

NCIT 2026



Trust in the Digital Age

Cybersecurity, Sovereignty and Pacific Resilience

Sagar Patel

Head of Cybersecurity Solutions & Architecture

 sagar.patel@datec.com.fj

Datec Fiji Pte Limited  www.datec.com.fj

*A Fiji-first perspective on securing our digital future
→ with lessons for the Pacific.*



Fiji is now a digital nation ➡ with digital risks to match.



2026

STRATEGY LAUNCH

Fiji National Cybersecurity and Resilience Strategy 2026–2031.



1st

IN THE PACIFIC

First Pacific nation to sign the Budapest Convention's Second Additional Protocol ➡ a signal of intent.



~85.2%

FIJIANS ONLINE

Fiji has one of the highest internet penetration rates in the Pacific ➡ with Facebook the de-facto public square.

Ref: Fiji National Digital Strategy 25-26



24×7

ATTACK SURFACE

Fiji's banks, telcos, ministries and utilities are targets ➡ every hour, every day, from every geography.

Cybersecurity is now a national interest ➡ as consequential to Fiji as our fisheries, our tourism, and our currency.



FIJI CERT: STRENGTHENING NATIONAL CYBER RESILIENCE

Building a secure digital Fiji for government, businesses and citizens.



✓ WHAT IS ALREADY WORKING

✓ **Website live at cyber.gov.fj**
Central hub for guidance, alerts and resources.

✓ **Incident reporting available**
Easy channels for reporting cyber incidents.

✓ **Cyber hygiene guidance**
Practical advice and best practices for all users.

✓ **Public threat alerts**
Timely advisories on threats and vulnerabilities.



FIJI CERT

[CYBER.GOV.FJ](https://cyber.gov.fj)

DIGITAL FIRST RESPONDER FOR FIJI



5.5 – 6.5 / 10

CONTINUOUS CAPABILITY ENHANCEMENT



Strengthening national cyber resilience through continuous improvement.

⚙️ WORK PROGRESSING UNDER NCRS

1 **Continuous Monitoring of Critical Infrastructure (CI)**
Enhanced visibility, monitoring and protection of critical national services.

2 **Critical Information Infrastructure Framework**
Formal CII designation, reporting mechanisms and sector guidance.

3 **Threat Intelligence Sharing**
Collect, analyse and share threat intelligence nationally and regionally.

4 **Public-Private Sector Trust**
Stronger collaboration and trusted information sharing with industry.

5 **Skilled Resources**
Build and retain cybersecurity talent to strengthen national resilience.



GOVERNMENT

BUSINESSES

CITIZENS

RESILIENCE

FIJI CERT IS OPERATIONAL.
CONTINUED NCRS IMPLEMENTATION
WILL FURTHER ENHANCE NATIONAL



<https://www.cyber.gov.fj/uploads/resources/fncrs.pdf>

Digital trust is engineered, not assumed.

For Fiji, trust must be culturally rooted and technically enforced.

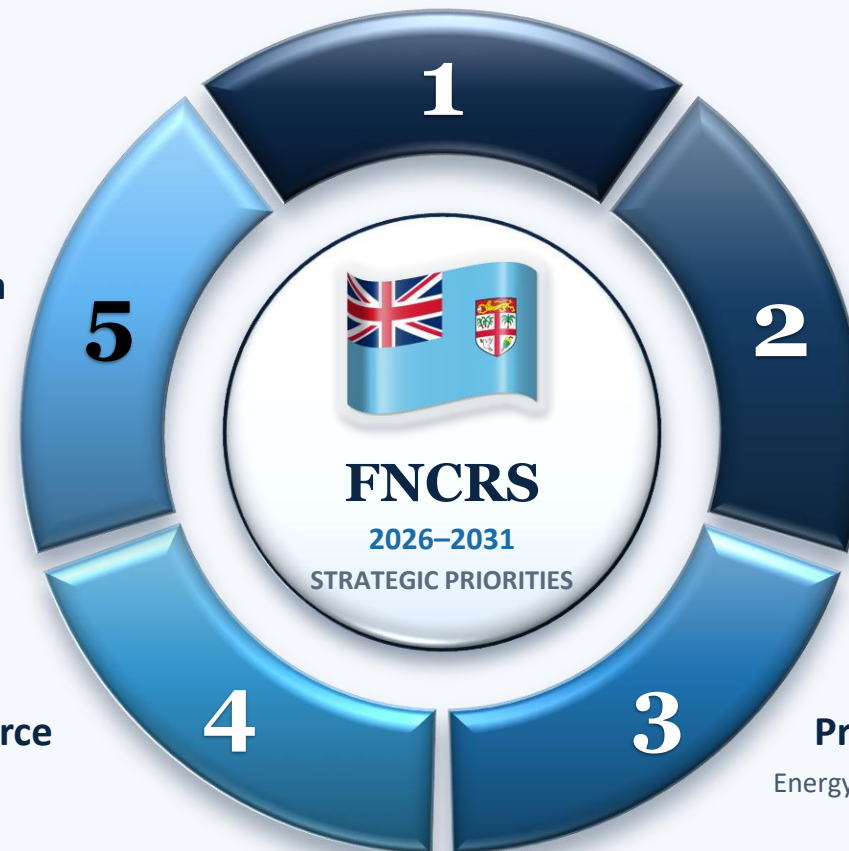


Fiji National Cybersecurity & Resilience Strategy 2026–2031.

The Strategy's five strategic priorities, anchored by the Cyber Affairs Unit, cyber.gov.fj and a national Action Plan with clear delivery owners.

Cyber-secure & Cyber-Aware Fijians & Businesses

A national culture of cyber hygiene ➡ citizens, MSMEs and enterprise.



Robust Incident & Cybercrime Response

National CERT capability; Cybercrime Act 2021, and Budapest 2AP enforced.

Protect Government, CI/CII, Data & Assets

Energy, finance, health, telco and aviation systems safeguarded.

Skilled, Talented & Diverse Cyber Workforce

FNU/USP pipeline; women in cyber; board-level literacy.

What Fiji industry must deliver.

Five national priorities. Five industry commitments — what Fiji's technology sector must put on the table.

MAPPED 1:1 TO THE FIVE STRATEGIC PRIORITIES · FNCRS 2026–2031

1

Cyber-Secure & Cyber-Aware Fijians

Cyber-hygiene programmes for MSMEs, phishing simulation and Fijian-language awareness campaigns at scale.

2

Robust Incident & Cybercrime Response

Sovereign 24x7 SOC/NOC run from Fiji, tested IR retainers and evidence-grade forensics supporting the national CERT.

3

Protect Government, CI/CII, Data & Assets

Zero-Trust, managed EDR/XDR and immutable backup as standard — plus sector playbooks for RBF, TAF, EFL and MHMS.

4

Skilled, Talented & Diverse Cyber Workforce

FNU/USP/Private Academy internships, SOC apprenticeships, women-in-cyber pathways and board-level literacy.

5

Cyber Leadership & International Cooperation

Board-ready GRC dashboards mapped to ISO 27001 and NIST CSF 2.0, plus twice-yearly national tabletops.

TAKEAWAY ➡ Government sets the priorities and industry must deliver the capability, built in Fiji, for Fiji.

When Fiji speaks, the Pacific listens.

Our national cyber diplomacy is punching above our weight ➡ and it protects Fiji interests at every table.



If it stops, Fiji stops.

Six sectors that must be protected as national assets — with named operators and mapped regulators.



Submarine Cables

*Southern Cross NEXT
· Tonga Cable · Tui-Samoa*

RISK Single-cable dependence; landing station security; repair-vessel scarcity.

ACTION Diverse routes; new 2nd landing station at Natadola (Google) for redundancy; national cable resilience plan.



Energy & Utilities

*Energy Fiji Ltd (EFL)
· Water Authority of Fiji*

RISK Legacy SCADA, OT/IT convergence, imported firmware, insider risk.

ACTION Air-gapped OT, IEC 62443, sector CERT, monitored PLC baselines.



Finance & Banking

*RBF · BSP · ANZ · Westpac
· HFC · FNPf · FRCS*

RISK SWIFT, ATM, RTGS, mobile-money fraud, KYC/AML pressure.

ACTION Regulator-mandated MFA, transaction anomaly AI, joint fraud hub.



Health

*MHMS · CWM · Lautoka
· Labasa Hospitals*

RISK EMR ransomware, medical device exposure, low IT maturity.

ACTION Immutable backup, network segmentation, sector MDR, DR playbooks.



Aviation & Ports

*CAAF · AFL · Fiji Airways
· Fiji Ports · FRCS Customs*

RISK GPS spoofing, ATC systems, port terminal OT, cargo systems.

ACTION ICAO cyber annex, tabletop exercises, secure comms hardening.



Government & e-Gov

*digitalFIJI · ITC Services
· cyber.gov.fj · FRA · FRCS*

RISK Identity theft, service impersonation, cloud misconfiguration.

ACTION National digital ID, Zero Trust for e-services, sovereign cloud landing zones.

The battle for trust is being fought on our timelines.

Between coconut wireless and Facebook feeds, false narratives now travel faster than truth — with real consequences for Fiji's civic life.



The Fiji threat landscape

- ▶ **Misinformation** during major public events and national decisions ➡ coordinated inauthentic behaviour online.
- ▶ **Health misinformation** ➡ false claims that spread quickly during health emergencies (e.g. COVID-19).
- ▶ **Deepfakes and synthetic media** of public figures and celebrities ➡ cheap to produce, expensive to disprove.
- ▶ **SMS & Messenger scams** targeting elderly citizens and diaspora remittances.
- ▶ **Cross-border narrative campaigns** reaching Fiji via global and regional platforms..
- ▶ **Online harms and hate speech** ➡ amplified by algorithmic reach.



A Fiji defence playbook

- ✓ **Digital literacy at scale** Cyber hygiene in schools & TVET — in English, iTaukei and Fiji-Hindi.
- ✓ **Cultural anchors first** Talanoa-based fact-checking; trusted community voices lead, tech follows.
- ✓ **Platform accountability** Standing engagement with Meta, TikTok, Google & X on takedown SLAs for Fiji.
- ✓ **Regulatory guardrails** Modernise the Online Safety Act — balance safety with civic free expression.
- ✓ **Provenance technology** C2PA content credentials & verified accounts for government & accredited media channels.

No government secures the digital nation alone.

Fiji cyber is a team sport ➡ with named players on the field, not just watching from the sidelines.



SHARE THREATS · SHARE PLAYBOOKS · SHARE PEOPLE · SHARE COST · KEEP FIJI SOVEREIGN

Sovereignty in cyberspace is not a slogan ➡ it is stack, staff and statute.



STACK *The Technology*

- ▶ Sovereign or aligned cloud landing zones ➡ incl. Google's Natadola ICT facility ➡ with Fiji data residency.
- ▶ National digital ID under digitalFIJI ➡ one strong identity, many services.
- ▶ Encrypted-by-default, backup-by-default, log-by-default for government workloads.
- ▶ Open standards ➡ avoid single-vendor lock-in on national infrastructure.



STAFF *The People*

- ▶ Fiji cyber workforce plan ➡ 500 certified professionals by 2030.
- ▶ Awareness in vernacular ➡ English, iTaukei and Fiji-Hindi content at every level.
- ▶ Diaspora bridge ➡ engage Fijian cyber talent in AU / NZ / US.
- ▶ Women in cyber ➡ deliberate pipeline via FNU and TVET, not aspiration.



STATUTE *The Law*

- ▶ Modernised Cybercrime Act aligned to the Budapest Convention (2AP) and the UN Cybercrime Convention.
- ▶ Fiji Data Protection & Privacy law with cross-border transfer provisions.
- ▶ Critical Infrastructure incident reporting to Fiji CERT.
- ▶ Judicial capacity ➡ trained magistrates and prosecutors for cyber cases.

Our values are the foundation of our defence.



FIJI VALUES *Vanua · Solesolevaki · Talanoa* *· Kerekere · Vasudhaiva* *Kutumbakam*

- ▶ Vanua ➡ land, people, identity (iTaukei)
- ▶ Solesolevaki ➡ collective action (iTaukei)
- ▶ Talanoa ➡ consensus through dialogue (Pacific)
- ▶ Kerekere ➡ reciprocity & obligation (iTaukei)
- ▶ Vasudhaiva Kutumbakam ➡ one family (Fiji-Hindi tradition)



CYBER TRANSLATION

How values become digital defences

- ▶ Custodial data governance ➡ held in trust, not exploited
- ▶ Community SOC ➡ solesolevaki for cyber defence
- ▶ Encrypted talanoa ➡ secure messaging that preserves dialogue
- ▶ Digital reciprocity ➡ shared threat intelligence
- ▶ One digital family ➡ inclusive design across communities

Fiji Cyber Shield — a 5-layer national resilience model.

Proposed to operationalise the Fiji Strategy 2026–31 — scalable, sequenced, and outcome-driven. Replicable across the Pacific.



The Strategy is already in Uplift — here is how we accelerate it.

01

Sustain the Delivery Momentum

Carry the Uplift phase through to completion ➡ milestones and public trust tracked on cyber.gov.fj.

02

Fiji CERT Progression + Sector CERTs

Fully resource Fiji CERT, plus sector CERTs for finance, telco, energy, health & aviation by 2027.

03

Back the Workforce Pipeline

500 certified Fiji cyber professionals by 2030, 40% women, delivered via FNU / USP / TVET / Similar.

04

Sovereign Cloud & digitalFIJI ID

Enforced Fiji data residency and a national digital ID scaling across every ministry.

05

Protect Truth in the Feed

Modernised Online Safety Act, platform accountability MoUs, and C2PA content credentials for government.

Every figure in this keynote is drawn from primary, official sources.

- 1 National Cybersecurity & Resilience Strategy 2026–2031 (cyber.gov.fj) & National Digital Strategy 2025–2030 (Govt of Fiji, digital.gov.fj)
- 2 Budapest Convention & 2nd Protocol (Fiji first Pacific); UN Cybercrime Convention, signed Dec 2025 — Council of Europe & Fiji Ministry of Foreign Affairs
- 3 Boe Declaration 2018 & Pacific Fusion Centre, Port Vila ➡ Pacific Islands Forum, forumsec.org
- 4 Lagatoi Declaration 2023, Port Moresby ➡ Pacific ICT Ministers' Dialogue (SPREP Library / PNG DICT)
- 5 Internet access ~85% (Govt of Fiji, National Digital Strategy 2025–2030); Google Natadola ICT facility & 2nd cable landing station ➡ Office of the PM, pmoffice.gov.fj

Questions worth answering together.

- Q What must run inside Fiji, and what can safely sit offshore with data residency?
- Q Where will 500 certified Fijian cyber professionals by 2030 come from?
- Q How do we balance the Online Safety Act with civic freedom of expression?

Secure-by-design, built in Fiji for the Pacific.

Helping citizens, businesses, BFSI, government and critical sectors build resilience and sovereignty.

CIVILIANS & COMMUNITIES

Cybersecurity CSR

Community awareness and cyber-hygiene outreach for citizens, schools and MSMEs.

BUSINESSES & MSMEs

Cyber GRC

ISO 27001, NIST CSF 2.0 and board-ready risk, audit and compliance.

BANKS & FINANCIAL SERVICES

Fractional vCIO & vCISO

Executive cyber and ICT leadership without the full-time cost.

GOVERNMENT & e-GOV

CRITICAL INFRASTRUCTURE

Tabletop Exercises

Board, sector and national crisis simulation with tested playbooks.

Comprehensive ICT Assessment

End-to-end architecture, maturity and gap review across the estate.

VAPT

Vulnerability assessment and penetration testing for apps, cloud and networks.

Capacity Building

Skills transfer, training and workforce development through Datec Academy and Training Centre.

DRP & Capacity Planning

Disaster recovery, business continuity and resilience capacity planning.

SNOC 360 Sooner

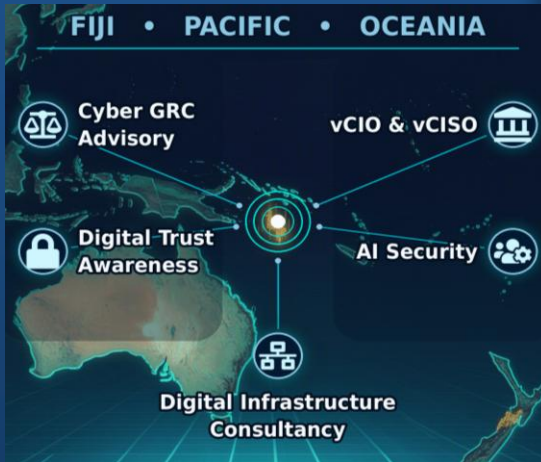
Managed Security & Network Operations Centre

24x7 monitoring, detection and response ➡ operated from Fiji, for Fiji and the Pacific.

SECURE-BY-DESIGN, BUILT IN FOR THE DIGITAL TRANSFORMATION JOURNEY ➡ SOVEREIGNTY AND RESILIENCE

A strong Fiji is a strong Pacific. Let us build the digital nation our people will trust.

**Vinaka Vakalevu.
Dhanyavaad.**



Strengthening Digital Trust



Secure-by-Design Architect

Digital Infrastructure, Zero Trust, SASE, hybrid cloud, and SOC/NOC integration for critical enterprises and infrastructure.



Trusted Advisor

vCISO, GRC & board-level guidance to Fiji CXOs, Boards, and Government.



Practitioner in Fiji and the Pacific

From the Pacific, extended my consultancy services across Fiji and the wider Pacific.



Thought Leadership

- ✓ Member of ISACA, AISA, ACS, CSI, and AICD
- ✓ Member of RSAC CISO under AISA
- ✓ Fractional Leadership ⇒ vCIO, vCISO, Board Advisory

CREDENTIALS

*CISM, CEH, Microsoft Cybersecurity Architect Expert
ACS CP ⇒ CIO | Cyber GRC Advisor | Cyber Security Architect
Microsoft Azure Cloud Solutions Architect Expert
Sophos MDR, Endpoint, and Firewall Architect
Fortinet Network Architect NSE7
CCNP, CCNA – Security, VCP*

AWARDS

*Fusion Factor Hall of Fame 2025 (For service in California, USA)
— SOC, NOC Operations, Secured IT Services, and Digital Transformation*



Sagar Patel

Head of Cybersecurity Solutions & Architecture

 sagar.patel@datec.com.fj

Datec Fiji Pte Limited

 www.datec.com.fj

Find me on  <https://www.linkedin.com/in/sagarkpatel/>



datec

NCIT 2026 | Keynote: Trust in the Digital Age ⇒ Cybersecurity, Sovereignty and Pacific Resilience

