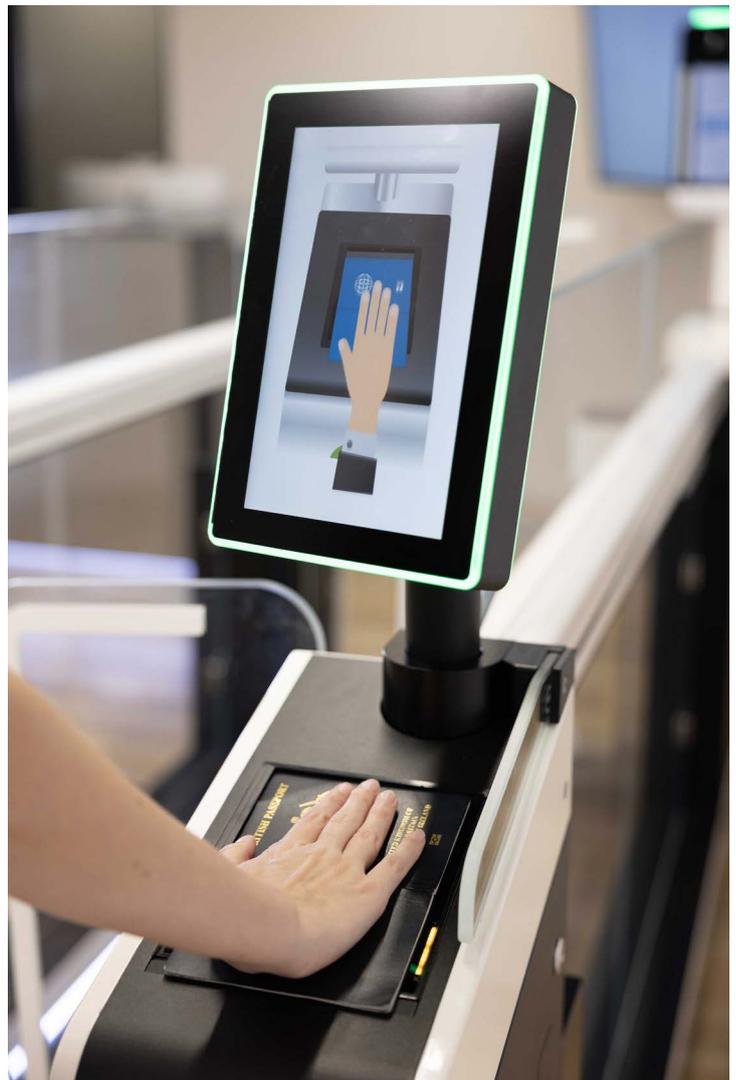
As global travel continues to grow, the way people and goods cross borders is becoming a quiet but powerful driver of economic success, prosperity and projection of modernization.

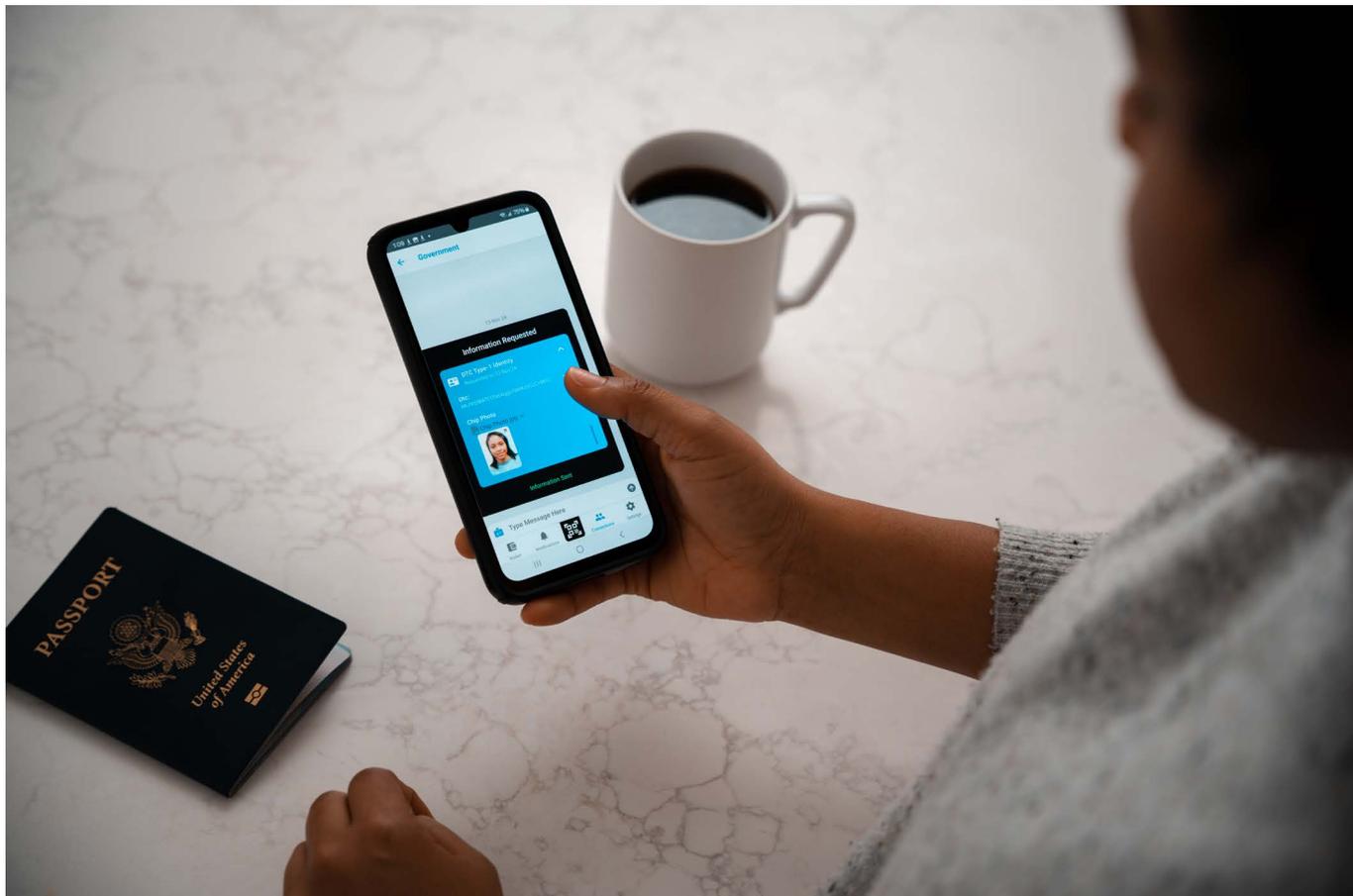
## AN OPPORTUNITY TO EVOLVE WITH MODERN TRAVEL

Travel today is increasingly digital, and visible touchpoints are simply the tip of the iceberg. People book flights online, check in on their phones and receive real-time updates throughout their journey. Expectations have changed. Travelers now value speed, clarity and reliability as much as price. An innovative and seamless experience is expected to be part of the journey.

Borders sit at a pivotal point in this journey. Many authorities have already taken steps to modernize their systems. Yet as travel volumes continue to rise, there is a growing opportunity to align border processes more closely with how people move today.

This is not about removing controls. It is about applying them earlier and more intelligently. When borders evolve alongside travel demand, they can support smoother journeys while maintaining strong security while maximizing the usage of infrastructure





through efficient operations.

The benefits go beyond passenger experience. Optimized Borders help grow tourism, encourage repeat visits and strengthen a country's appeal for business and investment. At the same time, agencies gain better visibility and stronger tools to manage risk.

As volumes increase and risks become more complex, the challenge is not choosing between security and growth. The opportunity is to move both forward together.

### THE SCALE OF THE OPPORTUNITY

Global passenger numbers were expected to reach 10 billion journeys in 2025 and rise to 12 billion by 2030, according to the Airports Council International. Governments and industry are responding with major investments in new airports and large-scale expansions across the world.

But infrastructure alone will not

unlock the full economic return.

Research from the World Travel & Tourism Council shows just how much is at stake. By 2035, travel and tourism are expected to contribute US\$16.5 trillion to global GDP. Modernizing borders could unlock a further US\$401 billion in economic growth and support millions of additional jobs across G20, EU and African Union countries.

This is not a theoretical benefit. It is real economic value waiting to be realized.

### FROM FIXED PROCESSES TO FLEXIBLE SYSTEMS

Borders have traditionally been built around fixed rules and static processes. Policies are written, translated into procedures and rolled out over time. This approach has delivered consistency, but it can struggle when conditions change quickly.

Recent years have shown how fast the world can shift. Health crises, sudden changes in travel patterns and major global events such as the FIFA World Cup all place intense, short-term pressure on border systems. These moments require authorities to prepare in advance and adapt quickly, often across multiple agencies and checkpoints.

Flexible, digital border systems make this possible. They allow rules and requirements to be updated consistently and applied in real time, helping borders scale smoothly when demand surges without adding pressure on frontline staff or travelers.

During COVID-19, many authorities discovered how difficult it could be to update rules quickly across systems. According to the World Economic Forum, only a small number of border agencies were able to adapt policies rapidly during the early

## UNLOCKING THE ECONOMIC POWER OF BORDERS THROUGH DIGITAL IDENTITY

stages of the pandemic.

The lesson is not about blame. It is about design. Modern borders need to be flexible by default.

### WHY INTEGRATION MATTERS

Border management is complex and involves multiple agencies: immigration, customs, public health, intelligence, tourism, law enforcement and others are gradually becoming stakeholders. Each plays a vital role. When systems are separate, information can be fragmented, and decisions can take longer than necessary.

An end-to-end, holistic approach through integration brings these pieces together. When agencies share data and work from a common picture, officers can make faster, better-informed decisions. Infrastructure can be better managed and resources can be focused where they are most needed.

This also helps to shape the country experience. [The International Air Transport Association](#) reports that more than 70% of passengers still face long queues and repeated document checks at borders. These moments often form a visitor's first and last impression.

By securely pre-clearing travelers using digital identities and real-time data, borders can reduce congestion while strengthening oversight. Security is not reduced. It's applied earlier, with better information.

### PROGRESS DOES NOT HAVE TO BE COMPLEX

Border modernization does not need to start with large, multi-year programs. Some of the most effective progress begins with small, focused steps.

Lima Airport in Peru offers a clear example. By introducing a mobile app for pre-travel declarations and automated eGates, the National Superintendency of Migration (Migraciones) now enables travelers to verify their identity, digitally, before they travel. This shift has cut wait times by



up to 50% and delivered a faster, more secure experience for both travelers and government agencies. This project proves that even small steps with digital identity can drive measurable results.

Travelers are ready for this change. More than 60% say they would be willing to pay for a faster, contactless travel experience.

Simple pilots, clear goals and early results can build confidence and momentum for wider transformation.

### BORDERS AS GATEWAYS TO GROWTH

Borders will always play a vital role in protecting countries and managing risk. That will not change. What is changing is how this responsibility can be delivered.

Biometrics, machine learning, and digital travel credentials are no longer experimental. They are proven tools that help borders work more smoothly and more securely.

The real choice for governments is whether borders remain points of friction or become gateways to growth. Whether they rely on yesterday's processes or adapt to today's reality.

When people, goods and information can move securely and efficiently, borders support stronger economies and more resilient societies. If done well, travelers may barely notice the process.

But the economic impact will be felt for years to come.

Pedro Alves is Senior Vice President of SITA Borders, the air transport industry's tech engine that works with over 75 governments, including every G20 nation, to modernize airport and border operations.

SITA Borders aims to help governments strike the right balance between keeping people safe, stopping threats and still making travel smooth and welcoming.

Its technology supports the entire passenger journey, end-to-end, from pre-travel authorization to arrival and clearance – making it easier for border teams and better for travelers.

Its systems enable more than 2.2 billion journeys every year and connects with 700+ airlines, meaning passengers can move through borders more easily, and agencies get the data they need to make smart decisions.

SITA started providing border solutions with the 2000 Sydney Olympics, helping manage travel for thousands of athletes and fans. And more recently it supported the FIFA World Cup in Qatar, where its systems helped link travel, accommodation, and stadium access, all in one.

Whether it's in the air, on land, or sea, SITA is helping governments to keep borders secure, travel flowing effectively, and people moving safely. Read more [here](#).



**IBMATA**  
INTERNATIONAL BORDER MANAGEMENT  
AND TECHNOLOGIES ASSOCIATION

# **BORDER MANAGEMENT & TECHNOLOGIES SUMMIT**

## **EUROPE 2026**

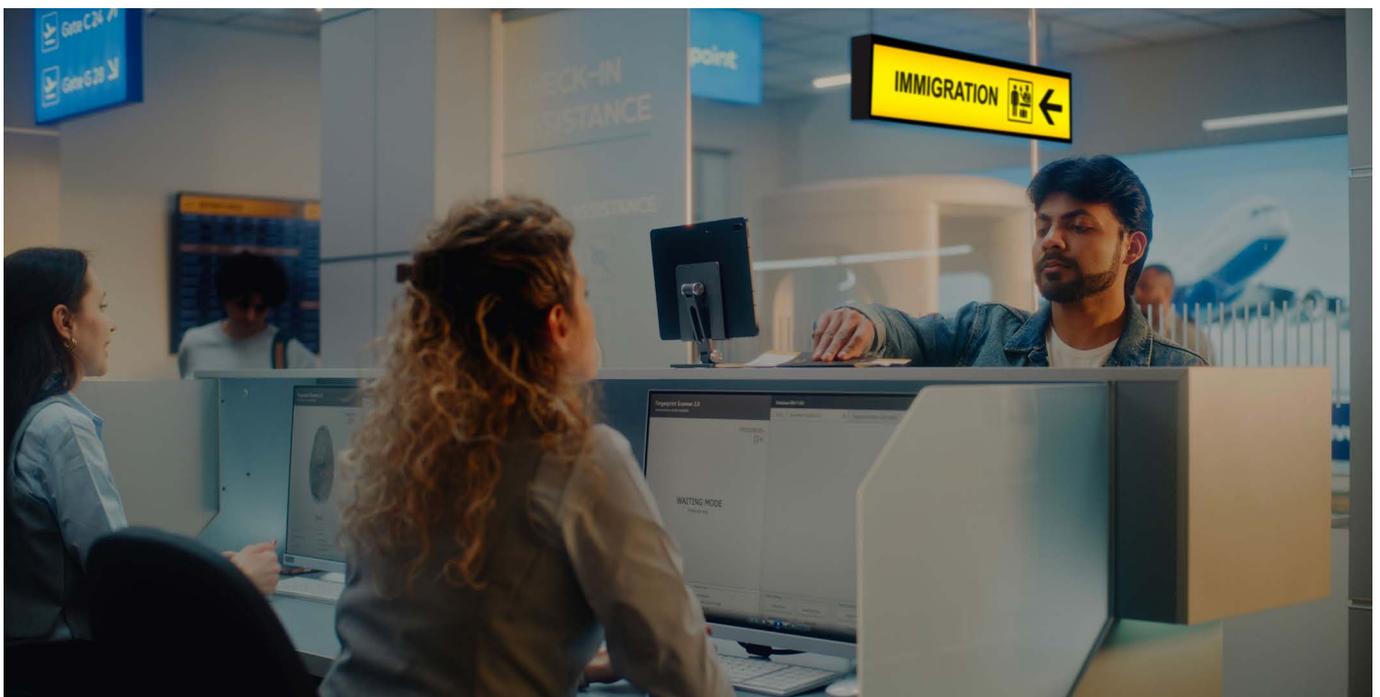
**22-24 June 2026**  
**Lisbon, Portugal**

**[WWW.IBMATA.ORG](http://WWW.IBMATA.ORG)**



By Yann Tréméac,  
the Border Control segment lead,  
Thales Cybersecurity and Digital

# No silver bullets: secure borders demand successful integration of multiple technologies



**T**o stay one step ahead of an increasingly complex threat landscape, authorities must adopt truly holistic approaches to their border management systems.

Around the world, criminals and other malign actors are relentlessly seeking to undermine the identity and document verification processes that underpin border security. In response,

authorities are turning to an array of biometric-based and automated systems. However, while such technologies represent powerful assets in the fight against identity fraud, there is no room for complacency.

The increasing use of biometric-based and automated document verification is inevitably driving fraudsters to look for potential

weaknesses in these mission-critical systems. Digitalisation is also expanding the attack surface exposed to cybercriminals. Within this evolving threat landscape, authorities need to adopt a holistic approach to their border management systems. In other words, traveller-facing verification processes are part of a much bigger picture. Secure borders ultimately

depend on the successful integration of multiple back-end and front-end technologies. What's more, these extended ecosystems must be agile enough to stay one step ahead of even the most sophisticated threats.

### **IDENTITY FRAUD IS A MULTI-BILLION-DOLLAR INDUSTRY**

Identity fraud is a global business. In the US, the Federal Trade Commission recorded 3.7 million identity theft and fraud reports in 2024, with total losses exceeding \$12.7 billion. For border authorities, organised crime and state-sponsored actors typically represent the most serious problems. With natural disasters and geopolitical tensions driving mass migration, human trafficking and people smuggling offer rich rewards for determined criminal networks. As a result, authorities are routinely dealing with highly complex and threatening situations at their borders.

### **SECURITY IS NOT THE ONLY CHALLENGE**

In an uncertain world, security is the obvious priority. But it is not the only challenge. Global passenger numbers are predicted to nearly double between 2024 and 2053. Border authorities are therefore under intense pressure to manage growing traveller throughputs, avoiding delays and delivering the best possible user experience.

Here again, biometric-based and automated document verification systems offer compelling benefits.

### **EFFECTIVE VERIFICATION IS KEY**

Verifying that each traveller is who they claim to be, and entitled to enter the country, has always been the foundation of border security. Traditionally, checks were performed manually, resulting in slow, labour-intensive processes prone to human



error. Over recent years, however, passports and visas have incorporated numerous advanced electronic and visual security features. Widespread adoption of this new generation of ePassports and other travel credentials has enabled border authorities to leverage biometric-based and automated document verification systems for fast and reliable assessment of travellers and their credentials. Deployed in self-service solutions such as eGates these systems also cut queue times and free staff to focus on higher-value activities.

### **PRIME TARGETS FOR MALIGN ACTORS**

As biometric-based and automated verification systems move centre stage, malign actors are redoubling their efforts to bypass them. The criminal groups fuelling identity fraud and theft are well-resourced and persistent. And the tools of the trade are easily accessible: for example, ready-made kits for creating fake fingerprints are widely available online and on the dark web. Criminals are increasingly employing technologies such as AI to enhance their identity fraud and theft techniques.

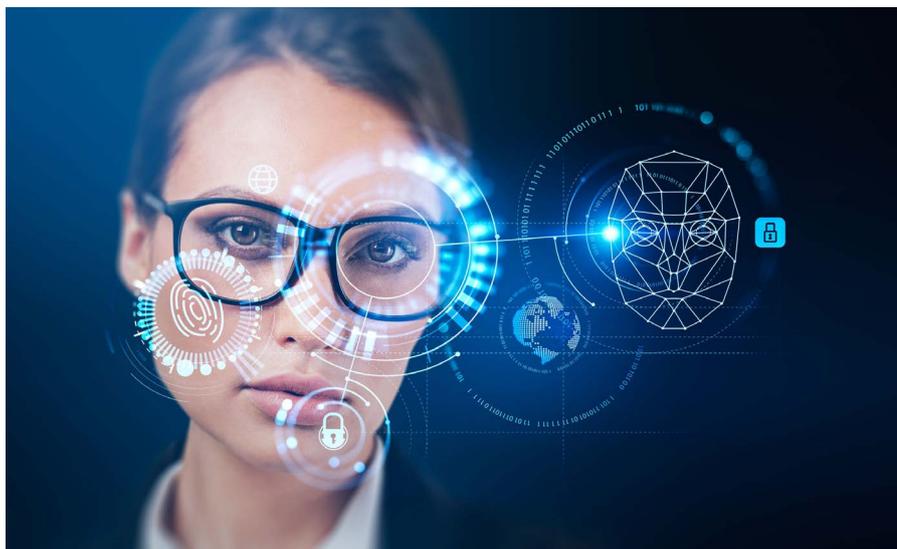
### **THE ROAD TO RESILIENCE**

To resist such threats, the obvious

starting point is to ensure that verification systems are capable of identifying even the smartest attempts at deception. Reflecting this, a growing number of border authorities are implementing multi-modal solutions that utilise biometric verification of two or three personal characteristics (face, fingerprint, iris) alongside advanced document verification technology to improve accuracy and resilience.

Crucially, solutions such as Thales' biometric-based systems also incorporate the latest Presentation Attack Detection (PAD - also known as liveness detection) techniques. For example, the facial recognition solutions integrated into the company's eGates employ best-in-class algorithms that marry outstanding accuracy with response times of no more than a couple of seconds. In addition, sophisticated liveness detection addresses spoofing threats that include the use of 3D masks.

Similar standards are evident in the Thales Gemalto Document Verification solution, which automatically verifies the electronic and optical security features of a wide array of ICAO and non-ICAO compliant documents including passports, visas, ID cards, and driver's licences. Again, AI supports advanced fraud detection.



For anyone still doubting the scale and seriousness of these threats, the figures speak for themselves: the global liveness detection market is predicted to grow from \$1.62 billion in 2026 to \$5.07 billion in 2035.

### **BUILDING COMPLETE BORDER MANAGEMENT ECOSYSTEMS**

As well as incorporating the latest anti-deception capabilities, verification systems must be fully integrated with an extended array of national and international databases and watchlists, detailing travellers' immigration, asylum, and residence statuses, for example, as well as fugitives and other persons of interest, and Interpol resources including the Stolen and Lost Travel Documents (SLTD) database.

Increasingly, governments also rely on comprehensive entry/exit systems that monitor the flow of individuals across all border crossings. This enables law enforcement and immigration agencies to rapidly identify issues such as visa overstays, while providing citizens with greater transparency and accountability around border movements.

Secure, reliable, and efficient back-end infrastructures are critical for combining all these systems, touchpoints, and data resources. Given the sheer complexity of modern

border management, successful strategies are invariably built on a powerful back-end platform. These platforms must also link a range of stakeholders, including airlines and airport operators, ensuring real-time information sharing and consistent verification throughout passenger terminals. What's more, border management infrastructures can no longer be limited to a single site; visibility needs to be provided across all crossing points, at all times.

### **ENABLING DIGITALISATION TO FLOURISH**

Across every aspect of modern border management, digitalisation is now an imperative. Yet it has the potential to create new vulnerabilities. Hacking, DDoS attacks, malware, and similar threats represent profound risks. Furthermore, the use of biometrics has massively increased the volume of sensitive personal data that authorities are responsible for storing, sharing, and managing. For criminals, all such data represents a highly valuable commodity in the illicit economy. Organisations must therefore ensure robust protection and rigorous compliance with relevant data privacy and cybersecurity regulations.

To create trusted environments in which digitalisation can flourish,

cybersecurity solutions should mirror the integrated, holistic approach of the border management systems they protect. Cloud-based security and cyber-resilient architectures, combined with secure-by-design components, can ensure scalability and flexibility – and provide authorities with the confidence to deploy new technologies and focus on core activities rather than cybercrime. Travellers are similarly given the confidence to share their personal details via self-service touchpoints.

### **HARNESSING THE POWER OF TEAMWORK**

For border authorities worldwide, there will be no let-up in the speed of change. Threats such as identity fraud and cyberattacks continue to evolve fast. In response, a fully integrated approach to border management system design is now a baseline requirement. The good news for authorities is that the latest wave of joined-up solutions is bringing people as well as technologies closer together - fostering the multi-stakeholder collaboration that is ultimately key to maintaining the integrity of national borders.

---

Yann Tréméac leads the Border Control segment at Thales Cybersecurity and Digital.

His teams work closely with clients, partners, and system integrators to meet the growing demand for advanced biometric and identity document verification technologies that improve border management

With over 20 years of experience, he accumulates deep understanding of border control, biometrics, document verification, and cybersecurity.

---



By Tony Smith CBE,  
chairman of IBMATA and  
former Head of UK Border Force

# Future Borders: Officers or Technology

Having worked “on the line” on border control for many years, I know full well the value of interaction between officers and passengers to assess risk. When you’ve been out there for long enough, you know instinctively whether the passenger in front of you is good to go - or whether there is something about them that suggests a further examination is called for. This may be in the document presented. Or the body language, or the appearance. Or even style of answering questions rather than the actual answers given. Some officers called it a “sixth sense”. Something that managers who never worked on the line often saw as some form of defect, or unconscious bias. But it was there – and many of our best catches were “clean skins” who had valid travel documents and did not appear on any watch lists. So it was inevitable that many of us viewed new technology with some suspicion. Was there any real substitute for “face to face” interviews, we wondered?

Whilst serving as an Assistant Director at Heathrow Airport in 1998 – with overall responsibility for passport controls at Terminals One and Two – I was invited by the UK Home Office Technology Team to participate in trials for new “iris gates”. The idea was to invite regular travellers to register their passport and immigration details with us prior to travel, and to voluntarily have their iris scanned. In return



they were promised that they would not need to queue up to be physically examined by an immigration officer anymore. They could instead use a special lane where they would look into a camera, and the machine would recognise their iris without any need to see their passport. Then off they would march to the baggage hall smiling, whilst other passengers queuing up to see immigration officers looked on with envy.

The Iris trials were ahead of their time, and the business case for them was compelling. On one hand officers could spend more time examining “more difficult” cases without wasting time on “low risk” passengers. On the other hand, the government could save money by replacing officers with machines. For the traveller this was a “win-win” because it meant they could pass through arrivals controls more quickly. (Assuming the technology

worked, that is).

Whilst technicians spent a lot of time and research on developing these gates, they lacked the professional knowledge and experience of those of us who spent many years “on the line” physically examining passengers and their travel documents. We all knew that the configuration of the arrivals hall at Terminal 2 meant that on a sunny day you would face the full glare of the sun in your face on an early shift. Even to the extent why some officers were chastised for wearing sunglasses on the control in the mornings. We also knew that passengers would often refuse to stand in front of our desks but would often creep round behind us. Particularly family groups with children. Of course, the technicians weren’t aware of such things. This is what prompted me to build communication channels between border agencies and technology

providers, one of the cornerstones of the IBMATA model.

As soon as the iris gates went live, we discovered that the cameras could not cope with bright sunlight in the mornings. The machines broke down regularly. To get them going again we had to “reboot” the entire system (remember that?) – a process that could take up to twenty minutes. Meanwhile disgruntled passengers looked on, not knowing whether to wait in line or to try to push in to the front of the manual control queues, on grounds that their “registered” status somehow entitled them to do so.

I was told that my staffing budget would be cut, because I needed less officers on the control and the gates could take over. But it soon became clear that the gates could not tell the difference between a bag and a child; so, passengers with children could use the gate themselves and bring through a child through without any checks or questions about status. A veritable haven for child traffickers. Lessons well learnt.

Fast forward 25 years, and most passengers now expect to be able to use some form of automated border control on arrival. Biometrically enabled passports mean that identity can be verified quickly by using facial recognition technology to match the live image to the passport chip. Entitlement to enter is increasingly being established by pre-travel online applications and digital permissions, without any “face to face” interviews by officers. More advanced countries are now looking for “biometric corridors” where passengers don’t even need to stop at all. They simply “walk-through” the border whilst a series of high-resolution cameras capture their faces for instant matching to expected arrivals.

So, is this the new “border control”? If we have universal e visa and ETA systems to capture biometrics and conduct risk assessments before entry,

then we don’t need any officers at the ports anymore – technology can do it all for us. Right?

Wrong. The race between law enforcement and organised crime goes on. For every step forward taken by law enforcement to invest in new technology, smugglers and traffickers step up in line to find ways to defeat us. The power of facial recognition to verify identity was brought home to us last year when we took several IBMATA experts to a meeting with EU LISA in Tallin, only to be shamed in a quiz about identifying imposters who were using deep fake AI technology to defeat border controls. Clearly technology is far better than the human eye in matching faces to photographs; but it isn’t perfect. It doesn’t have a “sixth sense” like we did.

Meanwhile, online assessments for granting permission to enter mean a total reliance upon data submitted and self-declared by applicants. Much of which cannot be independently verified. Whilst the vast majority of travellers are open and honest in the process, a significant minority are not.

We have yet to identify any technology that looks into the mind of a passenger to verify their intent. Our friends at Interpol and the UN work hard to establish global watch lists to help us identify criminals and terrorists – but their data is only as good as the data provided to them by law enforcement. So, it remains highly likely that some passengers are crossing our borders every day having concealed material facts or provided false representations from us to do so. This risk is significantly higher when dealing with irregular and inadequately documented arrivals, where we have no independent record of nationality or identity to match against – let alone travel history and other key ingredients needed to conduct effective risk management.

We live in a different world to the one we occupied in 1998, when those

first iris gates were installed. Now the talk is all about biometrics, data analytics, behavioural analysis and artificial intelligence.

We communicate more by digital platforms than by speaking face to face. Increasingly, we store and share more information about ourselves on Facebook, Instagram, X, Messenger, Tik Tok and so on whilst at the same time worrying about privacy and data protection. Most of this material is in the public domain, and our IBMATA members are developing some excellent tools to make best use of this in supporting our risk management capabilities.

But at the end of the day, the war between law enforcement and criminality will go on. It comes down to good guys stopping bad guys from doing bad things and bringing in bad stuff. That’s why we owe it to ourselves not only to invest in the very best technology to manage our borders; but also to support the next generation of border officers and ensure we keep them where they belong – at the border.

---

IBMATA is chaired by leading border management expert Tony Smith CBE, a former head of the UK Border Force. During his 40-year career, Tony served as Gold Commander for the London 2012 Olympic and Paralympic programme, which saw three million athletes, coaches, spectators and officials processed at the UK border for the competition on top of business as usual. He also served as Regional Director for London and the South East in the UK Border agency, Head of Border Control in the UK Immigration Service and Head of Ports and Border Management in Citizenship and Immigration Canada. Tony was awarded the CBE in 2013 for services to the safety and security of London 2012. After retiring from public service, he became Managing Director of Fortinus Global Ltd.

---

# JOIN THE GROWING IBMATA FAMILY



## Who can join?

### Supplier and Transportation Companies

- Transportation companies (including airlines, shipping companies, rail operators, freight forwarders) with a legitimate interest in supporting our aim;
- Port, airport, and other management entities with a legitimate interest in supporting our aim; and
- Those technology suppliers, business integrators and other private sector entities who, in the opinion of the Board, support the safe and secure movement of people and goods across international borders whilst facilitating flow, in accordance with the aims of the organisation.

### Public Sector Organisations and Academics

- All Government Departments and Agencies charged with the responsibility of managing the international movement of people, goods and materials across national borders; including pre-entry, on-entry and after entry applications;
- Intergovernmental organisations with a vested interest in the management of people and goods across international borders;
- Non-governmental organisations with a vested interest in the management of people and goods across international borders and legitimate academic organisations and research facilities.



## GET IN TOUCH

Email: [info@ibmata.org](mailto:info@ibmata.org)

[www.IBMATA.org](http://www.IBMATA.org)



[twitter.com/border\\_mgmt](https://twitter.com/border_mgmt)



[linkedin.com/company/ibmata/](https://linkedin.com/company/ibmata/)