



UPDATE TO THE CTU

Strengthening Cyber Resilience in the Regional Postal and Logistics Sector

**September 2026
Cayenne, French Guiana**

**Tracy Hackshaw
Head, .POST Business Management Unit | UPU Cyber Resilience Programme
Postal Technology Centre
Universal Postal Union**



Speaking from the UPU headquarters in Bern, SG Rodney Taylor stated, "The partnership between CTU and UPU will be a crucial element in promoting digital transformation and e-commerce in the Caribbean region. We believe that the deployment of the UPU's initiatives will greatly benefit the citizens and businesses in the region."



A STRONGER, MORE CONNECTED CARIBBEAN

Secure Digital Infrastructure for People, Parcels and Prosperity

CONNECTING OUR ISLANDS AND COASTS TO GLOBAL OPPORTUNITIES



PEOPLE. PARCELS. PROSPERITY.

A RESILIENT CARIBBEAN FOR A BRIGHTER TOMORROW.



PEOPLE

Stronger, more connected communities



POSTAL & LOGISTICS

Reliable delivery everywhere



E-COMMERCE

More opportunities for businesses and citizens



CYBERSECURITY

A safer, more resilient Caribbean



ECONOMIC GROWTH

A more prosperous and inclusive region



CYBER RESILIENCE



REGIONAL COLLABORATION



SUSTAINABLE DEVELOPMENT



GLOBAL CONNECTIONS

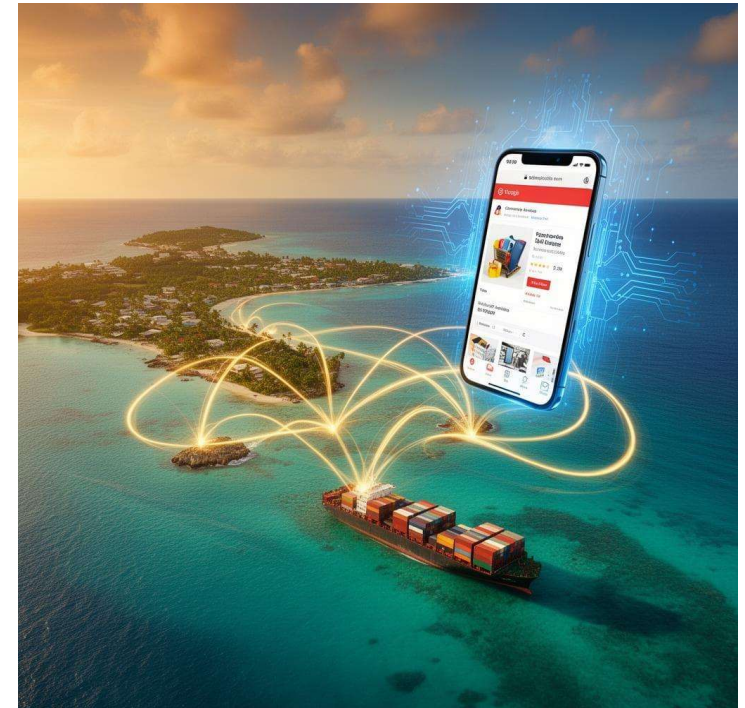
A SECURE CARIBBEAN
DELIVERS OPPORTUNITIES



Why Cybersecurity Matters to Caribbean Postal & e-Commerce Logistics

Cyber risk is now a business-continuity, trust and economic-development issue

- Postal operators are no longer only moving physical items — they increasingly depend on digital platforms, data, customs interfaces, tracking, payments and e-commerce systems.
- The UPU notes that attacks can disrupt international operations, expose sensitive personal data and erode customer trust — directly affecting the role of Posts as e-commerce delivery partners.
- The Caribbean is accelerating digital transformation, while regional cybersecurity capacity and incident-response capabilities remain uneven.
- For small island economies, a significant cyber incident can have an outsized effect because critical services, suppliers and connectivity are often concentrated in a small number of organisations and systems.



Sources: UPU, "A strong digital post starts with a secure digital postal network" (2025); ITU, Global Cybersecurity Index 2024; CARICOM, Updated Cyber Security and Cybercrime Action Plan (2025).



Where the Risk Materialises Across the Caribbean Value Chain

CUSTOMER & DATA

- Personal data
- Identity fraud
- Account takeover
- Phishing

POSTAL OPERATIONS

- Ransomware
- System outages
- IT/OT disruption
- Service interruption

E-COMMERCE & PAYMENTS

- Payment fraud
- Website compromise
- Credential theft
- Loss of customer trust

SUPPLY CHAIN

- Third-party risk
- Customs/data interfaces
- Cloud & SaaS dependencies
- Cross-border disruption

Sources: UPU Cybersecurity Framework (domain hijacking, phishing and spoofing as leading causes of breaches/fraud); UPU E-Commerce Guide; UPU/IGF 2025 cyber-resilience discussions.



Why a Regional Cyber-Resilience Approach Makes Sense

The objective is not simply prevention — it is the ability to anticipate, withstand, respond and recover

- Cross-border postal and logistics networks mean that cyber risk does not stop at national borders.
- CARICOM's updated 2025 Cyber Security and Cybercrime Action Plan explicitly strengthens regional cooperation and adds Incident Response as a strategic pillar.
- The ITU's 2024 Global Cybersecurity Index identifies continuing gaps in skills, staffing, equipment and funding across countries and regions.
- For Caribbean Posts and logistics providers, practical priorities include: baseline cyber hygiene; staff awareness; incident-response plans and exercises; protection of domains/email; third-party risk management; and trusted threat-information sharing.
- The UPU's .POST, SECURE.POST and POST-ISAC initiatives provide sector-specific mechanisms that can complement national and regional cybersecurity programmes.



Sources: CARICOM CCSCAP 2025; ITU Global Cybersecurity Index 2024; UPU Cybersecurity Framework; UPU POST-ISAC launch (23 June 2026).



AI Is Changing the Cyber Threat — Not Just Creating New Threats

The near-term concern is acceleration, scale and lower barriers to existing attack techniques

- AI is already being used to improve reconnaissance, phishing/social engineering, coding, vulnerability research and processing of stolen data.
- AI-generated or AI-assisted phishing can be more convincing, personalised and scalable — particularly relevant to postal customers, employees, suppliers and e-commerce merchants.
- AI-assisted vulnerability research can shorten the window between vulnerability disclosure and exploitation, increasing pressure on organisations that operate legacy or unpatched systems.
- AI-enabled automation lowers the technical barrier for less-skilled actors and expands the pool of potential attackers.
- Importantly, while the UK NCSC assesses that fully autonomous end-to-end advanced cyber attacks are unlikely in the near term; **human-machine teaming is the more immediate concern.**

Sources: UK NCSC, Impact of AI on cyber threat now to 2027 (2025); ENISA Threat Landscape 2025; European Commission, Advanced AI & Cybersecurity Plan (7 Jul 2026).





What This Means for Postal & E-Commerce Logistics

AI can attack the digital layer behind the physical movement of goods

IDENTITY & TRUST

- AI-enhanced phishing
- Deepfake impersonation
- Account takeover

TRANSACTION LAYER

- Payment fraud
- Fake orders / listings
- API abuse & bot activity

LOGISTICS LAYER

- Compromised broker/carrier accounts
- Fraudulent routing
- Tracking manipulation

SUPPLY CHAIN

- Vulnerability exploitation
- Third-party compromise
- AI-enabled reconnaissance

Example: FBI IC3 Public Service Announcement (30 Apr 2026) documents cyber-enabled cargo theft using compromised broker/carrier accounts, spoofed email/URLs and fraudulent load listings. Akamai (2026) reports commerce as a major target for AI-bot activity, SaaS, web/API attacks and botnet.



AI + Critical Infrastructure: The Wider Global Warning

Examples show how cyber disruption can propagate through essential services and supply chains

- Critical infrastructure is increasingly interconnected. ENISA warns that attacks exploiting digital dependencies can create ripple effects across supply chains.
- 2026: CISA/FBI and partners reported state-affiliated actors targeting programmable logic controllers (PLCs) used in US critical infrastructure — illustrating the continuing exposure of operational technology.
- 2025–26: La Poste Groupe disclosed an unprecedented-scale DDoS attack against its services; continuity of parcel delivery and payment services had to be actively protected.
- 2025: ENISA identified AI as a growing factor in phishing and social engineering, while also highlighting attacks against AI supply chains and increasing cyber dependency abuse.
- Strategic implication for the Caribbean: AI increases the speed and scale of threats against the digital systems that connect Posts, ports, customs, payment providers, telecoms, cloud services and e-commerce platforms.



Sources: CISA/FBI/EPA, Advisory on PLC targeting of US critical infrastructure (22 Jul 2026); La Poste Groupe, cyberattack interview (22 Jan 2026); ENISA Threat Landscape 2025; UK NCSC AI Cyber Threat Assessment.



Why This Matters for Caribbean & SIDS Critical Infrastructure

The same characteristics that make digitalisation valuable can amplify the impact of cyber disruption

CONCENTRATION OF DEPENDENCIES

Many SIDS depend on a limited number of telecom, submarine-cable, cloud, energy and service providers. A single disruption can therefore have disproportionate effects.

LIMITED REDUNDANCY & CAPACITY

Small markets and geographic isolation can mean fewer technical resources, specialist personnel and alternative routes for maintaining essential services.

CROSS-SECTOR CASCADE

Postal, banking, payments, ports, customs, telecoms, government and e-commerce increasingly depend on interconnected digital systems.

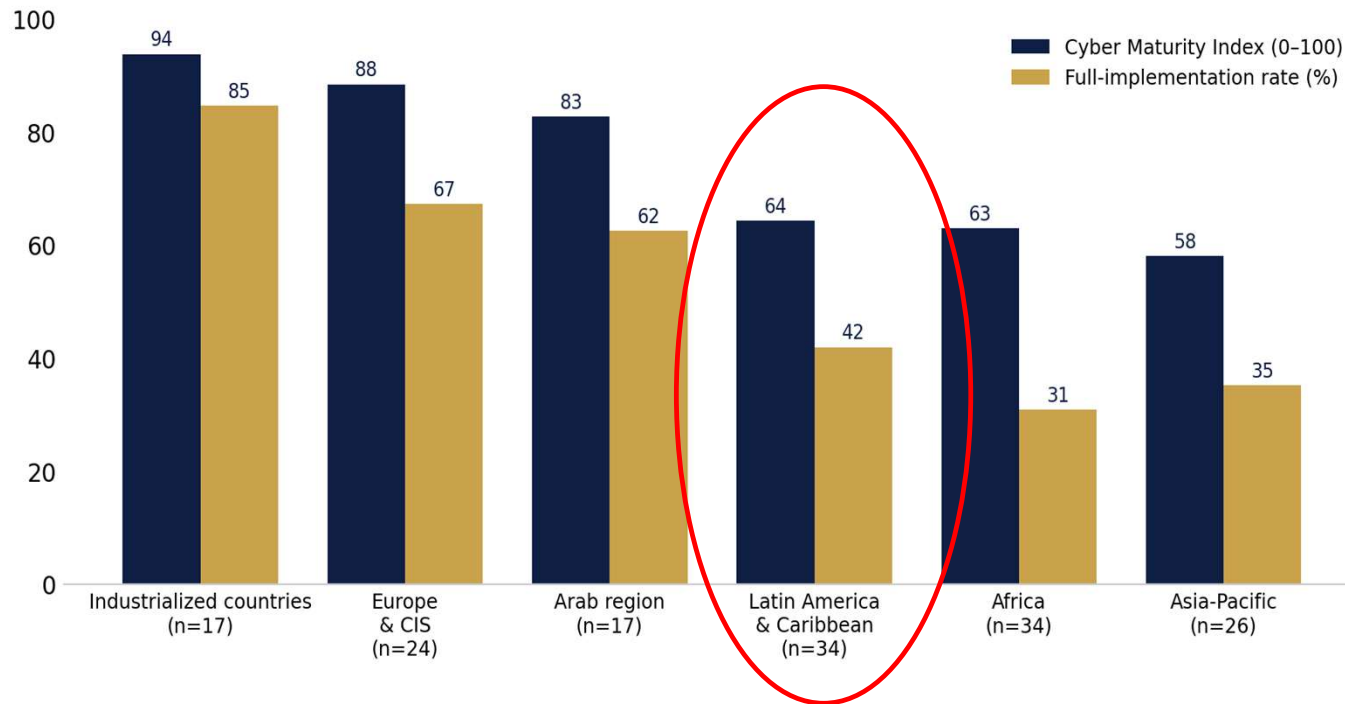
AI ACCELERATES THE RISK

AI can increase the speed, scale and sophistication of phishing, reconnaissance, fraud and vulnerability exploitation — reducing the time available to detect and respond.

Sources: CARICOM, Cyber Resilience Strategy 2030; CARICOM CCSCAP 2025; ITU, SIDS Connectivity (2024) and Submarine Cable Resilience Report (2026). ITU notes particular dependence of SIDS on a small number of cable systems.



Analysis by 6-region view



READ

Development tiers separate cleanly.

Industrialized countries (CMI 94, 85% implemented) and Europe & CIS (88) lead; the Arab region (83) sits mid-pack; Africa (63) and Asia-Pacific (58) anchor the bottom.

The analytical scheme sharpens the same ranking the governance scheme shows — the ordering by region signals the link between cyber maturity and postal development.

Source: UPU Cybersecurity 2024 Survey (152 member responses). Regional cuts use the six-region analytical scheme. Analysis: Pharand Advisors.



■ POST SIDS & LDCs Starter Package

Grenada Postal Corporation	Pending
BVI Post	Pending
Jamaica Post and Telecommunications Department	Pending
Bahamas Post Office	Approved, Implementing
Guyana Post Office Corporation	Approved, Implementing
SVG Postal Corporation	Approved, Implementing
Trinidad and Tobago Postal Corporation	Awaiting feedback
Postal Services Turk And Caicos Islands	Approved, Implementing
Belize Postal Service	Approved, Implementing
Anguilla Postal Service	Awaiting feedback
Saint Lucia Postal Service	Approved, implementing
Suriname Postal Corporation	Awaiting feedback





Delivered so far

8

national posts built on one
codebase

6

storefronts live, all available
for testing and deployment

100%

security score
on TEST.SECURE.POST

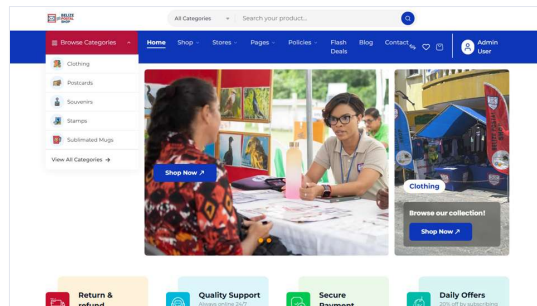
2

national banks engaged on
payments

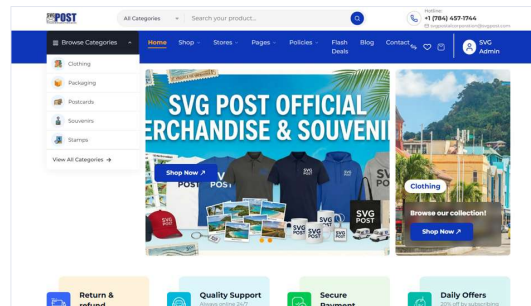


Live and ready to deploy - Today

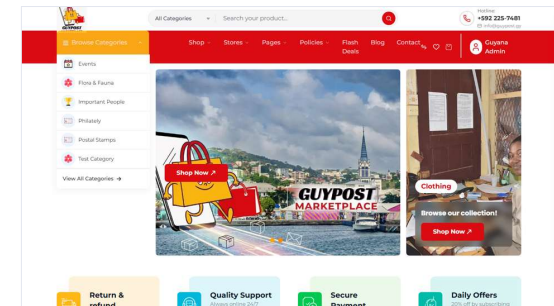
Six national storefronts, already running



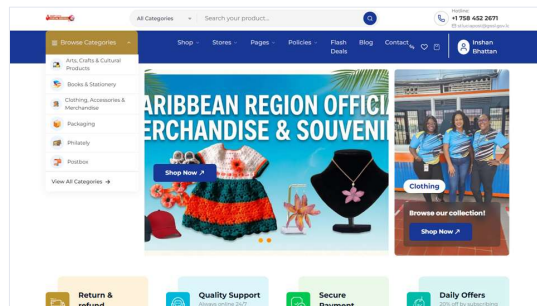
Belize
Bank-certified



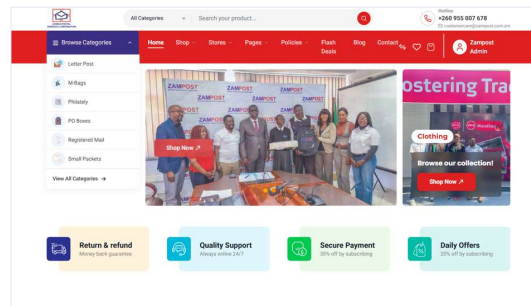
Saint Vincent
Payments integrating



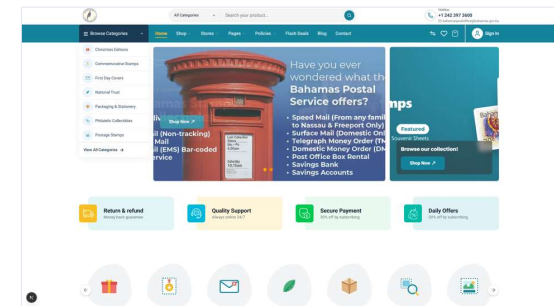
Guyana
Built and branded



Saint Lucia
Staged for review



Zambia — Makweb
Beyond the Caribbean



The Bahamas
Hosted, in live testing



The Foundation

Trust is built into the address itself



Vetted, not claimed

Every .POST address is verified before it is issued, so a shopper knows a store genuinely belongs to their national post.



Sponsored by the UPU

.POST is the sector's own top-level domain, sponsored by the United Nations' Universal Postal Union.



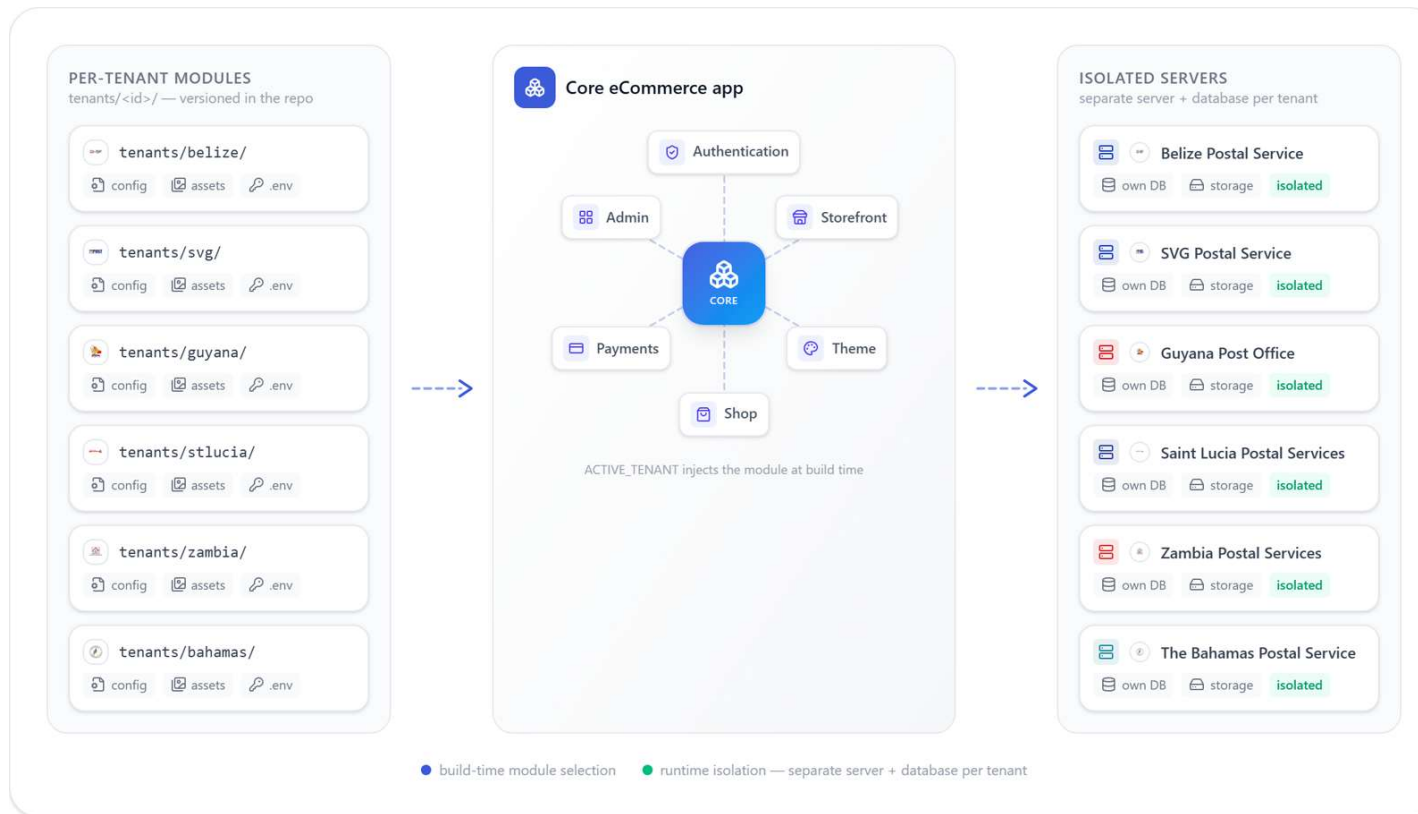
Secure by default

DNSSEC-signed domains, TLS 1.3 encryption and authorised routing on every deployment.



The Delivery Model

One codebase. A dedicated, isolated deployment per post.





Current Status

Eight posts built, each moving forward

Postal service	Where it stands
Belize Postal Service	Bank-certified, credentials issued
SVG Postal Service	Payment integration under way
Guyana Post Office	Built and branded, in review
Saint Lucia Postal Services	Staged for review
The Bahamas Postal Service	Domain hosted, in live testing
Turks & Caicos Islands Post	Staged for content review
Zambia — Makwebo	Newest member, in review
Tuvalu Post	Staged for content review



Coming up

What opens the network to the public

Next step	Who	Unlocks
Sensitization session	Belize team	Belize goes live to the public
Complete API integration	SVG Post	Second country taking card payments
Public launch	Bahamas Post	Sixth live storefront opens
Complete content review	Guyana, Saint Lucia, Zambia, Tuvalu, Turks & Caicos	Five more catalogues open for trade



APPLY NOW : .POST SIDS & LDCs Starter Package



SECURE **6** POST

• **POST**
SECURING your trusted
DIGITAL SPACE



POST-ISAC Pilot Onboarding

- UPU has officially launched the POST-ISAC pilot onboarding initiative on 23 June 2026.
- Early engagement opportunity with this vital project
- Pilot participants will help shape POST-ISAC's development
- Benefits include enhanced situational awareness, improved security posture, and strengthened cyber resilience.
- Access to timely threat information, and collaboration opportunities.
- Contact us today at [hello \[at\] trust \[dot\] post](mailto:hello@trust.post)

Your participation in the pilot will be instrumental in demonstrating the value and impact of this critical undertaking.



A Trusted Digital Space for the postal and logistics sector. The UPU-sponsored .POST Top Level Domain and its accompanying Shared Services Platform is intended to increase the security of postal digital services and serve as a digital trust infrastructure for the sector.



SECURE.POST: The Cybersecurity Awareness Portal for the global postal and logistics sector. This online portal will serve as a central gateway to cybersecurity and cyberhygiene awareness, sensitisation, and training resources for postal and logistics organisations worldwide.



The UPU has established a cybersecurity framework that includes recommended .POST Security policies aimed at reducing common cyber threats such as domain hijacking, phishing, and spoofing.



SECURE  POST

POST-ISAC
A SECURE SPACE FOR THE POSTAL SECTOR



HOW YOU CAN HELP

We strongly encourage your organisation to seize this opportunity and join our pilot onboarding initiative for the POST-ISAC scheduled to commence in 2025. Your active participation will be invaluable in shaping the future of cybersecurity collaboration within the postal and logistics sector, contributing to a safer and more secure global network.

We would be delighted to provide you with further information on our other cybersecurity initiatives, including the .POST Top Level Domain, the .POST Shared Services Platform, SECURE.POST and the UPU .POST Cybersecurity Framework.

We believe that by working together, we can significantly enhance the cyber resilience of the global postal and logistics sector and ensure the continued delivery of essential services in the face of evolving cyber threats.

We look forward to your active engagement in these critical endeavours.

Scan to join:



UPU | UNIVERSAL
POSTAL
UNION

Postal Technology Centre
.POST Business Management Unit
International Bureau
Weltpoststrasse 4
3015 BERNE
SWITZERLAND

email: [hello \[at\] trust \[dot\] post](mailto:hello@trust.dot.post)
website: <https://isac.post>



SECURE .POST

POST-ISAC
A SECURE SPACE FOR THE POSTAL SECTOR



UPDATE TO THE CTU

Strengthening Cyber Resilience in the Global Postal and Logistics Sector

**September 2026
Cayenne, French Guiana**

**Tracy Hackshaw
Head, .POST Business Management Unit | UPU Cyber Resilience Programme
Postal Technology Centre
Universal Postal Union**

A STRONGER, MORE CONNECTED CARIBBEAN

Secure Digital Infrastructure for People, Parcels and Prosperity

CONNECTING OUR ISLANDS AND COASTS TO GLOBAL OPPORTUNITIES

PEOPLE. PARCELS. PROSPERITY.

A RESILIENT CARIBBEAN FOR A BRIGHTER TOMORROW.



PEOPLE

Stronger, more connected communities



POSTAL & LOGISTICS

Reliable delivery everywhere



E-COMMERCE

More opportunities for businesses and citizens



CYBERSECURITY

A safer, more resilient Caribbean



ECONOMIC GROWTH

A more prosperous and inclusive region



To Europe and Africa

To North America and the World



CYBER RESILIENCE



REGIONAL COLLABORATION



SUSTAINABLE DEVELOPMENT



GLOBAL CONNECTIONS

A SECURE CARIBBEAN
DELIVERS OPPORTUNITIES