NATIONAL CYBERSECURITY AND RESILIENCE STRATEGY 2026 - 2031

Vision

A cyber-secure, safe and resilient Fiji where all Fijians can benefit from meaningful connectivity and digital transformation

Publication can be accessed online at:

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

Ministry of Policing and Communications

Suva, Fiji

Please consider the environment before printing this report.

TABLE OF CONTENTS

FOREWORD BY THE PRIME MINISTER OF FIJI

It gives me great pride to present Fiji's National Cybersecurity and Resilience Strategy 2026-2031.

We stand at a decisive moment in our cybersecurity journey. As a nation, we are embracing the opportunities of digital transformation: from the increasing use of e-commerce platforms and online banking, to the increased delivery of digital government services and the rise of smart education, healthcare, and connectivity across our islands. But as our reliance on technology and connectivity grows, so too do the risks.

Fiji is not immune to cyber threats that affect our world. The Government of Fiji is concerned by the increasing scale, sophistication and impact of cyber incidents on our country. In this environment, uplifting our cybersecurity and resilience is a national imperative.

This Strategy is a call to action to secure our digital future and safeguard our progress, national security and prosperity. It commits us to act decisively on cyber threats and risks and invest in cybersecurity awareness and capabilities that strengthen our posture.

To reach our ambitions, our efforts rely on partnerships across our society – government, businesses and our communities – to uplift our collective cybersecurity and resilience.

The Strategy is not only about combatting cyber threats, but also about seizing the opportunities from a rapidly growing cybersecurity industry. By fostering interest in cybersecurity careers in our youth, we can ensure that Fiji is the talent hub of cybersecurity professionals in the Pacific.

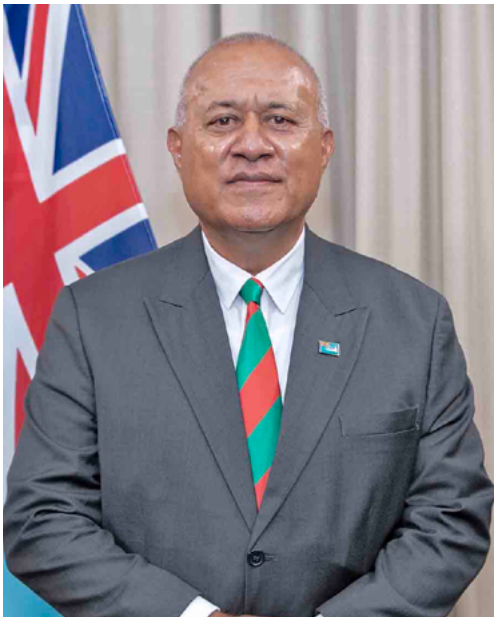
Cybersecurity is a shared challenge that affects our region and the globe. Our efforts in cybersecurity support the Ocean of Peace. As part of our Strategy, we will remain a steadfast advocate for strengthening cybersecurity and resilience across our Pacific family and promoting global rules and norms on peace and security in cyberspace.

This Strategy is bold in its ambition and clear in its purpose: to secure Fiji's digital future, so all Fijians can benefit from meaningful connectivity and digital transformation. By working together to uplift our cybersecurity, we can ensure a stronger, safer and more resilient Fiji for generations to come.

Honourable Sitiveni Ligamamada Rabuka CF, OBE, MSD

Prime Minister & Minister for Civil Service, Strategic Planning, National Development and Statistics

MESSAGE FROM THE MINISTER FOR POLICING AND COMMUNICATIONS



As Fiji continues its digital transformation journey, cybersecurity has become fundamental to our national security, economic resilience, and public trust. Digital technologies now underpin government service delivery, business operations, critical infrastructure and critical information infrastructure, and daily life for our people. With these opportunities come evolving cyber risks that require a coordinated, forward-looking, and resilient national response.

The National Cybersecurity and Resilience Strategy 2026–2031 sets out Fiji's strategic approach to strengthening our national cybersecurity posture and ensuring that our digital future is secure, inclusive, and resilient. The Strategy is guided by five strategic priorities that together provide a comprehensive framework for addressing current and emerging cyber threats.

The first priority is to ensure secure, safe, and cyber-aware Fijians and businesses. Empowering our citizens and enterprises with the knowledge, skills, and tools to navigate the digital environment safely is essential to reducing cyber risks, building trust in digital services, and supporting inclusive economic growth.

The second priority focuses on strong cyber incident and cybercrime response capabilities. As cyber threats grow in scale and sophistication, Fiji must be able to effectively prevent, detect, respond to, and recover from cyber incidents. Strengthening national coordination mechanisms, operational readiness, and law enforcement capabilities is critical to protecting our people and maintaining confidence in our digital ecosystem.

The third priority is the protection of government, critical infrastructure and critical information infrastructure, data, and assets. Safeguarding essential services and sensitive information is vital to national security, public safety, and economic stability. This priority ensures that appropriate safeguards, resilience measures, and risk management practices are embedded across critical sectors.

The fourth priority recognises the importance of a skilled, talented, and diverse cybersecurity workforce. A strong national cybersecurity posture depends on people. Investing in education, training, and professional development will build sustainable local expertise, promote diversity, and ensure Fiji has the talent required to meet present and future cyber challenges.

The fifth priority underscores cybersecurity leadership and global advocacy. Cybersecurity is a global issue that requires international cooperation. Through regional and global engagement, alignment with international norms and conventions, and proactive advocacy, Fiji will contribute to a safe, open, and secure cyberspace while strengthening its own national capabilities.

Together, these five strategic priorities provide a clear and practical roadmap to enhance Fiji's cybersecurity resilience over the next five years. Their successful implementation will strengthen national security, protect our digital assets, support economic development, and reinforce public trust in digital transformation.

I commend all stakeholders who contributed to the development of this Strategy and call upon all sectors to work collectively in its implementation. My special appreciation goes to the Cyber Affairs team within the Ministry and the Director-General for Digital Government Transformation, Cybersecurity and Communications for leading the development of this Strategy. The Cyber Affairs Team will also be responsible for monitoring that the activities planned through this strategy are successfully completed. Equally important is the need for all stakeholders to do our part. Through shared commitment and coordinated action across all stakeholders, we can build a secure, resilient, and trusted digital future for all Fijians.

Honourable Ioane Naivalurua

Minister for Policing and Communications

EXECUTIVE SUMMARY

Cybersecurity touches the lives of all Fijians. A strong cybersecurity and resilience posture is critical for socio-economic growth, sustainable development and national security and resilience; and, for our society to harness the benefits of increasing connectivity, digital infrastructure and technology. Subsea cables, satellite technologies and new and emerging technologies like 5G, Artificial Intelligence (AI), Cloud Computing, Quantum Technologies and Biotechnologies, are transforming how we live, work, connect, access, and contribute to the digital economy.

Fiji is embracing the opportunities of digital transformation to drive inclusive and sustainable development, strengthen economic resilience, enhance border security and defence, and improve public service delivery. However, as Fiji becomes increasingly connected, the cybersecurity landscape becomes more complex and challenging. Greater reliance on digital technologies and services across our society increases risks and the potential for cyber threats and attacks. Malicious cyber actors are targeting government, critical infrastructure (CI) and critical information infrastructure (CII), businesses and individuals. These risks and threats have consequences for Fiji's national security and resilience, economic stability and the safety of our communities.

Fiji's digital future relies on uplifting and strengthening our cybersecurity and resilience. Fiji must act now to strengthen our ability to identify, protect, detect, respond to and recover from cyber threats and secure our digital future. It is not just about protecting Fiji against threats; the need for stronger cybersecurity also presents an opportunity to turbo-charge our ICT and cybersecurity sectors, create new jobs, and promote Fiji as a cybersecurity education and workforce hub in the Pacific.

The National Cybersecurity and Resilience Strategy 2026-2031 (NCRS) is a bold and ambitious framework to uplift and strengthen Fiji's cybersecurity and for our nation to be a cybersecurity leader in our region. The accompanying Action Plan details the initiatives we will implement to reach our vision and deliver on our strategic priorities. This ensures Fiji can take advantage of digital transformation while protecting our socio-economic growth, sustainable development and national security and resilience.

2031 Vision

By 2031, we envisage a cyber-secure, safe and resilient Fiji where all Fijians can benefit from meaningful connectivity and digital transformation.

Strategic Priorities

1. Secure, safe and cyber-aware Fijians and businesses
2. Strong cyber incident and cybercrime response capabilities
3. Protected government, critical infrastructure and critical information infrastructure, data and assets
4. Skilled, talented and diverse cybersecurity workforce
5. Cybersecurity leadership and global advocacy

ROLE OF THE STRATEGY

Guiding the National Strategic Direction

The NCRS is the overarching framework that sets the Government of Fiji's vision for protecting and safeguarding our nation and community in cyberspace. It communicates our intentions, goals and actions we will take at a national and international level to achieve our 2031 Vision.

To this end, we must focus our collective efforts on implementation so we can deliver the best possible outcomes for all Fijians. The accompanying Action Plan details the specific initiatives, timeframes for implementation and lead ministries, agencies and entities responsible for delivery, for effective monitoring and evaluation on the implementation of the NCRS.

Aligning Efforts with National and International Frameworks

The NCRS and Action Plan are aligned with the broader national development priorities outlined in the 7 focus areas and 5 x-factors of the National Development Plan 2025-2029 and Vision 2050. The NCRS aligns with and complements Fiji's sectoral strategies like the National Digital Strategy 2025--2030, the National Security Strategy 2025-2029, the National E-Commerce Strategy 2025-2029, National Privacy and Personal Data Protection Policy 2025 and the Foreign Policy White Paper 2024.

The NCRS aligns with key regional commitments, including the Pacific ICT Ministers' 2023 Lagatoi Declaration and the 2025 Action Plan[i], the 2018 Boe Declaration, and the 2050 Strategy for the Blue Pacific Continent; and international frameworks, such as the UN cumulative and evolving framework for responsible State behaviour in cyberspace, UN Convention against Cybercrime, Council of Europe Budapest Convention and its Protocols, and the 2030 Agenda for Sustainable Development.

Creating a Shared Understanding of Fiji's Cyber Threat Environment

The NCRS identifies key risks and challenges that could affect our economic growth and development, national security and resilience and social wellbeing. The NCRS identifies the global trends shaping the current cyber threat environment, from increasing digitalisation and technology adoption, to risks posed by the rise in cybercrime and cyber as Statecraft. Creating this collective understanding of the risks we face means that Government, critical sectors, businesses and our community have a clear picture about the scale and nature of the challenge, and what we must do to address this as a nation.

Reflecting Diverse Perspectives from Across Fiji

The NCRS and Action Plan were shaped through an inclusive, nationwide consultation process conducted over May and June 2025. The Ministry of Communications acknowledges the participation of over 60 stakeholders from across the Government of Fiji, law enforcement, the private sector, academia and civil society in the development of the NCRS and Action Plan.

The 2031 Vision and Strategic Priorities were guided by the findings and recommendations from Fiji's second Cybersecurity Capacity Maturity Model (CMM) Review completed in December 2024. These inputs ensured efforts to uplift cybersecurity detailed in the NCRS and Action Plan are founded on a robust and strong evidence-base, grounded in local context and realities.

Promoting Accountability, Collaboration and Partnerships

Cybersecurity is a shared responsibility that extends beyond the Government of Fiji; it requires active involvement from the private sector, civil society, academia, technical experts, international partners and our communities. The NCRS and Action Plan promote a whole-of-society approach to achieving our 2031 Vision, in the spirit of accountability, collaboration and partnerships.

Cybersecurity is a shared global challenge that is fundamental to international peace and security. Fiji will continue to deepen our regional, cross-regional and international partnerships to implement the NCRS. With our partners, we will address cyber risks and harness opportunities for a cyber-secure and resilient region.

OUR STRATEGY ON A PAGE

VISION

A cyber-secure, safe and resilient Fiji where all Fijians can benefit from meaningful connectivity and digital transformation.

KEY DRIVERS

- Economic Growth & Digital Development
- Social Inclusion
- Human Rights & Fundamental Freedoms
- National Resilience
- International Peace & Security

INTRODUCTION

As our nation embraces digital transformation to drive economic growth and sustainable development, improve public services, and connect Fijians across islands and oceans, we must also uplift our cybersecurity. Stronger cybersecurity and resilience will empower our communities, businesses, critical sectors and government to thrive in the digital age.

The National Cybersecurity and Resilience Strategy (NCRS) sets out Fiji's vision for a cyber-safe, secure, resilient, and inclusive digital future. It reflects our shared values, our international commitments and is a call to action in the face of growing cyber threats. The NCRS takes on a multifaceted, collaborative and holistic approach with a focus on cyber safety and awareness; strengthening cyber incident and cybercrime response capacity; protecting our government, critical infrastructure (CI) and critical information infrastructure (CII); developing cybersecurity talent and addressing workforce shortages; and amplifying Pacific voices through regional advocacy, leadership and international partnerships.

A Cyber-secure, Safe and Resilient Nation Begins with an Informed, Aware and Engaged Community

Building a cyber-secure Fiji starts at the community level by empowering Fijians with knowledge, skills, tools and awareness - the key to our collective resilience.

Strategic Priority 1: ***Secure, safe and cyber-aware Fijians and businesses*** focuses on empowering our communities to proactively protect themselves online. This includes building national awareness of cyber threats, promoting basic cyber hygiene practices, and equipping individuals and businesses with practical guidance to improve their cybersecurity practices. Strategic Priority 1 will also support micro, small and medium enterprises (MSMEs) and larger businesses to uplift their cybersecurity capabilities through tailored resources and outreach. Cybersecurity and resilience initiatives must bridge, not widen, the digital divide. To this end, Strategic Priority 1 will prioritise equity and inclusion, so Fiji's youth, women, marginalised peoples and remote and maritime communities are not left behind in our cybersecurity journey.

Cybersecurity is a Foundation for Fiji's Development, Economic Growth and National Security and Resilience

Fiji's ability to safeguard its economy and sovereignty relies on strong cyber defences and capabilities against malicious cyber activities and cybercrime on our government, critical infrastructure and critical information infrastructure, businesses and individuals.

Strategic Priority 2: ***Strong cyber incident and cybercrime response capabilities*** focuses on strengthening Fiji's sovereign capacity to identify, protect, detect, respond to and recover from nationally significant cyber incidents and address threats and impacts from cybercrime. This includes uplifting the capabilities of the National Computer Emergency Response Team (Fiji CERT), as the lead Government entity for national cyber incident response, governance and coordination. Strategic Priority 2 focuses on enhancing the technical and investigative capabilities of law enforcement and prosecutors and strengthening legal frameworks to enable timely action against cyber risks and threats. This includes

ensuring law enforcement and prosecutorial agencies are empowered under the laws of Fiji, including the Cybercrime Act 2021, to effectively combat cybercrimes and prosecute cybercriminals. Strategic Priority 2 also promotes trusted partnerships between government and critical sectors to share cyber threat intelligence, improve preparedness, and build national resilience.

Strategic Priority 3: ***Protected government, critical infrastructure and critical information infrastructure, data and assets*** focuses on safeguarding our networks, systems, information and data. This includes efforts to uplift the security of government networks and systems, support the cybersecurity and integrity of ICT supply chains, promote the adoption of international cybersecurity standards and cyber risk management frameworks, and strengthen our privacy and data protection policies and legislation. Strategic Priority 3 also prioritises identifying and protecting our CI and CII and setting clear expectations and cyber risk management obligations.

Realising Our Digital Future Requires a Skilled, Talented and Diverse Cybersecurity Workforce

Cybersecurity professionals must be equipped with knowledge, skills, training and access to opportunities to make a meaningful contribution to national cybersecurity and resilience and participate in the cyber workforce.

Strategic Priority 4: ***Skilled, talented and diverse cybersecurity workforce*** *focuses on growing the talent pool to meet Fiji's growing needs for skilled cybersecurity professionals. This includes initiatives to boost student enrolment in cyber-related fields, increase workforce participation particularly among women and underrepresented groups, and retain talented cybersecurity professionals in Fiji. Strategic Priority 4 supports Fiji's ambition to become a regional cyber talent and learning & development hub for the Pacific. It also focuses on strong partnerships between government, academia, and the private sector to develop employment pathways for cybersecurity professionals.*

Advocating for a Secure and Rules-based Cyberspace in Our Region and on the International Stage

Cybersecurity and resilience are key components of Fiji's foreign policy. Fiji will work with our regional and international partners to promote responsible State behaviour in the use of ICTs.

Strategic Priority 5: ***Cybersecurity leadership and global advocacy*** focuses on positioning Fiji as a champion and regional exemplar for a more secure, resilient, and inclusive cyberspace. It sets out how Fiji will strengthen partnerships across the Pacific and across regions to build collective cybersecurity and resilience. Strategic Priority 5 promotes Fiji's adherence to international law, rules and norms on responsible State behaviour in cyberspace. Our role includes active participation in UN processes on the security of and in the use of ICTs and the development of the Global Digital Compact on digital cooperation, Council of Europe Cybercrime processes, and governance of new and emerging technology like Artificial Intelligence. Strategic Priority 5 also commits to Fiji amplifying the voices of Pacific Small Island Developing States (SIDS) in global cybersecurity and cybercrime forums and continuing to stand up for the Pacific's priorities on the international stage.

Shaping Our Vision and Strategic Direction

Fiji undertook its second CMM Review from March to April 2024. A total of 78 stakeholders participated across government, criminal justice authorities and law enforcement, regulators, CI and CII operators, academia, civil society and international partners.

The NCRS was shaped by an inclusive, nationwide consultation process conducted from May to July 2025 and building from the CMM consultations. This included four national validation workshops across stakeholder groups, targeted discussions in the Western Division with critical sectors, and in-depth consultations with key government agencies. These engagements provided practical insights into Fiji's cybersecurity needs, challenges, and opportunities, ensuring the NCRS reflects the realities on the ground.

National consultations for the National Cybersecurity and Resilience Strategy, 25-26 May 2025

Progressing and Implementing Our Strategic Priorities

The Government is taking a phased approach to strengthen cybersecurity and resilience. Through strategic investment, collaboration and building capability sustainably, we will protect our digital infrastructure, empower our people and position Fiji as a cybersecurity leader. The implementation of the NCRS and Action Plan will occur over three phases: **Uplift** (2026-2027), **Scale** (2028-2029), and **Enhance** (2030-2031). The Action Plan will include milestones for tracking progress of our initiatives, mechanisms for coordination and accountability, and indicators to measure impact.

A dedicated Cyber Affairs Unit will be established within the Ministry of Communications to progress initiatives under the NCRS. The Unit will lead inter-governmental coordination, monitor progress against the Action Plan, and evaluate outcomes under a formal monitoring and evaluation framework. The NCRS and Action Plan will introduce governance and coordination mechanisms to drive national alignment, accountability and collaboration at all levels. The NCRS Consultative Committee will be formed to oversee and track commitments and progress against the Action Plan.

Partnerships will be essential to implementing the NCRS and Action Plan. The Action Plan identifies lead and supporting ministries and agencies for each initiative, and outlines the roles of other stakeholders across government, CIs and CIIs, civil society and academia. It is designed to be agile and adaptive, periodically updated and reviewed in response to emerging cyber threats, technological change, and stakeholder feedback.

PHASES OF ACTION

UPLIFT – 2026-2027

In our first phase, the Fiji Government will establish core organisational capabilities and launch high-impact initiatives for our cyber-secure and resilient future. We will promote national cyber awareness through targeted campaigns, education programs and public outreach to foster a cybersecurity culture across society. We will introduce cyber incident reporting mechanisms and publish technical guidance and advisory materials to support early detection and coordinated incident response. We will strengthen and enhance the capacity and capabilities of our National Computer Emergency Response Team – Fiji CERT. We will assess and baseline the cybersecurity posture of our critical sectors. We will implement governance frameworks, define clear roles and responsibilities, and drive collaboration to lay the groundwork for integrated coordination across government, industry, and the community.

SCALE – 2028-2029

In our second phase, the Fiji Government will focus on scaling and embedding the foundational gains by growing our human, technical, organisational and institutional cybersecurity capacity. We will prioritise enacting robust expectations and reforms for government and industry, establish clear obligations, and improve our enforcement capability. We will invest in skills development, promote career pathways in cybersecurity, and foster partnerships with academia and industry to meet the growing demand for a cybersecurity workforce. Critical sectors will be supported to implement resilience measures and adopt international standards. Our initiatives will see increased deployment of innovative technologies and security tools across government systems and networks to identify, protect, detect, respond to and recover from cyber threats.

ENHANCE – 2030-2031

In our third phase, the Fiji Government will enhance our cybersecurity and resilience and advance national capabilities to manage more complex cyber threats and risks and their consequences and impacts. We will proactively manage risks associated with critical and emerging technologies through uptake of robust cybersecurity and data protection standards across sectors and mandating the adoption of secure by-design technologies. We will co-design cybersecurity policy, regulation and legislation with key stakeholders. We will position Fiji as a regional centre of excellence for cybersecurity education and workforce development, attracting and retaining top talent in Fiji. We will embed cybersecurity cooperation within our security, economic and development agreements with our international partners.

STRATEGIC CONTEXT

What We Mean by Cybersecurity and Resilience

Cybersecurity refers to measures used to protect the confidentiality, integrity and availability of information, data, applications, operational systems, services and infrastructure.

- **Confidentiality** is the assurance that information processed, stored or communicated by applications, systems, services and infrastructure is only disclosed to authorised entities.
- **Integrity** is ensuring the authenticity and protection of data, applications, systems, services and infrastructure against modification or destruction.
- **Availability** is ensuring timely and reliable access to data, applications, systems, services and infrastructure.

Cyber resilience is the ability to identify, protect, detect, respond to and recover quickly from cybersecurity incidents and cybercrimes. This includes individuals and entities adopting and implementing appropriate cybersecurity controls, measures, safeguards and practices to minimise harm and manage cybersecurity risks.

Cyber Threat Environment

Government, CIs and CIIs, businesses and individuals are facing increased exposure to cybercrime and malicious cyber incidents and attacks that could disrupt essential services, erode public trust, and harm the economy. Cybercrime and malicious cyber incidents are rising across the Pacific, targeting and exploiting vulnerable or legacy systems. Key cyber threats the Government is observing in the Pacific and within Fiji include:

- An increase in cyber extortion including ransomware and data theft extortion against governments, CIs and CIIs, businesses and individuals.
- An increase in cybercrime such as data theft, business email compromise, phishing, and consumer fraud and scams.
- Website defacement and Distributed Denial of Service (DDoS) attacks by hacktivist groups disrupting services and causing reputational damage.
- Malicious insider events targeting governments and CI and CII sectors.
- Malicious use of emerging technologies including AI-generated disinformation and creation of deepfake content.
- Misinformation and disinformation that can undermine democracy, national security, and public trust in institutions.

Who are Cyber Threat Actors?

Cyber threat actors refer to individuals or organisations that commit malicious activity or have the intention or willingness to do so. In general, cyber threat actors target vulnerabilities of internet-connected devices, networks, systems and applications.

Cybercriminals are cyber threat actors targeting computers or using computers to commit criminal offences (under the laws of Fiji, as defined under the Cybercrime Act 2021). They include ransomware actors, hackers and scammers; and persons committing offences related to online child exploitation and abuse.

Non-state entities are cyber threat actors that are not acting on behalf of a government. This may include cybercriminals with financial or political motivations.

State-sponsored actors refer to a cyber threat actor conducting malicious activities on behalf of a government.

Digitalisation

Fiji is one of the most digitalised and connected countries in the Pacific, with 96% of the population covered by 3G and 4G networks and plans underway to expand 5G and satellite connectivity. Investments such as the Google-backed Tabua Cable, Bulikula interconnection, and licensing of Starlink are strengthening digital resilience. The National Digital Strategy 2025-2030 positions Fiji as a regional digital leader, prioritising access to the digital economy, essential service delivery, economic growth, and disaster recovery. Initiatives like universal services funding and digital literacy programs are bridging digital divides. However, increased connectivity also raises cyber risk. As more sectors digitalise, CIs and CIIs, businesses and our communities may be affected by cyber-attacks that could disrupt essential and critical services, such as connectivity and payment systems, which could impact our economic stability, national security, and community safety.

Technology Adoption

The rapid adoption of technologies like AI, cloud computing and the Internet of Things (IoT) is transforming Fiji's economy, driving innovation, productivity, and improved service delivery. As smart devices become more accessible there are increasingly trade-offs between affordability, functionality, and cybersecurity. Low-cost or unofficial software may lack encryption or include hidden vulnerabilities. Legacy systems that are often outdated and unsupported are commonly exploited by malicious actors due to known vulnerabilities and weak security controls. It can be difficult to integrate legacy systems with modern cybersecurity tools, and buying newer secure by-design technologies can be costly for MSMEs and businesses. Procurement decisions often prioritise cost over security, increasing risk to organisations.

Key Trends

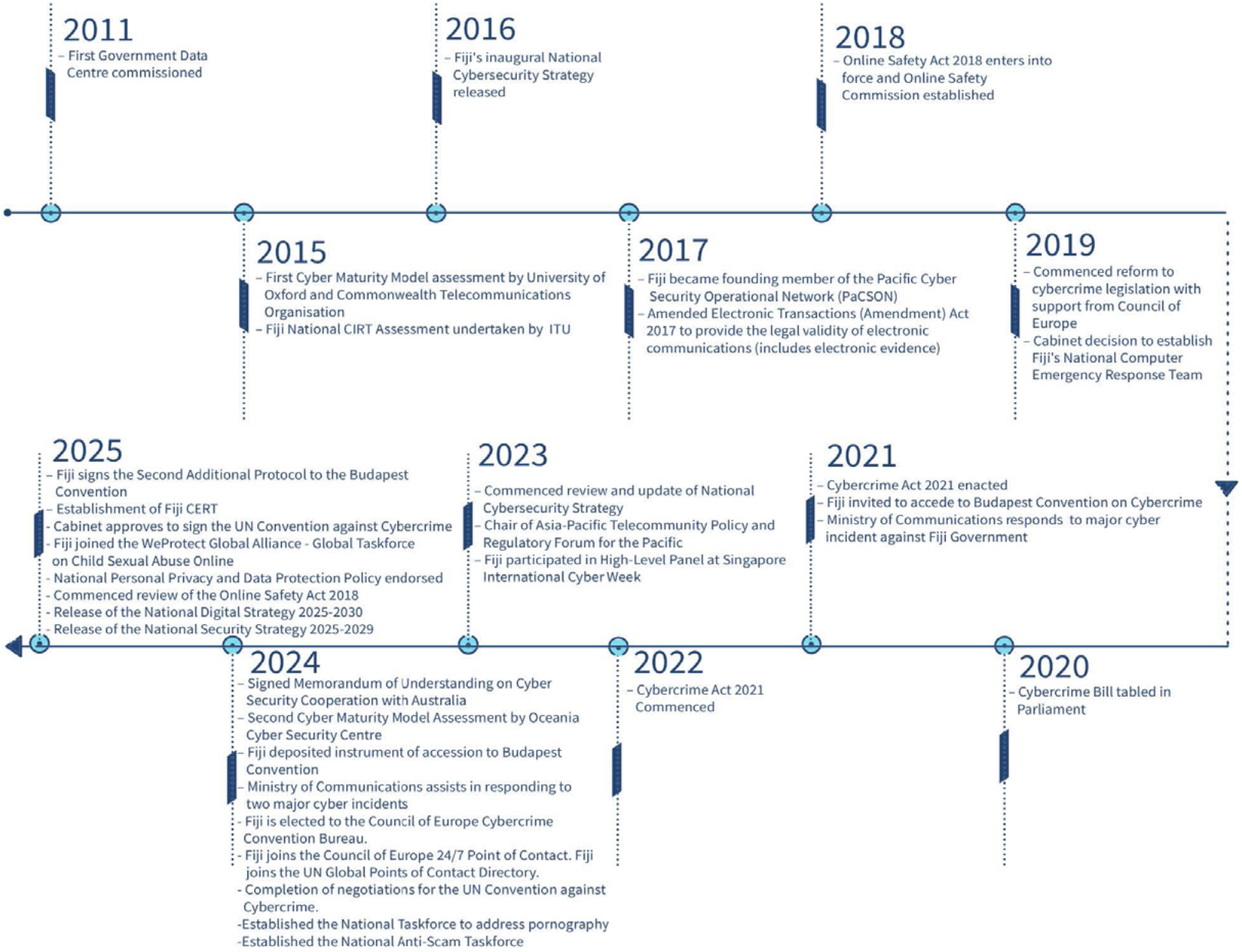
Cybercrime

Cybercrime is a growing, complex threat that causes financial, psychological and reputational harm to our communities and businesses. Offenders exploit vulnerabilities in unsecured systems and target personal and financial data, using social engineering tactics like phishing and scams to manipulate victims and steal identities or funds. Our communities are particularly affected by cybercriminal activities like phishing and scams. The low risk and high profitability make cybercrime an attractive global industry. Cybercriminals can target CIs and CIIs that hold sensitive data that can be used for extortion or sold on the dark web. These attacks erode trust in digital platforms and services, disrupt essential operations, and jeopardise our national security and resilience and societal wellbeing.

Cyber as Statecraft

Cyber operations are becoming an instrument of statecraft, with some states employing these for espionage, data theft, misinformation and disruption of government infrastructure, CIs and CIIs to advance strategic, political, or economic aims. State-sponsored actors may steal sensitive information, or preposition on government systems to collect information or prepare for sabotage. Governments are high-value targets due to the sensitive information they hold. Disruption of CIs and CIIs can undermine national security and resilience, destabilise economies and erode public trust. The World Economic Forum consistently ranks cyber warfare among the top global risks.[ii] As cyber threats grow more complex, protecting government infrastructure, CIs and CIIs, networks, data and assets is a strategic imperative.

OUR CYBERSECURITY JOURNEY SO FAR

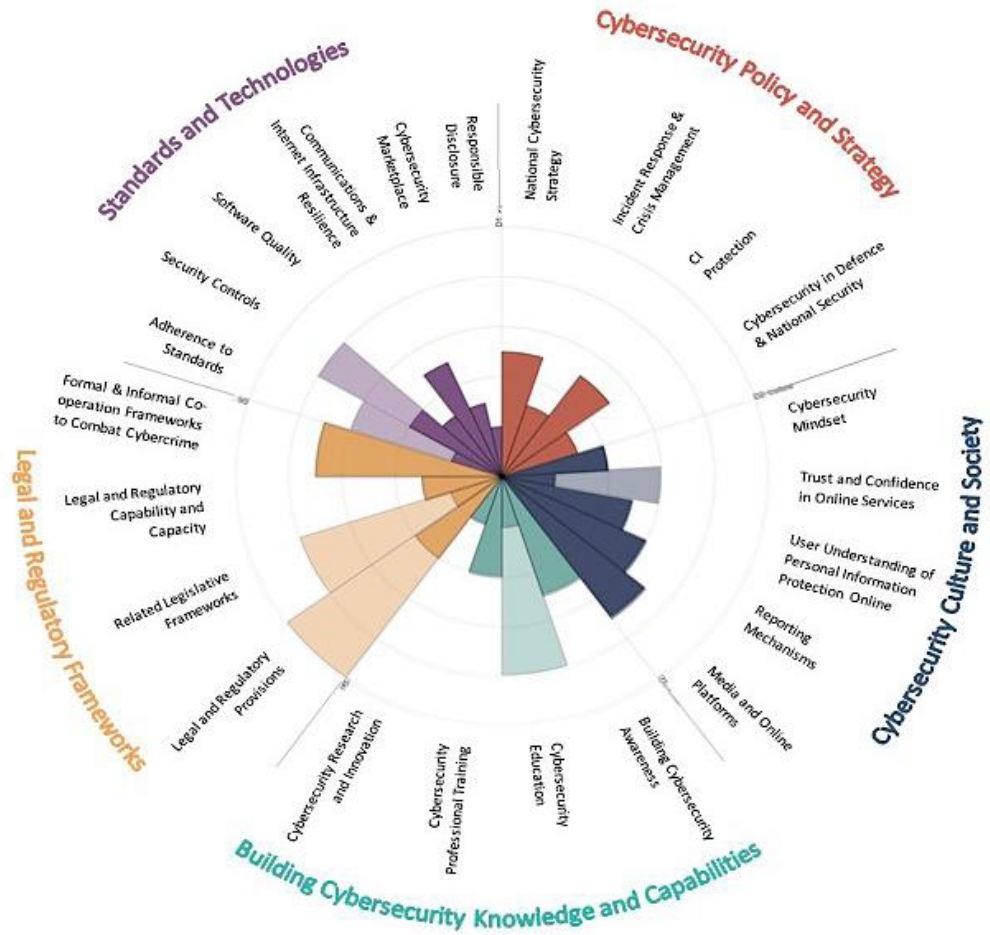


Cybersecurity Maturity Model for Nations Review

The 2024 CMM review, undertaken by the Oceania Cyber Security Centre with support from the UK Foreign, Commonwealth and Development Office, identified strengths and opportunities to protect, promote and enhance Fiji's cybersecurity and resilience. It assessed Fiji's cybersecurity maturity across five dimensions:

1. Cybersecurity Policy and Strategy
2. Cybersecurity Culture and Society
3. Building Cybersecurity Knowledge and Capabilities
4. Legal and Regulatory Frameworks
5. Standards and Technologies

This chart represents the assessment of Fiji's cybersecurity maturity. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre and 'dynamic' is at the perimeter.



Stages of Cyber Maturity

- **Start-up:** either no cybersecurity maturity exists, or it is at an early stage. There may be an absence of observable evidence of action.
- **Formative:** some cybersecurity maturity has begun to grow and be formulated, but it may be ad-hoc, new or not well-defined. Evidence of cybersecurity uplift can be demonstrated.

- **Established:** evidence indicates progress and demonstrates cybersecurity initiatives are working. There is some consideration of allocating resources or decisions on prioritisation in investing in cybersecurity uplift.
- **Strategic:** prioritisation on cybersecurity uplift activities and aspects has occurred. Decisions have been made to prioritise, conditional on context and circumstances of each nation.
- **Dynamic:** there are clear processes in place to alter national strategy depending on circumstances. There is evidence in global leadership on cybersecurity issues, rapid decision-making, allocation of resources and constant attention to changing circumstances.

Dimension 1: Cybersecurity Policy and Strategy

Fiji's current maturity is at the "start-up" to "formative" stages across this dimension. The CMM review highlighted Fiji's strength in regional and global engagement and government-led national initiatives but indicated the need for definition and designation of CIs and CIIs. Since the completion of the CMM, the Government has established Fiji CERT as the focal point for cyber incident response in Fiji.

Dimension 2: Cybersecurity Culture and Society

Fiji's current maturity is at the "start-up" to "established" stages across this dimension. The CMM review indicated a strong need for public awareness programs, cyber hygiene and literacy initiatives, and mechanisms to build user confidence in using digital platforms securely; and the integration existing cyber safety and cybercrime reporting mechanisms.

Dimension 3: Building Cybersecurity Knowledge and Capabilities

Fiji's current maturity is at the "start-up" to "strategic" stages across this dimension. The CMM review highlighted Fiji's strength in cybersecurity education offerings through our tertiary institutions; however, it also identified opportunities to boost cybersecurity skills through increasing continuous education offerings for ICT and cybersecurity professionals and investing in Fiji's research and development capacity.

Dimension 4: Legal and Regulatory Framework

Fiji's current maturity is at the "established" to "dynamic" stages across this dimension. The CMM review found that Fiji has one of the most legally mature cybercrime legislative and enforcement frameworks in the Pacific with strong linkages with international cybercrime cooperation networks. It highlighted the need to focus on uplifting legal and prosecutorial capacity on cybercrime.

Dimension 5: Standards and Technologies

Fiji's current maturity is at the "start-up" to "strategic" stages across this dimension. The CMM review found Fijian entities are adopting standards as the foundation for cybersecurity risk management, with strong uptake in the finance sector, government and many CI and CII operators. The Review emphasised the need to focus on supply chain risk, best practices guiding procurement processes (including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services) and uplifting cybersecurity maturity across the private sector.

KEY DRIVERS

Economic Growth and Digital Development

Cybersecurity is essential to Fiji's economic stability and growth, sustainable development and trust in the digital ecosystem. As set out in Fiji's National Digital Strategy 2025-2030, digital transformation will improve public service delivery, enhance productivity, and connect Fiji to global markets. But fully realising the benefits of digital transformation relies on a secure and resilient cyberspace.

Cyber threats can have significant impacts on economic stability and sustainable development. Cyber industry projections on the direct and indirect costs of cyber incidents estimate the worldwide cost to reach USD265 billion by 2031.[iii] In 2024, the global average cost of a data breach was USD4.88 million, with breaches in government and CI and CII sectors often exceeding this amount.[iv] Cybercriminals are increasingly exploiting supply chains and gaps in defences as seen in the 2020 SolarWinds cyber attack[v], or third-party compromises of external vendors such as the Qantas cyber incident in July 2025[vi]. For Fiji, a single security breach in critical sectors like telecommunications, energy, or financial services could disrupt essential services, undermine investor confidence, and inflict major recovery costs. Micro, Small and Medium Enterprises (MSMEs) are especially vulnerable due to limited cybersecurity awareness and incident response capacity. To address this, the Government is committed to building capacity, strengthening coordination, investing in cyber incident and cybercrime response capabilities, and raising national awareness of cyber threats.

Long-term and sustained investments in cybersecurity and resilience across our economy and society support innovation and secure access to new technologies and global markets. As Fiji embraces digital transformation, cybersecurity ensures that emerging technologies, e-commerce and e-government services deliver their intended benefits without exposing Fijians to cyber risks. In this way, cybersecurity and resilience is about creating the conditions for economic growth and sustainable development in an increasingly connected world.

Social Inclusion and Diversity

Cybersecurity and social inclusion are deeply connected. Ensuring all Fijians, regardless of age, gender, location, or socio-economic background, can participate and engage safely in cyberspace is critical to closing the digital divide. Vulnerable groups often face greater cyber risks, and without protection, online harm can deepen existing inequalities. Inclusive cybersecurity and resilience means tailoring support to diverse needs, such as translating guidance into the vernacular language and making resources accessible for persons with a disability and delivering targeted community outreach. Cybersecurity is a social imperative as well as a technical one, and must have diversity, non-discrimination and inclusion at its heart to ensure that everyone can benefit from digital transformation.

The National Development Plan 2025 - 2029 and Vision 2050 and the National Digital Strategy 2025 - 2030 commits to gender equality, and the NCRS aligns by integrating gender considerations across activities on cyber awareness and education and workforce development. The inclusion of women and underrepresented groups such as people with a disability in the cybersecurity workforce is an urgent challenge. Women comprise approximately 25% of the cybersecurity workforce in the Asia-Pacific region, highlighting a significant gender gap in the industry.[vii] In Fiji, this shortfall risks progress in women's

empowerment, diversity in leadership, and women's safety and rights online. The Government has been undertaking efforts to address gender disparities in cybersecurity and the broader ICT workforce. The Girls in ICT Initiative is a key priority for the Government to uplift cyber and online safety awareness among women and girls. The Fiji Chapter of the Women in Tech Network was launched in April 2025 to strengthen efforts to bridge the gender gap by providing mentorship, advocacy, skills development and capacity-building for women and girls.

A vital component of an inclusive cyberspace is the safety of Fijians online. The Online Safety Commission (OSC), established under the Online Safety Act 2018, is the primary body in Fiji that promotes responsible digital behaviour and supports individuals facing cyberbullying and online abuse. The OSC has delivered education campaigns, school outreach, and distributed over 60,000 safety booklets. In 2024, the OSC launched the Swipe Safe training and app with UNICEF and ChildFund, targeting social media use, scams, and grooming risks. An independent review of the Online Safety Act is underway to ensure the law remains effective in addressing online harms.

Online child sexual exploitation and abuse (OCSEA) is a serious and growing challenge to Fiji's society and social wellbeing. Fiji received 6,046 reports of child sexual abuse material in 2022, 3,638 in 2023, and 1,875 in 2024 through NCMEC's CyberTipline.[viii] The Government is committed to urgent action to protect children and our communities from OCSEA and combat this crime type. In response, the Government established the National Taskforce to Address Pornography in 2024. The first workstream of this national taskforce is to address and combat OCSEA. In 2023, OSC became a member of the WeProtect Global Alliance, a global movement that brings together governments, private sector, civil society and international organisations to end OCSEA.[ix] In 2025, the Government of Fiji became a member and joined the WeProtect Global Alliance's Global Taskforce on Child Sexual Abuse Online that supports international cooperation for cross-border investigations, victim support and capacity-building on combatting OCSEA.

Human Rights and Fundamental Freedoms

Our efforts towards a secure and resilient cyberspace must uphold rights to privacy, freedom of expression, dignity, and access to information as enshrined in the Universal Declaration of Human Rights, the 1966 United Nations International Covenant on Civil and Political Rights, UN Convention on the Rights of the Child, the Convention on the Elimination of all Forms of Discrimination Against Women, and the International Convention on the Elimination of All Forms of Racial Discrimination. This is cemented in the 2013 Constitution of the Republic of Fiji and sectoral laws. This is further affirmed at the regional level in the 2018 Boe Declaration and the 2050 Strategy of the Blue Pacific Continent. Cybersecurity efforts must also support the realisation of the UN Sustainable Development Goals 9 and 17 on increasing access to ICTs and providing universal and affordable access to the internet. To this end, Fiji is focused on the protection of human rights and sustainable development in its policy-making on cybersecurity by ensuring any protections in cyberspace are balanced with principles of transparency, proportionality and accountability. As cyberspace is an arena for civic engagement, our efforts must both defend against cybercrime, exploitation and mis/disinformation while safeguarding human rights and fundamental freedoms online.

The rise of AI brings both opportunities and risks for human rights in cyberspace. AI can enhance cybersecurity through advanced cyber threat detection, predictive analysis, and automated response, helping to protect personal and sensitive data and critical services. However, without safeguards, AI-enabled surveillance, algorithmic bias, and misuse of data could undermine human rights. Malicious cyber actors can weaponise AI for deepfakes, disinformation and committing cybercrimes, eroding trust in digital systems and democratic institutions. The Government is dedicated to ensuring that AI use in cybersecurity aligns with Fiji's laws, international human rights obligations and ethical principles, so that technology empowers rather than exploits our people and communities. To this end, the Government is proactively working on deepening our understanding and prioritises participating in international processes on AI governance, including the UN Global Digital Compact, the Council of Europe Cybercrime

Convention Committee AI Mapping Study and regional discussions on the safe, ethical and responsible development and deployment of AI.

National Resilience

The cybersecurity and resilience of government networks and e-government services is essential to safeguard national security, ensure continuity of public services, and protect sensitive citizen and Government data from malicious cyber actors. The Government has made significant investments to strengthen and maintain the cybersecurity of the Government Network (GOVNET), data and government devices. The Ministry of Communications' Department of ITC Services operates Fiji's Government Security Operations Centre (SOC), which monitors cyber threats to GOVNET and secures government systems. The SOC has rolled out civil service cyber awareness training and implemented multi-factor authentication for government devices. The Digital Government Transformation Office (DGTO) leads the digitalFIJI program, embedding security and privacy by-design principles into digitalFIJI developed and maintained government e-services.

Combatting cybercrime is a key priority for Fiji to boost our national resilience. To respond to this crime type, Fiji has rapidly advanced its cybercrime response framework, culminating in the passage of the Cybercrime Act 2021 and accession to the Budapest Convention. Together, this framework places Fiji among the most legally mature countries in the Pacific on cybercrime. In June 2025, Fiji signed the Second Additional Protocol to the Budapest Convention, becoming the first country in the Pacific and the 50th globally. Once ratified, the Second Additional Protocol will make it easier for our criminal justice authorities to access electronic evidence from service providers offshore. Fiji was an active contributor to the drafting of the UN Convention against Cybercrime and became the 74th Party to sign the Convention in December 2025. The Government is focused on uplifting the capacity of law enforcement and the judiciary to bring cybercriminals to justice. Fiji maintains a dedicated Cybercrime Unit within the Fiji Police Force and leverages international cooperation networks, including INTERPOL and the Budapest Convention 24 by 7 Points of Contact, to support swift cybercrime investigations and prosecution. Through a close partnership with the Council of Europe, Fiji has received training for judiciary, law enforcement and prosecutors under the GLACY-e and GLACY+ initiatives. The annual National Conference on Cybercrime and e-Evidence enhances prosecutorial capability and coordination across the criminal justice sector.

Regional and International Peace and Security

Fiji advocates for an open, safe, secure, stable, accessible, peaceful and interoperable ICT environment where Pacific SIDS meaningfully engage in regional and international discussions on cyber non-binding norms of responsible State behaviour and cross-border cooperation. At the regional level, Fiji is helping to advance collective regional action on cybersecurity and resilience through the Pacific Islands Forum's Pacific ICT Minister's Dialogue and the implementation of the 2023 Pacific ICT Minister's Lagatoi Declaration on Digital Transformation of the Pacific and the Action Plan. In August 2025, Pacific ICT Ministers endorsed the Pacific ICT and Digital Transformation Action Plan for the Lagatoi Declaration that sets out actions for strengthening digital security and trust.

Globally, Fiji is an active contributor to international cyber diplomacy and governance forums and continues to demonstrate our commitment to upholding the rules-based international order and responsible State behaviour in cyberspace. Over 2020 to 2025, Fiji has consistently participated in the United Nations Open-Ended Working Group (UN OEWG) on the security of and in the use of ICTs, contributing to the setting of international rules and norms on the application of international law in cyberspace, amplifying Pacific voices and perspectives, engaging in multistakeholder cooperation, and advocating for capacity-building for SIDS and other developing States. At the UN OEWG, Fiji has advocated for inclusive global governance that respects cultural diversity, safeguards digital rights, and ensures cyber capabilities are not misused for coercive or destabilising purposes.

The Government of Fiji represented by the Ministry of Communications and Office of the Attorney-General with the Chair of the UN Open-Ended Working Group on the security of and in the use of ICTs (2021-2025), Ambassador Burhan Gafoor (Singapore) and his team.

In 2024, Fiji joined the UN intergovernmental Global Points of Contact Network Directory to share information on cyber threats, coordinate responses, and build trust to respond to cyber incidents and attacks across borders. Fiji has also participated in the simulation exercises that simulate the practical aspects of participating in the intergovernmental global points of contact directory and to better understand the diplomatic and technical roles.

Fiji is also committed to engagement in the UN Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs (the UN Global Mechanism). The UN Global Mechanism will carry forward the UN OEWG's work and serve as a global permanent platform for implementing voluntary norms and confidence-building measures.

The Women, Peace and Security Agenda (WPS) recognises that women experience conflict and security threats, including cyber threats, uniquely and disproportionately. This disparity extends to cyberspace, where ransomware, data breaches, disinformation, and internet shutdowns have gendered and intersectional impacts shaped by factors such as race, ethnicity, age, class, and sexual orientation.[x] Fiji is committed to advancing gender equality and the empowerment of all women and girls by embedding and mainstreaming across all aspects of cybersecurity governance and peacebuilding, from cybersecurity policy and legislative development and design, to gender-sensitive and inclusive cybersecurity capacity building. Fiji participates in and contributes to the Women in International Security and Cyberspace (WiC) Fellowship program, that enables senior Fijian women cyber diplomats to represent Fiji at the UN OEWG sessions and meaningfully participate in decision-making processes related to the use of ICTs in the context of international peace and security.

Pacific WiC Fellows at the UN OEWG 11th Substantive Session

VISION

A cyber-secure, safe and resilient Fiji where all Fijians can benefit from meaningful connectivity and digital transformation

Strategic Priorities and 2031 Goals

1. Secure, safe and cyber-aware Fijians and businesses

- A cyber-secure and resilient Fiji enables increased access to meaningful connectivity, technologies, digital government services and the digital economy for our communities and businesses.
- All Fijians and businesses adopt a culture of good cyber hygiene. Fijians are vigilant to protect themselves against cybersecurity risks and adopt strong cybersecurity practices.
- Government, businesses and Fijians engage in genuine partnership to strengthen our cybersecurity and resilience at the national level.

2. Strong cyber incident and cybercrime response capabilities

- Fiji's sovereign capabilities deter and mitigate the impacts of cyber incidents and cybercrime.
- Our capabilities enable government, critical infrastructure and critical information infrastructure to identify, protect, detect, respond to and recover quickly from cyber incidents and cybercrime.
- Fiji's national resilience is strengthened and bolstered by our cyber incident response and cybercrime capabilities. Cybersecurity and combatting cybercrime forms part of our national security frameworks.

3. Protected government, critical infrastructure and critical information infrastructure, data and assets

- Fiji's prosperity and sustainable development are strengthened by cyber-secure and resilient government, critical infrastructure and critical information infrastructure, systems and applications.
- Government and critical infrastructure and critical information infrastructure remain resilient by managing supply chain risks by adopting cybersecurity standards including for procurement processes of technologies.
- The sensitive data of our community, critical infrastructure and critical information infrastructure, and government are protected through strong data security and privacy frameworks.

4. Skilled, talented and diverse cybersecurity workforce

- Fiji has an ongoing talent pipeline of skilled, diverse cyber professionals, and a sustainable cybersecurity workforce.
- Fiji's cybersecurity professionals trained by Fijian universities and training institutes are equipped with world-class skills.
- Fiji is the most attractive destination in the Pacific for cybersecurity professionals.

5. Cybersecurity leadership and global advocacy

- Fiji, as a regional leader in cybersecurity, advocates for cross-regional cooperation in cybersecurity. Fiji promotes and implements our regional and global commitments on cybersecurity and combatting cybercrime.
- Fiji continues to adhere to international law and promotes international rules and norms of responsible State behaviour in cyberspace.
- The Government and civil society actively participate in regional and global forums. Fiji continues to amplify the voices from our Blue Pacific in global cybersecurity and cybercrime forums.

OUR STRATEGY 2026 - 2031

STRATEGIC PRIORITY 1

Secure, Safe and Cyber-aware Fijians and Businesses

2031
Goals

- **A cyber-secure and resilient Fiji enables increased access to meaningful connectivity, technologies, digital government services and the digital economy for our communities and businesses.**
- **All Fijians and businesses adopt a culture of good cyber hygiene. Fijians are vigilant to protect themselves against cybersecurity risks and adopt strong cybersecurity practices.**
- **Government, businesses and Fijians engage in genuine partnership to strengthen our cybersecurity and resilience at the national level.**

Challenges and Opportunities

Using technology is part of our everyday life. It is critical that, as part of our national and inclusive approach, Fijians are aware of and vigilant against cyber risks and feel empowered to take steps to protect themselves, their families and their businesses. Embedding cybersecurity and resilience across our society and community is a national priority. Good cyber hygiene is the first line of defence in Fiji's cybersecurity and must form part of everyday practices when accessing the internet and using technology. According to Microsoft, embedding a culture of good cyber practices could prevent 99% of cyber incidents.[xi] But not all Fijians are adopting good or consistent cybersecurity practices. A 2023 study by the UN Capital Development Fund on digital and financial literacy in Fiji found that 74% of Fijians surveyed lock their phone when not in use, 63% use virus protection and 46% reuse the same password across their devices and accounts.[xii]

What is cyber hygiene?

Cyber hygiene refers to taking steps to protect your accounts and devices from cyber threats. Actions to improve cyber hygiene include:

- Using strong passwords, passcodes or passphrases that are personalised to you, different for each account and difficult for cybercriminals to guess.
- Updating software on your mobile phone, apps and computers that fixes software bugs and vulnerabilities that cybercriminals can exploit to access your data or accounts.
- Not clicking on unknown or suspicious links or downloading files or apps from unknown sources, which could introduce malware and other malicious software on your devices.
- Activate multi-factor authentication for your important accounts, like online banking, social media and your email accounts.

The Government is committed to supporting MSMEs and larger business owners to increase their awareness of cyber risks that can affect business operations and protect their data. Fijian businesses hold sensitive personal and financial information and data that could be exploited by cybercriminals and ransomware actors. Business email compromise and phishing can particularly affect MSMEs and larger businesses. Where an MSME with lower cybersecurity is integrated into the networks of larger organisations, this can create a backdoor that malicious cyber actors can exploit. Raising cybersecurity awareness is a national priority to mitigate these risks and protect MSMEs and larger business owners.

To build a truly national cybersecurity culture, the Government is committed to creating more pathways to engage youth, remote and maritime communities and disadvantaged populations that may be more vulnerable to cybercrime and cyber incidents. Targeted outreach to remote communities, embedding cybersecurity into existing digital literacy and inclusion initiatives, and leveraging grassroots and community networks will ensure no one is left behind in Fiji's cybersecurity journey.

Activities

1.1 Enhance National Cybersecurity Awareness

1.1.1 The Government will empower Fijians to uplift their cybersecurity and boost their resilience through **national cybersecurity awareness campaigns**, promoting the adoption of a culture of basic cybersecurity and cyber hygiene practices. The Government will coordinate this work with related efforts on combatting scams, fraud, online safety, privacy and data protection.

1.1.2 Key government ministries and agencies, critical sectors, larger businesses, MSMEs, civil society and academia will engage in a **national partnership to design and deliver awareness-raising activities** tailored to the local Fiji context. Partners will co-host key annual events, such as Safer Internet Day, Cybersecurity Awareness Month and National Scam Awareness Week, using these events to promote cybersecurity awareness at scale.

1.1.3 The Government will empower community leaders, Online Safety Commission and Fiji Police to perform **community outreach and awareness-raising** activities, leveraging initiatives such as the Pacific Islands Chiefs of Police (PICP) Cyber Safety Pasifika program.

1.2 Provide Guidance and Advice on Cybersecurity and Resilience

1.2.1 The Government will create a **national cyber website** as a central point for advice and guidance. Operated by Fiji CERT, the website will feature practical advice on staying cyber-secure, updates on cyber threats, and advice on how to access support and subsequently, report cyber incidents.

1.2.2 **Cybersecurity checklists and advice** will be published regularly on the cyber website. This will be tailored for audiences and age groups, with content adapted for different literacy levels and accessibility needs, and in the vernacular languages.

1.2.3 The Government will release **online cybersecurity training for individuals and businesses**. This self-directed training will be aimed across age groups and cohorts and in the vernacular languages, to maximise its reach.

1.2.4 The Government will develop **data privacy and protection guidance for MSMEs and larger businesses** on Fiji's Privacy and Personal Data Protection Policy. By increasing understanding of responsible use of data and privacy protections, these efforts will prevent misuse of data, build public trust and support compliance.

1.3 Help Victims Affected by Cyber Incidents and Cybercrime

1.3.1 The national cyber website will include a **cyber incident reporting portal** to direct victims to the appropriate authorities for assistance. This portal will be coordinated with existing reporting and support mechanisms of OSC, Fiji Police and the Consumer Council of Fiji.

1.3.2 The Government will publish a **ransomware playbook and guide** on the national cyber website. This playbook will ensure businesses know what to do if they are the victim of a data theft extortion or ransomware incident.

1.4 Support MSMEs and Businesses to Adopt Good Practices and Requirements

1.4.1 The Government will prioritise mitigation strategies to help MSMEs and businesses to protect themselves against cyber threats by developing **essential cybersecurity good practice principles**. These principles will set expectations for businesses to lift their cybersecurity.

1.4.2 To limit regulatory burden, the Government will **co-design a cybersecurity baseline for MSMEs and businesses**. As cybersecurity requirements evolve over time, the Government will provide guidance to MSMEs and businesses to meet the cybersecurity baseline.

1.5 Build Genuine Partnerships and Promote Shared Responsibility

1.5.1 The Government will establish the **Cyber Champions program** to form a nationwide network across government, businesses, CIs and CIIs, civil society and community organisations who are trained to promote cybersecurity awareness and good practices within their organisations and communities.

1.5.2 The Government will raise executive awareness and responsibility for strong cybersecurity by establishing a **National Executive Cyber Advisory Council**. The Council, comprised of Permanent Secretaries, Regulators, Executives of CIs and CIIs, senior representatives from Government, industry, civil society and academia, will meet regularly to share experiences of addressing cyber risks, advise on priorities and promote coordination and transparency.

1.6 Promote Inclusive Awareness-raising and Capacity-building

1.6.1 In line with Fiji's National Development Plan, the Government will **embed gender equity and social inclusion** considerations in all policy development on cybersecurity and resilience. We will achieve this by consulting with relevant civil society stakeholders during the design and delivery of our initiatives.

1.6.2 To bridge the digital divide and address the unique needs of diverse cohorts, the Government will make advice accessible in Fiji's vernacular languages and for persons with disabilities. We will also focus on reaching remote and maritime communities by continuing **to incorporate cybersecurity into digital inclusion initiatives**, such as the Ministry of Communications' Telecentre Programme, the ITU Smart Islands Programme, the Connecting the Unconnected Programme, and the Universal Service Scheme.

1.7 Strengthen Institutional and Governance Arrangements on Cybersecurity

1.7.1 Through a national consultation process, the Government will **scope the establishment of a National Cyber Agency** by 2030. The scoping would identify the role of a National Cyber Agency to lead national cybersecurity policy, coordinate across government and industry, and provide oversight of national activities to uplift cybersecurity and resilience.

1.7.2 As part of the NCRS implementation process, the Government will undertake a **formal review on the development of cybersecurity legislation**. This will support identifying key gaps in our legislative and regulatory environment and potential reform measures.

STRATEGIC PRIORITY 2

Strong Cyber Incident and Cybercrime Response Capabilities

2031

Goals

- **Fiji's sovereign capabilities deter and mitigate the impacts of cyber incidents and cybercrime.**
- **Our capabilities enable government, critical infrastructure and critical information infrastructure to identify, protect, detect, respond to and recover quickly from cyber incidents and cybercrime.**
- **Fiji's national resilience is strengthened and bolstered by our cyber incident response and cybercrime capabilities. Cybersecurity and combatting cybercrime forms part of our national security frameworks.**

Challenges and Opportunities

Establishing Fiji's sovereign capabilities to address cyber incidents and attacks, and sustaining these capabilities, is imperative to keep our nation safe and secure. Without decisive action to build strong cyber incident and cybercrime response capabilities and foster public-private cooperation, Fiji risks falling behind in our ability to identify, protect, detect, respond to and recover from cyber threats and attacks. Proactive investment in cyber incident and cybercrime response capabilities boosts our capacity to protect our communities, MSMEs, businesses, critical sectors and government.

What is cyber incident response?

Source: NIST Cybersecurity Framework 2.0

A cybersecurity incident is an unwanted or unexpected cyber security event, or a series of such events, that has compromised business operations or has a probability of compromising business operations.

Cyber incident response involves structured phases to manage risk and respond to incidents effectively. The cyber incident response lifecycle phases are: govern, identify, protect, detect, respond, and recover.

Having a capable national incident response function is vital to protect Fiji's most sensitive and significant data, networks, and systems. In 2025, the Government launched Fiji CERT as the focal point for nationally-significant cyber incident response. Fiji CERT is responsible for monitoring malicious cyber activity, coordinating nationally-significant cyber incident responses and recovery, and promoting cybersecurity awareness. Establishing Fiji CERT is a highly significant milestone in Fiji's journey to uplift cybersecurity and resilience and protect our nation from cyber incidents.

A well-managed response enables organisations to quickly regain control and prevent escalation. It can also reduce data loss, limit financial impacts, and protect the reputation of affected organisations. A strong cyber incident response capability and the establishment of Fiji CERT improves national resilience by strengthening defences before incidents occur and ensuring lessons are learned and applied afterwards. Preparing for incidents also supports compliance with national standards, laws, and regulations. A challenge often faced during a cyber incident is a lack of coordination and flow of information. When a cyber incident occurs, time is of the essence. Effective governance and clear roles and responsibilities are critical to ensure Fiji can quickly respond to cyber incidents.

The National Security Strategy 2025-2029 highlights cybercrime as transnational threat requiring international collaboration and cooperation. Criminal networks often operate across borders, making it difficult for any one country to tackle cybercrime alone. The Government is committed to working with international partners, regional organisations, and global forums to strengthen cybercrime response cooperation, share intelligence, and improve joint investigation and response capabilities. The evolving nature of cybercrime means our law enforcement must be equipped with tools, technologies and skills to effectively investigate these crimes. This must also be complemented through strong support for our prosecutors to uphold the law and bring cybercriminals to justice.

Activities

2.1 Boost Fiji's Cyber Incident Response Planning and Coordination

2.1.1 The Government will grow Fiji's national cyber incident response capacity by **enhancing Fiji CERT's capabilities, technology and resources**. Fiji CERT will develop a five-year plan to determine resourcing requirements to ensure sustainability and effectiveness.

2.1.2 Fiji CERT will build preparedness for cyber incidents by developing a **National Cyber Incident Response Plan**. The Plan will build on existing crisis and disaster management plans and international best practice.

2.1.3 The Government will regularly benchmark Fiji's incident response capabilities and test our National Cyber Incident Response Plan. Fiji CERT will **conduct national cyber drills and exercises** with Government, CIs and CIIs and businesses, with support from international partners, to test our readiness and preparedness.

2.2. Implement Effective Incident Response Governance Mechanisms

The Government will implement governance through two mechanisms: the **Cyber Incident Response Steering Committee and the Cyber Incident Crisis Committee**.

2.2.1 The **Cyber Incident Response Steering Committee** will be comprised of senior officials and cyber leaders as the primary governance body for cyber incident response in Fiji. The Forum will conduct post-incident reviews as necessary.

2.2.2 The **Cyber Incident Crisis Committee** will be stood up when a nationally-significant cyber incident occurs. The Committee will enable real-time collaboration and be a central point of coordination during a cyber crisis. The Committee will be chaired by the Minister for Communications and will report progress and outcomes of remediation of the cyber incident to the National Security Council of the Cabinet.

2.3 Encourage cybersecurity information and cyber threat-sharing

2.3.1 The Government, through Fiji CERT, will facilitate strong public-private collaboration by **sharing cyber threat advisories** for CIs and CIIs, businesses and MSMEs, published on the national cyber website.

2.3.2 The Government will partner with CIs, CIIs and businesses to **create protocols for cyber threat intelligence sharing within sectors**. The Government will ensure any information shared with sectors is labelled, handled and stored appropriately using agreed protocols, including the Government's Protective Security Framework, to build a culture of proactive and timely information-sharing of cyber intelligence.

2.4 Engage international partners on cyber incident response

2.4.1 Fiji will continue to support our region through **collaboration and information-sharing with Pacific CERTs**, bilaterally and through the Pacific Cyber Security Operational Network (PaCSON) community.

2.4.2 The Government will leverage international and regional expertise by **participating in international forums for incident response**, including the Forum for Incident Response Security Teams (FIRST) and the Asia Pacific Computer Emergency Response Team (APCERT).

2.4.3 The Government will enhance its cyber readiness and incident response capabilities by **participating in regional and international cyber incident response exercises and drills**, including the ITU regional and global cyberDrills, PaCSON exercises, and at the UN Global Mechanism.

2.4.4 The Government will **develop thresholds for requests for international assistance for significant cyber incidents** affecting Fiji. Thresholds for requesting international assistance will be included in the National Cyber Incident Response Plan.

2.5 Modernise legislation, regulation and institutional cooperation

2.5.1 Following the release of the National Privacy and Personal Data Protection Policy, the Government will **develop privacy and data protection legislation**. The proposed legislation will establish remedies for those affected by data breaches and penalties for violations. It will be aligned with international best practice such as the European Union's General Data Protection Regulation (GDPR). The Government will also take steps towards becoming a party to the Council of Europe's Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (108+ Convention).

2.5.2 The Government will **establish an independent and impartial data protection authority** to oversee and monitor compliance, protect individuals' data protection and privacy rights, and enforce proposed legislation.

2.5.3 The Government will **align legal frameworks with the Second Additional Protocol** to the Budapest Convention on Cybercrime. This includes updating the Cybercrime Act 2021 to facilitate direct requests for subscriber information and data, enhancing cooperation in emergencies, and ensuring human rights safeguards.

2.5.4 The Government will **enhance institutional capacity on mutual legal assistance requests and emergency disclosure**, including investment in the technical capabilities for timely transmission of electronic communications to meet obligations under the Second Additional Protocol to the Budapest Convention.

2.6 Strengthen law enforcement and prosecutorial capacity on cybercrime

2.6.1 The Government will amplify our domestic efforts to effectively investigate and respond to cybercrime and cyber-enabled crimes, by bolstering cybercrime capability and capacity in the Fiji Police Force. This includes efforts to **upgrade the national digital forensic lab**, equipping it with state-of-the-art and advanced tools and technologies.

2.6.2 The Government will continue to build partnerships to **strengthen capability to investigate and prosecute cybercrime offences** through capacity-building and strengthening partnerships through events like the National Conference on Cybercrime and e-Evidence for Prosecutors. This will enable prosecutors and law enforcement officers to discuss legal developments, build practical skills in electronic evidence handling and address emerging challenges like cross-border data access and digital chain of custody.

2.7 Participate in International Cybercrime Cooperation Mechanisms and Frameworks

2.7.1 The Government will leverage existing relationships and **deepen international partnerships to combat cybercrime**, including through the Budapest Convention 24 by 7 Points of Contact Network.

2.7.2 The Government will continue to engage in **operational police-to-police cybercrime cooperation**, including the Pacific Island Law Officers' Network (PILON) and PICP. We will also continue to work with our international partners through our INTERPOL National Central Bureau and the Online Child Sexual Exploitation and Abuse Unit.

2.7.3 The Government has signed the **UN Convention against Cybercrime in December 2025** after it opened for signature in October 2025. Following this, the Government will work to harmonise domestic frameworks with the new convention.

STRATEGIC PRIORITY 3

Protected Government, Critical Infrastructure and Critical Information Infrastructure, Data and Assets

2031

Goals

- **Fiji's prosperity and sustainable development are strengthened by cyber-secure and resilient government, critical infrastructure and critical information infrastructure, systems and applications.**
- **Government, critical infrastructure and critical information infrastructure remain resilient by managing supply chain risks, and adopting cybersecurity standards, including for procurement processes of technologies.**
- **The sensitive data of our community, critical infrastructure and critical information infrastructure, and government are protected through strong data security and privacy frameworks.**

Challenges and Opportunities

Fijians must have confidence that all infrastructure that underpins our economic resilience and national security – including government infrastructure, CIs and CIIs and their networks, systems, data and assets – are cyber-secure and resilient. Global cyber incidents and attacks show that insecure infrastructure can leave nations exposed, with disruptions to CIs and CIIs causing cascading impacts. Defining and designating CI and CII is a vital first step to improve government visibility of key assets and assess their cyber risk. This allows for more targeted, proportionate cybersecurity obligations and coordinated response when significant incidents occur. The Government will build shared responsibility by setting rules and expectations for CI and CII operators, supported by sector-specific reporting and cyber threat information sharing via secure channels.

To make Fiji a hard target for malicious cyber actors, the Government is committed to strengthening economy-wide awareness, compliance, and adoption of international cybersecurity standards, such as International Organization for Standardization's ISO/IEC 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 and other sector-specific standards. We are focused on addressing challenges faced by CIs and CIIs in implementing standards through practical and regulatory measures, procurement guidance, capacity-building, and public-private partnerships. The Government is also committed to promoting security and privacy by-design in procurement practices across entities. Aligning with international best practice ensures trust is maintained in the cybersecurity and resilience of our "crown jewels" – our most critical systems, networks, data and assets.

Case Study: Financial Services Sector

The financial services sector is an attractive target for cybercriminals. It faces unique cyber risks due to the industry's reliance on sensitive financial, commercial and personal data, and connected digital systems for real-time transactions. Significant efforts are being undertaken by the sector, led by the Reserve Bank of Fiji, to manage, mitigate and respond to these risks. As a result, the financial sector has the most comprehensive cybersecurity requirements in place for any sector in Fiji.

In March 2023, the RBF issued the Prudential Supervision Policy Statement No. 2 Minimum Requirements for the Management of Cybersecurity Risk by Supervised Entities to address the evolving cyber threat landscape. The Statement places requirements on supervised entities to establish cybersecurity governance structures, create and implement risk management frameworks and practices, and implement information controls; delegate responsibility to boards and senior management to manage cyber risks and develop an enterprise-level cybersecurity strategy; implement human resource measures and uplift organisational capacity; protect assets like sensitive data and documents, establish access, physical and environmental controls, and put in place operational security procedures; implement cyber incident management practices, security audits and testing; and, report cyber incidents to RBF within 24 hours after becoming aware of the incident.

As a provider of essential services, the Government strives for the highest level of cybersecurity and cyber maturity. Government data and services can be a high-value target for malicious cyber actors, and therefore the Government is committed to bolstering cybersecurity and resilience across its networks, systems and assets. To do this, the Department of ITC Services is investing in advanced capabilities to keep up with the tactics of cyber threat actors and effectively defend the Government from malicious cyber activity. Further investment in innovative cybersecurity technologies will help to manage risks to our government networks, systems and assets. Investments are also being made to uplift our immigration, health records, digital welfare, and national defence networks and systems that hold sensitive biometric data of our citizens.

The Government is committed to strengthening cybersecurity awareness across the civil service. Civil servants play a vital role in safeguarding data and personal information, and the Government is investing in regular training and awareness programs to build their skills and confidence. By fostering a security-first culture, we are enhancing institutional resilience, protecting public trust, and ensuring government systems and data remain secure for our community.

Activities

3.1 Uplift the Cybersecurity and Resilience of CI and CIIs

3.1.1 As an immediate first step, the Government will **focus on defining and designating CI and CII sectors** in legislation and regulation. This clarity is vital for directing cybersecurity efforts and resources where they matter most.

3.1.2 To improve visibility of what must be protected, following the definition and designation of sectors, the Government will partner with sectors to **conduct a risk assessment of CI and CII sectors and their systems, data and assets**. The results of the risk assessments will help to inform the revision of frameworks, incident response plans and future resourcing requirements.

3.1.3 As part of the national cyber website, the Government will **create a reporting channel for CI and CII operators** for nationally significant cyber incidents that may affect the delivery of Fiji's essential goods and services.

3.1.4 The Government will **mandate minimum reporting timeframes** for CIs and CIIs if they become aware that they are affected by a cyber incident or attack. These reforms will be undertaken in consultation with CIs and CIIs, supporting Fiji to swiftly recover from cyber incidents affecting essential services, the economy and national security.

3.2 Provide Guidance and Undertake Activities to Build Cyber Preparedness

3.2.1 The Government will **create a CI and CII Cyber Information Hub** on the national cyber website. The Hub will be a central point for guidance on obligations and expectations, toolkits and checklists for cyber preparedness and uplift, and recovery guidelines aligned with ISO 22301 on managing business continuity.

3.2.2 The Government will work will conduct targeted consultations with CI and CII operators to co-design **mandatory cyber incident response plans** for designated CI and CII entities.

3.2.3 CIs and CIIs will be required to engage in the national cyber drills and exercises delivered by Fiji CERT. CI and CII sectors will also be encouraged to undertake **sector-specific cyber drills and exercises**.

3.3 Promote Cyber Risk Management Practices and Set Expectations of Industry

3.3.1 The Government will engage with CIs and CIIs to develop a **Cyber Risk Management Policy** that applies across sectors. This would include minimum cybersecurity obligations for CIs and CIIs, including baseline cybersecurity obligations, expectations on standards adoption, and data protection requirements.

3.3.2 The Government will work with CIs and CIIs to create **expectations and requirements for Executives in cyber governance** in their organisations. Fiji CERT will host cybersecurity workshops for Executives and Boards to raise awareness of cyber incident response, risk management, cyber insurance, business continuity, aligning with international standards and best practices.

3.3.3 The Government will continue to consult with CIs and CIIs on how it can help entities to better manage the consequences of cyber incidents. This includes considering last resort **consequence management assistance** when entities are overwhelmed with a cyber crisis. Focus will be placed on secondary consequences or the disruptions that result from a cyber incident, such as supply chain failures, public service outages, or economic effects.

3.4 Protect and secure our government networks, assets and data

3.4.1 The Government will **establish a 24 by 7 Security Operations Centre** (SOC) under the Ministry of Communications. The SOC will be the frontline for detecting, analysing, and responding to cyber threats targeting GOVNET. The SOC will monitor and identify suspicious activities or security breaches and provide early warnings to mitigate risks.

3.4.2 Building on the ITC Review, the Government will **prioritise modernisation of government systems and infrastructure**. This includes investing in innovative, secure-by-design technologies for monitor and detect cyber incidents targeting Government systems and networks, and infrastructure upgrades to the Government Data Centre. It will also include updating policies and standard operating procedures for Ministries on cybersecurity and cyber incident reporting.

3.4.3 The Government will identify its "crown jewels" and **conducting regular vulnerability assessments and penetration testing** of its systems and networks. These activities ensure Fiji's most sensitive national systems, networks, assets and data are protected against cyber threats.

3.4.4 The Government will implement **next-generation cyber threat blocking capabilities** through utilising innovative technologies to block malicious cyber activity at scale. The Government will also encourage CIs and CIIs to implement cyber threat blocking technologies.

3.5 Uplift Cyber Awareness and Good Practices in Government

3.5.1 The Government will build a culture of cyber awareness and good cyber hygiene in the civil service through **online cyber training modules for government**. Training would be developed by the Department of ITC Services, in partnership with the Ministry of Civil Service. Civil servants would be required to undertake this training on a regular basis. This will complement existing in-person cybersecurity awareness training delivered by the Ministry of Communications.

3.5.2 Senior officials of government ministries, agencies and law enforcement will be encouraged to join the Cyber Champions program.

3.6 Promote Adoption of International Cybersecurity Standards and Secure by-design Technologies

3.6.1 The Government will lead by example by integrating **international cybersecurity standards in the National Cyber Incident Response Plan and national cyber exercises**. This will support harmonised application of standards, risk management protocols and incident response practices across public and private sectors.

3.6.2 As part of its legislative review, the Government will identify options to **mandate the adoption of international standards by CIs and CIIs**.

3.6.3 The Government will **publish sector-specific national baselines and maturity models for required standards** to enable benchmarking and inform targeted improvements.

3.6.4 The Government will **develop guidance on third-party data protection and vendor management** for CIs and CIIs, focusing on secure procurement practices, contractual risk management and mitigation and protection of data flows.

STRATEGIC PRIORITY 4

Skilled, Talented and Diverse Cybersecurity Workforce

2031

Goals

- **Fiji has an ongoing talent pipeline of skilled, diverse cyber professionals, and a sustainable cybersecurity workforce.**
- **Fiji's cybersecurity professionals trained by Fijian universities and training institutes are equipped with world-class skills.**
- **Fiji is the most attractive destination in the Pacific for cybersecurity professionals.**

Challenges and Opportunities

Talent attraction and retention in Fiji's cybersecurity workforce is a persistent and growing challenge, driven global demand for skilled professionals. Fiji's local pipeline is limited, with few graduates entering the field and little exposure to cybersecurity at secondary or early tertiary levels. Studies show that there is a global cybersecurity workforce gap of 4.7 million cybersecurity professionals,[iv] highlighting the scale of the issue. For Fiji, this shortage creates pressure to both attract and retain talent against higher-paying employers overseas.

Postgraduate cybersecurity courses exist locally but are insufficient to meet demand. Specialised, practical training aligned with international certifications is urgently needed, yet access in Fiji is limited. The Government is committed to expanding access through online and hybrid learning, regional partnerships, and national training hubs with industry, which will help ICT workers transition into cybersecurity roles and ensure consistent professional development pathways.

Fiji's workforce must also reflect the diversity of its communities, and the Government is focused on supporting diversity and inclusion in the cybersecurity workforce. Women, persons with disabilities, and disadvantaged groups remain underrepresented in the cybersecurity workforce and at the leadership and executive level. Without inclusive strategies, Fiji risks missing out on valuable skills and perspectives that a diverse workforce brings. Public and private organisations must foster inclusive workplace cultures that reduce bias and support career progression. Strengthening diversity will not only sustain the workforce but also enable innovative, user-centred solutions. With the right initiatives in place, Fiji can position itself as a regional leader in cybersecurity workforce development. This long-term investment will pay dividends in strengthening innovation and economic opportunity in Fiji and across the Pacific.

Activities

4.1 Establish Fiji as a Regional Cybersecurity Skills and Training Hub

4.1.1 The Government will partner with the ICT and cybersecurity sector, academia, and CIs and CIIs to **establish a flagship regional Cybersecurity Centre of Excellence**. This will serve as Fiji's focal point for cyber skills and workforce development, innovation and public-private collaboration, positioning our nation as a regional leader in cybersecurity.

4.1.2 Fiji will engage with development partners, international tertiary education partners and international cybersecurity companies to **facilitate international training and knowledge exchanges.**

4.2 Grow and Develop the National Cybersecurity Workforce

4.2.1 The Government will **establish a Cyber Education and Workforce Taskforce**, in partnership with academia. The Taskforce will review and identify gaps in the curriculum, delivery and student experiences of educational and professional training on offer.

4.2.2 The Cyber Education and Workforce Taskforce will **develop a National Cybersecurity Education and Workforce Plan,** to improve educational offerings and quality in Fiji.

4.2.3 The Taskforce will engage with industry to **conduct a survey of sectoral training and skills requirements** and core competencies. Industry feedback will also inform innovative ways to boost the cybersecurity workforce, including how to encourage transition by mid-career professionals into the sector.

4.3 Embed Cybersecurity Education into Primary and Secondary Curricula

4.3.1 The Government will encourage cybersecurity as a career path by continuing to **include cybersecurity in the national education curriculum**. Resources and tailored training will be provided for our educators to teach primary and secondary-level students. This will align with existing efforts by the Ministry of Communications, Ministry of Education, Fiji Police and OSC on cyber safety and literacy and reducing online harms.

4.3.2 The Government will continue to **enhance cybersecurity awareness among women and girls** through the Girls in ICT program, including hands-on workshops and awareness events for women and girls, and mentorship opportunities.

4.4 Expand Tertiary Education and Training Opportunities

4.4.1 The Government will partner with academic and tertiary institutions to **promote specialised courses, degrees and certification programs**, specifically targeting undergraduates. These courses will be complemented by internship and apprenticeship programs to provide hands-on experience for students.

4.4.2 To build foundational awareness and attract more students to the field, the Government will support integrating **cybersecurity content into related degree programs,** such as computer science, ICT and software engineering.

4.4.3 To promote and expose students to real-world problems and evolving cyber threats, the Government will **facilitate academic-industry partnerships** for guest lectures and events, for example Cybersecurity Awareness Month.

4.5 Provide ICT and Cybersecurity Training Opportunities for Civil Servants

4.5.1 The Regional Centre of Excellence will offer opportunities for **technical cybersecurity training for ICT professionals in the civil service,** as well as recognition for and access to international certifications.

4.5.2 Civil servants working in ICT will be offered **short-term rotations in cybersecurity** in Fiji CERT, the Digital Government Transformation Office and the 24 by 7 Government SOC. This will enable greater knowledge, information-sharing and practical experience.

4.6 Promote Gender Balance and Diversity in Cybersecurity Workforce

4.6.1 The Government will work with civil society organisations on **career and leadership pathways for women and underrepresented groups in cybersecurity.** This includes supporting mentorship programs and peer support networks, holding hackathons and innovation labs, and hosting executive masterclasses to promote women in leadership.

4.6.2 The Government will encourage businesses to **implement diversity and inclusion policies** for cybersecurity roles. This includes advocating for measurable diversity targets, addressing gender bias in recruitment and promotion practices and creating inclusive workplace cultures.

STRATEGIC PRIORITY 5

Cybersecurity Leadership and Global Advocacy

2031
Goals

- **Fiji, as a regional leader in cybersecurity, advocates for cross-regional cooperation in cybersecurity. Fiji promotes and implements our regional and global commitments on cybersecurity and combatting cybercrime.**
- **Fiji continues to adhere to international law and promotes international rules and norms of responsible State behaviour in cyberspace.**
- **The Government and civil society actively participate in regional and global forums. Fiji continues to amplify the voices from our Blue Pacific in global cybersecurity and cybercrime forums.**

Challenges and Opportunities

Recognising that cybersecurity is a global challenge that transcends borders, Fiji is committed to meaningful regional and international cooperation on cybersecurity and resilience. Cybersecurity and resilience is recognised as a critical part of our foreign policy, and regional stability.[xiii] As a regional hub and active multilateral partner, Fiji has a unique opportunity to lead on cybersecurity and resilience in the Pacific. By championing rules-based shared values such as sovereignty, openness, and digital inclusion, Fiji shapes a regional approach that reflects the priorities and needs of Pacific SIDS.

Fiji's national approach to international peace and security, including in cyberspace, is guided by the Blue Pacific Ocean of Peace Declaration[xiv], endorsed by Pacific Islands Forum Leaders in September 2025, that reflects the Pacific's commitment to cooperation and consensus-building. The Declaration commits to cultivating a culture of peace grounded in the Pacific Way, which fosters common ground, manages disagreements and reduces tensions. Further, the Declaration calls upon all States and non-State actors to "promote the responsible use of technology and innovation". This aligns with Fiji's emphasis on the Talanoa concept, an approach that promotes respect for international law, rules and norms, reinforcing the UN Charter and the principle of non-interference in States' internal affairs. It opposes the use of economic, political, or military coercion by states to achieve strategic advantages. The Declaration underpins Fiji's commitment to international peace-making efforts, including in cyberspace, and acknowledges the right of States to self-defence and security policies to address evolving threats and challenges.

Case Study: Applying UN Norms of Responsible State Behaviour

At the UN, Fiji and our partners are working to address cyber threats, cybercrime and malicious cyber activity as a global community. UN Member States have developed a cumulative and evolving framework of responsible State behaviour in cyberspace, including non-binding norms. To this end, the Fiji Government is actively engaging with our partners in the UN OEWG to implement the 11 voluntary norms of responsible State behaviour in cyberspace and encourage capacity-building that supports Pacific SIDS to implement norms.

***UN NORMS** OF **RESPONSIBLE STATE BEHAVIOUR** IN CYBERSPACE*

Aligning Fiji's domestic reforms with the norms of responsible state behaviour, such as standing up Fiji CERT, enhancing cybercrime legislation, law enforcement and prosecution, and defining and designating CI and CII, is essential to demonstrating responsible governance. As cyber threats grow more complex and cross-border in nature, aligning to these norms reinforces Fiji's commitment to peace and security in cyberspace.

In May 2025, Fiji supported the development of the PIF Working Paper 'Strengthening Cyber Capacity Building in the Pacific – Connecting Regional Priorities to the UN OEWG Framework'[xv] that argues that effective cyber stability requires not only adherence to UN norms, but also equitable access to implementing them. The paper highlights the needs for contextually appropriate, coordinated, sustainable, inclusive and Pacific-led capacity-building – framing cyber capacity-building as a prerequisite and enabler of Pacific SIDS to uphold and operationalise the UN norms of responsible State behaviour in cyberspace.

Fiji has built deep relationships on uplifting cybersecurity and resilience and combatting cybercrime with partners across the Pacific and beyond. These partnerships have supported Fiji's efforts to strengthen cyber capabilities, improve incident response and build a more secure digital environment for government, businesses, and communities. By working with partners on capacity-building, information-sharing and exchanges and technical cooperation, Fiji has accelerated progress in key areas including combatting cybercrime, cyber incident response, strategy and governance. These relationships also boost Fiji's influence and to regional, cross-regional and global discussions on governance and digital inclusion, including at the PIF, Council of Europe and UN. Continued collaboration and maintaining these strong relationships is important to ensuring Fiji remains cyber-secure and resilient.

Activities

5.1 Prioritise Regional and Cross-regional Coordination and Cooperation

5.1.1 The Government will continue to advocate for and to **embed cybersecurity and resilience in regional digital transformation, security and development agendas**, including in the implementing regional strategies like the Lagatoi Declaration Action Plan. The Government will engage in discussions and coordination on cybersecurity priorities through the Pacific ICT Ministerial Dialogue and other PIF frameworks, the Asia-Pacific Telecommunity and other forums.

5.1.2 The Government will continue to **engage on Pacific priorities with development partners** at regional cybersecurity forums, for example at the Pacific Cyber Coordination and Capacity-Building Conference (P4C) and Pacific Cyber Week. Fiji will advocate for Pacific leadership in cybersecurity, contextualised and fit-for-purpose capacity-building, an improved regional cyber ecosystem, embedded sustainability, and inclusive development.

5.2 Assist Pacific Small Island Developing States to Build Resilience

5.2.1 The Government will continue to strengthen partnerships with our neighbours and play an active role in building cybersecurity and resilience in the Pacific. We will work with PaCSON to share best practices, cyber threat intelligence, technical expertise and resources on cyber incident response.

5.2.2 The Government will position **Fiji CERT as a regional support node** for the Pacific, to provide surge response support for other CERTs at their request.

5.2.3 The Government will strengthen efforts with our neighbours to develop a **shared Pacific cyber incident response playbook**, to promote common procedures, communication protocols, and mutual assistance mechanisms.

5.3 Contribute to regional legal harmonisation

5.3.1 The Government will continue to support efforts to **harmonise cybercrime legislation and electronic evidence standards across the Pacific** aligned with international frameworks, such as the Budapest Convention and the UN Convention against Cybercrime. The Government will leverage the PILON Cybercrime Working Group, the Cybercrime Convention Committee (T-CY) and the UN Global Mechanism to strengthen legal responses and promote harmonised approaches to cybercrime legislation.

5.3.2 The Government will continue to promote the development of **model cybercrime legislation and regional and cross-regional legal toolkits** to support legislative consistency across jurisdictions.

5.4 Uphold International Law, Norms and Rules of Responsible State Behaviour in Cyberspace

5.4.1 The Government will continue to actively engage in international forums to promote and uphold **adherence to international law and voluntary norms** of responsible State behaviour in cyberspace, including at the UN Global Mechanism.

5.4.2 Across all forums, the Government will continue **advocate for the interests and values of Pacific SIDS**, including sovereignty, human rights and peaceful dispute resolution.

5.4.3 The Government will advance the **UN Women, Peace and Security (WPS) Agenda** by promoting gender inclusion and the empowerment of women and girls across all aspects of cybersecurity policy, governance, and capacity-building initiatives. The Government will continue to participate in the Women in Cyber Fellowship to ensure our women cyber diplomats are at the forefront of international peace and security decision-making at the UN Global Mechanism.

5.5 Strengthen key partnerships on cybersecurity and resilience

5.5.1 The Government will deepen **partnerships with our key development partners** to build Fiji's cybersecurity capacity.

5.5.2 The Government will embed **cybersecurity cooperation in our development and security agreements** with international partners to align with our national cybersecurity priorities.

KEY MILESTONES

Phase 1 (2026-2027): Uplift

In Phase 1, we will:

- Commence annual cybersecurity awareness campaigns
- Create the national cyber website
- Define and designate CI and CII sectors
- Stand up the Cyber Champions Program
- Publish resources and guidance for individuals, MSMEs and businesses
- Establish the National Computer Emergency Response Team
- Establish the 24 by 7 Government Security Operations Centre
- Participate in international Cyberdrills
- Develop the National Privacy and Personal Data Protection Policy and draft privacy and data protection legislation
- Stand up the National Executive Cyber Advisory Council and the National Cyber Education and Workforce Taskforce
- Continue to shape international rules and norms, and contribute to confidence building measures at the UN Global Mechanism on Responsible State Behaviour in Cyberspace
- Continue to represent the Pacific Region at the UN Convention against Cybercrime Conference of Parties sessions

Phase 2 (2028-2029): Scale

In Phase 2, we will:

- Roll out online cybersecurity training for individuals and businesses
- Co-design and release the Essential Cybersecurity Good Practice Principles
- Increase investment in Fiji CERT's technology and resourcing
- Formalise protocols for cyber threat intelligence and information-sharing
- Complete upgrading the National Digital Forensic Lab
- Launch the Regional Cybersecurity Centre of Excellence
- Implement the National Cybersecurity Education and Workforce Plan
- Develop a long-term roadmap for implementation of cybersecurity standards
- Forge new cybersecurity partnerships with development partners

Phase 3 (2030-2031): Enhance

In Phase 3, we will:

- Complete scoping for a National Cyber Agency
- Develop comprehensive and fit-for-purpose cybersecurity legislation
- Implement robust cybersecurity standards compliance frameworks
- Launch a public-private cyber threat intelligence exchange
- Invest in critical and emerging cybersecurity technologies for our government networks and systems
- Continue our support for regional legal harmonisation on combatting cybercrime

NEXT STEPS

Governance and Coordination

Implementation of the NCRS and Action Plan will be progressed by the Cyber Affairs Unit in the Ministry of Communications. The Minister for Communications will maintain oversight of whole-of-Government coordination and international engagement on the NCRS and Action Plan and chair the National Cybersecurity and Resilience Strategy Consultative Committee. We will create accountability across responsible ministries and agencies through regular reporting to the Consultative Committee.

Inclusive and Participatory Approach

The Government recognises that not all individuals, businesses or sectors have the same capacity to adopt and implement activities in the NCRS, due to varying levels of cyber maturity, resources, and digital access. To address this, the NCRS and Action Plan are guided by the principles of equity, inclusivity, cooperation and resource availability. Responsibilities for achieving our 2031 Vision are allocated in a way that accounts for these differences, to ensure no group is left behind.

Implementation, Monitoring and Evaluation

The Government recognises that we must continue to ensure our progress is monitored and evaluated so we stay on track to deliver tangible outcomes for all Fijians.

Monitoring and Evaluation Responsibilities

The Government will create a Cyber Affairs Unit in the Ministry of Communications; and increase staffing for monitoring and evaluation, in collaboration with Government stakeholders, CIs and CIIs, private sector and civil society organisations.

The Unit will develop a monitoring and evaluation framework to track progress against the NCRS and Action Plan. This framework will include key indicators that identify how activities will be measured using the SMART framework: Specific, Measurable, Achievable, Responsible, and Time-related.

- **Specific:** our activities are targeted, detailed and focused on our 2031 Vision.
- **Measurable:** using quantitative and qualitative metrics to measure our progress over time.
- **Achievable:** our activities are realistic and sustainable, and consider our budgetary, fiscal and socio-economic environment.
- **Responsible:** our Action Plan identifies the accountable entities responsible for implementation of each activity, and key partners for delivery.
- **Time-related:** our Action Plan identifies implementation of these activities over the three phases.

Budgetary considerations

Resourcing is essential to meet the 2031 Vision in the NCRS. Securing adequate and sustained funding is essential to deliver the goals and activities in the NCRS. Budget allocations must cover both program activities and human resourcing needed for implementation. To ensure agencies are consistently and sufficiently resourced, the monitoring and evaluation framework will consider Government budget cycles.

Reporting

The Government is committed to maintaining open and transparent communication about major cybersecurity reforms and activities, particularly those that affect the community, businesses and critical sectors. We will provide regular updates, undertake outreach efforts, and co-design initiatives with affected groups. This approach will strengthen economy-wide understanding and compliance, ensure reforms are better tailored and more sustainable, and enable more effective implementation of the NCRS.

ANNEX A

Cyber Roles and Responsibilities in the Government of Fiji

Cybersecurity is a cross-cutting policy issue across digital, economic, national security and social welfare policy. The ministries and agencies listed below all play a role in contributing to a safe, secure and cyber-resilient Fiji.

Cyber Policy and Strategy

Ministry of Communications

The Communications portfolio in the Ministry of Policing and Communications is responsible for leading the coordination of national cybersecurity policy and strategy and developing policy and technical advice on all cyber and digital matters including cyber threats. The Ministry's role ensures cybersecurity policy is holistic, proactive and aligned with the Government's digital, economic, foreign policy and security agendas. The Ministry is mandated for oversight of the following legislation:

(i) Telecommunications Act 2008,

(ii) Electronic Transactions (Amendment) Act 2017,

(iii) Online Safety Act 2018,

(iv) Cybercrime Act 2021.

The Ministry has completed the National Privacy and Data Protection Policy and is currently drafting the law. The Ministry is the technical and diplomatic point of contact for the UNOEWG designated Global Directory and represents Fiji as the National Coordinator to the Budapest Convention Committee (T-CY) and is a member of the T-CY Bureau. The Ministry also chairs the National Anti-Scam Taskforce and the National Taskforce to Address Pornography.

Within the Ministry, the following functions exist:

1. Department of Communications

The Department of Communications is responsible for policy and regulation of Fiji's telecommunications and ICT sector including, critical information infrastructure and new and emerging technologies. The Department engages with international partners on cybersecurity and cybercrime-related forums, including at the UN, ITU, and the Council of Europe.

The Cyber Affairs Unit in the Department is responsible for developing cybersecurity policy, overseeing cybersecurity initiatives, and coordinating the implementation of the National Cybersecurity and Resilience Strategy 2026-2031 and Action Plan.

2. National Computer Emergency Response Team (Fiji CERT)

Fiji CERT is the focal point for nationally significant cyber incident response in Fiji. It is responsible for receiving reporting, managing, and responding to cyber incidents affecting government, CIs and CIIs and industry and coordinating responses. Fiji CERT has a central role in strengthening national cybersecurity and resilience, facilitating information sharing and raising awareness of cyber threats. Fiji CERT represents Fiji at regional and international networks and forums on cyber incident response, including PaCSON.

3. Department of ITC Services

The Department of ITC Services Security Operations Centre (SOC) and Network Operations Centre (NOC) are responsible for the cybersecurity of Fiji Government's digital infrastructure, systems and applications, including the government data centre. ITC Services manages the Government Network (GOVNET) and manages the procurement of cyber-secure digital equipment and technologies for government ministries and agencies.

4. Digital Government Transformation Office

The Digital Government Transformation Office (DGTO) is responsible for driving digital transformation of government services. DGTO oversees the digitalFIJI platform and the cyber-secure integration of government services through the Fiji Government Stack, including data exchange infrastructure. DGTO adopts a data protection and cybersecurity by-design in the digitalFIJI initiative. It is responsible for developing and coordinating digital policies including the National Digital Strategy 2025-2030 and Implementation Plan, driving reforms to data security and privacy protections and providing advice to ministries and agencies on digital transformation.

Law Enforcement and Public Safety

Ministry of Policing

The Policing portfolio in the Ministry of Policing and Communications is responsible for overseeing law enforcement policy in Fiji, including the strategic direction and resourcing of the Fiji Police Force to maintain public safety, uphold the rule of law and enable law enforcement to respond to emerging cybercrime threats. The Ministry is responsible for creating a policy and operational environment for the FPF's enforcement of the Cybercrime Act 2021.

Fiji Police Force

Fiji Police Force (FPF) is Fiji's unified national law enforcement body, mandated under the Police Act 1965 and the Constitution to uphold public safety and order. It is responsible for investigation and law enforcement of cybercrime offences under the Cybercrime Act 2021.

Cybercrime Unit

The Cybercrime Unit in the Criminal Investigations Department investigates cybercrime cases, collects digital evidence, supports the prosecution of cybercrimes and works closely with regional and international law enforcement partners. The Unit is designated as one of Fiji's 24 by 7 Point of Contact as prescribed by the Budapest Convention. It also coordinates community outreach by police on cyber safety and cybersecurity.

Digital Forensics Unit

The Digital Forensics Unit in the Critical Investigations Department is responsible for analysing digital evidence to support criminal investigations, including those related to cybercrime. It provides specialised technical capabilities such as forensics and analysis, data recovery and verifying the integrity of digital evidence.

INTERPOL National Central Bureau

Fiji' National Central Bureau (NCB) is hosted by the National Police Intelligence Bureau. The NCB cooperates with other bureaus on cross-border investigations, operations and arrests relating to cybercrime activities. The NCB links national law enforcement and other countries through INTERPOL's I-24/7 secure global police communications system.

Office of the Director of Public Prosecutions

The Office of the Director of Public Prosecutions (ODPP) is responsible for prosecuting cybercrime offences under Cybercrime Act 2021 and other relevant cyberlaws. It assesses electronic evidence, prepares legal cases, and leads court proceedings against individuals or entities accused of committing cyber-enabled crimes. The ODPP is Fiji's second 24 by 7 Point of Contact under the Budapest Convention and also works with the FPF and international partners to build prosecutorial capacity in handling complex digital cases and ensuring offenders are held accountable under the laws of Fiji.

National Security and Defence

Ministry of Defence and Veterans Affairs

The Ministry of Defence and Veterans Affairs maintains overall responsibility for the protection of Fiji's national security. It leads the development and implementation of national security policies including the National Security Strategy, supports coordination across security agencies, and contributes to crisis response planning. It is responsible for the development and implementation of policies and measures relating to the protection of critical infrastructure. It maintains the national register of critical infrastructure assets.

Republic of Fiji Military Force

The Republic of Fiji Military Force (RFMF) is responsible for the protection of Fiji's sovereignty across the land and maritime domains. Its secondary responsibilities are to support nation-building activities as determined by the Government. This may include humanitarian & disaster response; infrastructure development; youth programs and outreach; promoting regional stability; and global peacekeeping.

Office of National Security Assessments

The Office of National Security Assessments (ONSA) is an intelligence and advisory hub to enhance national security coordination and situational awareness across agencies. It works with Fiji CERT to integrate cyber threat intelligence into security assessments.

Cyber Safety and Online Safety

Online Safety Commission

The Online Safety Commission (OSC) is responsible for promoting safe and responsible online behaviour and preventing harmful online communications. It provides a complaints mechanism for individuals

affected by cyberbullying, image-based abuse, and other online harms. OSC also plays an educational role by raising public awareness about online safety and supporting a safer digital environment for all Fijians, especially children, youth and vulnerable groups.

National Taskforce to Address Pornography

The Taskforce is a multi-stakeholder and agency initiative co-chaired by the Minister for Policing and Communications and the Minister for Women, Children and Social Protection. The Taskforce focuses on addressing the impacts of the proliferation of pornography across society. The primary workstream under the Taskforce is dedicated to addressing the impacts and harnessing a collective and holistic response to OCSEA and the proliferation of CSAM.

National Anti-Scam Taskforce

The Taskforce is a multi-agency initiative that brings together key stakeholders from Government, law enforcement, regulatory agencies and the private sector to monitor scams, release public alerts, undertake legislative review, boost consumer protections and run public awareness campaigns.

Fiji Competition & Consumer Commission

The Fiji Competition and Consumer Commission (FCCC) is responsible for promoting fair competition, regulating prices and protecting consumer rights to ensure a transparent and efficient marketplace in Fiji. FCCC plays a key role in cyber safety and protecting consumers from scams by monitoring deceptive digital practices, issuing public alerts and investigating unfair conduct in online marketplaces.

Ministry of Women, Children & Social Protection

The Ministry of Women, Children & Social Protection (MWCSP) is responsible for promoting the welfare, rights, and protection of vulnerable groups in Fiji. It plays a role in awareness, advocacy and protection measures to prevent online abuse, exploitation, and technology-facilitated gender-based violence against women, children and disadvantaged people. The Ministry also works in partnership with agencies like the OSC and the Ministry of Communications to advance digital inclusion and ensure that social protection policies address the risks associated with harmful online behaviour.

Ministry of Education

The Ministry of Education plays a key role in promoting cyber safety and is responsible for integrating digital literacy, online safety and cybersecurity into school curricula, equipping students with the skills to navigate cyberspace responsibly. It partners with the OSC and the Ministry of Communications to raise **awareness and protect children from online harms such as cyberbullying and exploitation.**

Ministry of Civil Service

Ministry of Civil Service responsible for leading human resource management, capability and capacity-building, and workforce policy across the Fijian public sector. In the context of cybersecurity, it supports the development of a digitally skilled and cyber-aware civil service by facilitating cyber awareness-raising and training.

Ministry of Information

The Ministry of Information is the Government's primary information agency responsible for informing the public about government policies, programmes and plans. It manages the Fiji Government official website that serves as the government's information portal. It also collects, collates and disseminates Government information to the public through mainstream media and social media. It has a role in preventing misinformation and disinformation relating to government policies and programs.

Legislation and Legal Reforms

Office of the Attorney-General

The Attorney-General (AG) is the Government's chief legal advisor, providing independent counsel on constitutional, legislative and administrative matters, and representing the State in civil litigation and other legal proceedings, as mandated by the Constitution and enabling legislation. The AG is responsible for drafting and publishing laws, in consultation with the relevant ministry, for submission to Cabinet and Parliament, ensuring Fiji's legal framework is consistent with the Constitution, international conventions and legal best practices. The AG represents Fiji in key international legal forums.

Solicitor-General's Office

The Solicitor-General's Office (SG's Office) provides legal advice and opinions to government ministries and agencies, supporting drafting legislation including cyberlaws, vetting legal instruments and advising on Fiji's obligations under international frameworks including the Budapest Convention on Cybercrime. The SG's Office supports the Attorney-General in ensuring legal coherence across national security, privacy and cyber and digital issues.

Law Reform Commission

The Law Reform Commission is an independent statutory body responsible for reviewing, modernising, and recommending reforms to Fiji's laws to ensure they are fair, relevant and effective. In the context of cyber, the Commission may review existing laws or propose new legal frameworks to address new and emerging considerations.

Regulators of Critical Sectors

Telecommunications Authority of Fiji

The Telecommunications Authority of Fiji (TAF) is the national regulator for the telecommunications sector, responsible for ensuring fair competition among service providers. It plays a key role in universal access to reliable and affordable telecommunications services, including oversight of network infrastructure and service quality. TAF supports the adoption technical standards and coordinates with other agencies on the resilience and security of Fiji's critical information infrastructure.

Reserve Bank of Fiji

The Reserve Bank of Fiji (RBF) is the national central bank responsible for maintaining financial stability, regulating the monetary system and supervising licensed financial institutions. It plays a key role in cybersecurity by setting regulatory standards like the Prudential Supervision Policy Statement No. 2 regulation aligned with ISO 27001 for managing cyber risk in the banking and payments sector. The RBF is a partner of PaCSON.

Financial Intelligence Unit

The Financial Intelligence Unit (FIU) is responsible for collecting, analysing and disseminating financial intelligence related to money laundering, terrorist financing and other serious financial crimes. It works closely with law enforcement and international counterparts in cases involving cyber-enabled financial crimes and scams.

Regional and International Partnerships and Cooperation

International Networks and Communities

Pacific Islands Forum

The Pacific Islands Forum (PIF) is the region's premier political and economic policy organisation, bringing together Pacific leaders to advance collective action on regional priorities, including digital transformation and cybersecurity. Fiji plays an active role in PIF mechanisms such as the Pacific ICT Ministers Dialogue and implementation of the Lagatoi Declaration and Action Plan which commits members to secure, inclusive, and resilient digital development. Fiji's engagement with PIF helps ensure that cybersecurity is embedded within the 2050 Strategy for the Blue Pacific Continent. The PIF Secretariat publishes the Pacific Security Outlook Report annually.

Pacific ICT Ministers Dialogue

The Pacific ICT Ministers Dialogue is a high-level annual forum where ICT Pacific ministers meet to discuss and coordinate regional ICT, digital development, infrastructure, and cybersecurity priorities. The Lagatoi Declaration on the Digital Transformation of the Pacific, endorsed at the 2023 Dialogue in Papua New Guinea and the 2025 Action Plan endorsed in Fiji, sets out a shared vision for secure, trusted and inclusive digital transformation across the region.

Pacific Cyber Capacity-Building and Coordination Conference

The Pacific Cyber Capacity Building and Coordination Conference (P4C), hosted by the Partners in the Blue Pacific, is a regional forum focused on Pacific-led, coordinated, sustainable and contextualised cybersecurity and cyber safety capacity-building.

Pacific Cyber Security Operational Network

The Pacific Cyber Security Operational Network (PaCSON) is a multi-national Pacific operational cybersecurity community. PaCSON promotes sharing of cyber threat information, tools, techniques and ideas between Pacific nations. Fiji is a founding member of PaCSON and attends events and capacity-building.

Asia Pacific Computer Emergency Response Team

The Asia Pacific Computer Emergency Response Team (APCERT) is a trusted contact network for collaboration across CERTs and Cyber Security Incident Response Teams (CSIRTs) in the Asia Pacific.

Forum for Incident Response Security Teams

The Forum of Incident Response Security Teams (FIRST) is a global network of computer emergency or incident response teams aimed at improving incident coordination and promoting best practices. FIRST provides a platform for knowledge sharing, technical collaboration, and capacity-building among national CERTs, industry and academia worldwide.

Asia-Pacific Network Information Centre

The Asia-Pacific Network Information Centre (APNIC) is an open, member-based, not-for-profit organization, whose primary role is to distribute and manage Internet number resources (IP addresses and AS numbers) in the Asia Pacific region. APNIC helps build essential technical skills across the region, supports internet infrastructure development, and is actively involved in internet cooperation and governance.

Pacific Islands Law Officers' Network

The Pacific Islands Law Officers' Network (PILON) is a regional forum of senior law officers and legal advisers. PILON members work to address domestic and regional law and justice issues. PILON supports efforts by the region to combat cybercrime by facilitating capacity-building, legal harmonisation and regional cooperation.

Pacific Islands Chiefs of Police

The Pacific Islands Chiefs of Police (PICP) is a regional organisation comprising the heads of police from Pacific Island countries, focused on enhancing law enforcement cooperation, capability, and regional security. It plays a key role in transnational crime prevention in the Pacific, including cybercrime.

Cyber Safety Pasifika

The Cyber Safety Pasifika Program (CSP) is a PICP initiative is aimed at building law enforcement capacity across the region to address cybercrime and promote online safety. CSP provides training and operational support to Pacific police forces, including Fiji Police Force, to strengthen investigation skills and deliver cyber and online safety awareness programs in communities.

Multilateral and Bilateral Partners

International Telecommunications Union

The International Telecommunications Union (ITU) is the specialised agency of the United Nations responsible for ICTs, supporting global standards, connectivity and digital development. Fiji became a member of the ITU in 1971. Fiji partners with the ITU through capacity-building initiatives, technical assistance and policy guidance on areas such as digital transformation and cybersecurity. The ITU provided technical support for Fiji's National Digital Strategy 2025-2030. In 2015, ITU also supported a study and analysis into Fiji's cybersecurity needs and the institutional and organisational requirements for a national CERT, and training on the operations and maintenance of a CERT.

Council of Europe

Fiji has a longstanding partnership with the Council of Europe on cybercrime and data protection. Following the passage of the Cybercrime Act 2021, Fiji acceded to the Budapest Convention on Cybercrime in December 2024, reinforcing its commitment to international cooperation and legal harmonisation in combating cybercrime. Through the GLACY+ and GLACY-e initiatives, Fiji has received targeted support in strengthening cybercrime legislation, developing prosecutorial and judicial capacity, and improving the handling of electronic evidence. These partnerships have enhanced Fiji's ability to respond to cybercrime threats and participate effectively in global cooperation frameworks. The Council of Europe supported the development of Fiji's National Privacy and Personal Data Protection Policy and is providing support for the legal framework on data protection. Fiji is a Bureau Member of the Budapest Convention Committee (T-CY).

Commonwealth Telecommunications Organisation

Fiji is a member of the Commonwealth Telecommunications Organisation (CTO), the Commonwealth's intergovernmental organisation in the field of ICTs. Fiji was Council Chair of the 2019 CTO Forum and Vice Chair in 2016. The CTO, in partnership with the University of Oxford's Global Cyber Security Capacity Centre, conducted Fiji's first Cybersecurity Maturity Model for Nations (CMM) Review in 2015 that benchmarked Fiji's cybersecurity posture.

Australia

Under the elevated Vuvale Partnership, Australia and Fiji share a commitment to regional peace and security and engage in bilateral cooperation on cybersecurity and resilience, online safety and cyber incident response. In April 2024, Australia and Fiji signed a Memorandum of Understanding on Cyber Security Cooperation that provides a framework for continued engagement and capacity-building. Australia has provided technical assistance to uplift Fiji's cybersecurity governance, policy and strategy and critical information infrastructure. Australia has provided incident response support to critical sectors in Fiji under the Cyber Rapid Assistance for Pacific Incidents and Disasters (RAPID) Program.

New Zealand

Under the Duavata Partnership, New Zealand and Fiji have a shared commitment to cooperation on regional peace and security, with cybersecurity as a mutual priority. New Zealand supports Pacific Island countries including Fiji to uplift their cybersecurity and resilience through CERT NZ's Pacific Partnerships Programme and the Pacific Cybersecurity Capacity Building Fund.

European Union

The European Union, through the EU CyberNet capacity-building program, supports Fiji's cybersecurity through enhanced cooperation on cyber learning, data protection and cyber professional uplift.

United States

The US supports Fiji's cybersecurity efforts through regional capacity-building under the Digital Connectivity and Cybersecurity Partnership (DCCP) initiative. The DCCP supports cybersecurity capacity-building, policy development and technical assistance.

United Kingdom

The UK supports Fiji's cybersecurity efforts through technical assistance, policy development and capacity-building. The UK, supported the development of Fiji's second Cybersecurity Maturity Model for Nations (CMM) Review through its Cyber Capacity Building Fund, a dedicated program that supports countries in the Indo-Pacific to build their cybersecurity.

Israel

Israel and Fiji signed the Memorandum of Understanding on Digital Security and Cybersecurity in October 2025, which enables technical assistance on cybersecurity, cyber incident response and cyber awareness. Israel and Fiji have committed to enhanced information-sharing on cybersecurity.

Japan

Japan's support for Fiji's cybersecurity efforts is focused on capacity-building and technical cooperation, particularly on critical infrastructure cybersecurity. In June 2025, Fiji and Japan signed a Record of Discussions for the Government of Japan's Technical Cooperation Project for Improving Cybersecurity Capability in the Pacific Islands, aimed at enhancing critical infrastructure cybersecurity for Fiji and the Pacific through training and awareness-raising.

Republic of Korea

South Korea's support for Fiji's cybersecurity efforts is focused on capacity-building relating to strengthening cyber resilience and critical infrastructure cybersecurity under the Korea Digital Development (KoDI) Program.

ANNEX B

Glossary of Key Terms and Acronyms

Term	Definition
5G	Fifth generation of wireless technology.
Artificial Intelligence (AI)	The simulation of intelligence processes by machines, especially computer systems.
Availability	The property of data and systems being accessible and usable on demand by authorised users.
Backup	A copy of data stored separately to allow recovery in case of data loss or corruption.
Child Sexual Abuse Material (CSAM)	Any visual depiction of sexually explicit conduct involving a minor, including real, morphed, or computer-generated images that appear to depict a minor.
Computer Emergency Response Team (CERT)	A group of cybersecurity experts that handle incidents and coordinate responses to cyber threats at a national or organisational level. Also known as a Computer Security Incident Response Team (CSIRT).
Confidentiality	The assurance that information is only accessible to those with authorised access.
Consumer fraud	Deceptive, unfair or misleading practices intended to cause a consumer to part with money, property or sensitive information under false pretences.
Critical Information Infrastructure	Communications infrastructure (real or virtual), assets, networks and systems of national significance. This may include telecommunications networks, data centres, and subsea cables.
Critical Infrastructure	Systems and assets vital to national security, economy, public health or safety, the loss or compromise of which would have a significant impact.
Crown jewels	Important digital assets of an organisation, such as intellectual property, personal and financial data, and trade secrets.

Term	Definition
Cyber attack	An attempt to gain unauthorised access to system services, resources, or information, or an attempt to compromise system integrity.
Cyber bullying	Bullying that takes place over digital devices or platforms, including threats and harassment online.
Cybercrime	Criminal offences against the confidentiality, integrity and availability of computer data and systems. In Fiji, offences are defined in the Cybercrime Act 2021.
Cyber extortion	Criminal demand for payment or ransom in exchange for stopping or reversing a cyber attack. See: Data extortion, Ransomware.
Cyber hygiene	Basic cybersecurity and safety practices and steps for individuals and organisations, for example using strong passwords and passphrases; installing software updates; and turning on multi-factor authentication.
Cyber incident	An unwanted or unexpected cyber security event, or a series of such events, that has either compromised business operations or has a significant probability of compromising business operations
Cybersecurity Incident Response Plan (CIRP)	A document that outlines the plan for how an organisation will respond to a cyber incident or attack. Also known as a CSIRP.
Cyber resilience	The ability to detect, manage and recover from cyber incidents. This includes individuals and entities adopting and implementing appropriate cybersecurity controls, measures, safeguards and practices.
Cybersecurity	Measures used to protect the availability, integrity and confidentiality of information and data, applications, systems, operational networks and technologies.
Cyber safety	The safe and secure use of information and communications technologies such as the internet, computers, mobile phones, social media and apps.
Cyber threat actor	An individual or organisation that commits malicious cyber activity or have the intention or willingness to do so. In general, cyber threat actors target vulnerable computers or internet-connected devices, networks, systems and applications to conduct their activities.
Data breach	A breach of security by any person leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Data protection	Ensuring that personal data is collected, stored, processed and shared in a lawful, fair and transparent manner, and that individuals maintain control over their data.

Term	Definition
Data security	Security measures to protect the confidentiality, integrity and availability of data.
Data sovereignty	The concept that data is subject to the laws and governance structures within the nation it is collected or stored
Data theft extortion	An attack in which an adversary demands payment in exchange for not carrying out a threat such as releasing data or exposing a vulnerability.
Deepfake	A video or image of a person created using AI techniques, in which their face and/or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information.
Denial-of-service (DoS) attack	An attempt by malicious actors to prevent legitimate access to online services (typically a website), for example, by consuming the amount of available bandwidth or the processing capacity of the server hosting the online service.
Digital asset	Any item of text or media formatted into a binary source that includes the right to use it, such as digital documents, images, or videos.
Disinformation	False information deliberately spread to influence public opinion or obscure the truth.
General Data Protection Regulation (GDPR)	A regulation in European Union law on data protection and privacy in the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA.
Hack	The unauthorised exploitation of weaknesses in a computer system or network.
Indicator of compromise (IOC)	A piece of digital forensics and evidence that suggests a cyber attack has occurred.
Information classification	The process of categorising data based on its level of sensitivity and required protection.
Information security	The protection of information from unauthorised access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.
Integrity	The assurance that data has been created, amended or deleted only by authorised individuals.

Term	Definition
Internet of Things (IoT)	The network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors and network connectivity, which enables these objects to connect to the internet and collect and exchange data.
ISO 27000 series	ISO's family of standards relating to standards on information security, cyber security and privacy protection.
ISO 27001	ISO's standard for Information Security Management Systems.
Malicious cyber actor	An individual or organisation that conducts malicious activities, such as cyber espionage, cyber attacks or cyber-enabled crime.
Malicious software (malware)	Any software that brings harm to a computer system. Malware can be in the form of worms, viruses, Trojans, spyware, adware which steal protected data, delete documents or add software not approved by a user.
Misinformation	Incorrect or misleading information.
Multi-factor authentication (MFA)	Authentication using two or more different authentication factors. This may include something users know, something users have or something users are.
Online child sexual exploitation and abuse (OCSEA)	Any form of child sexual abuse partly or entirely facilitated by digital technology (the internet or other wireless communications).
Online safety	Protection from harmful online behaviours like cyberbullying, cyber-stalking and misuse of digital platforms for harm.
Personal data	Any information or data, whether included in a record or not, relating to an identified or identifiable individual, or which may allow to single out or individualise one person from others.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details), encouraging them to open a malicious attachment, or visit a fake website that will ask the user to provide sensitive information or download malicious content.
Ransomware	A common type of malicious software that makes data or systems unusable until the victim makes a payment. A ransom, typically cryptocurrency, is demanded by the malicious cyber actor to restore access and functionality of systems.

Term	Definition
Recovery plan	A plan that outlines an organisation's recovery strategy for how they are going to restore IT systems, operational technology or other functions following a cybersecurity incident. Similar to a CIRP.
Scam	A fraudulent scheme performed by a dishonest or deceitful individual, group or company to obtain money or something else of value.
Security assessment	An activity undertaken to assess controls for a system and its environment to determine if they have been implemented correctly and are operating as intended.
Security-by-design	A software development principle whereby security is designed into every stage of a product or service's development.
Security breach	An act that leads to damage of a system or unauthorised access to the system.
Social engineering	The methods used to manipulate people into carrying out specific actions, or divulging information.
State-sponsored actor	A malicious cyber actor that conducts activity on behalf of a state, for example, a contracted hacker or company.
Vulnerability	A weakness in a system's security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited, and result in a violation of the system's security policy.
Website defacement	Illegitimate changes made to the appearance and content of a website. Often likened to graffiti or online vandalism.

NATIONAL STRATEGIES AND FRAMEWORKS

National Development Plan 2025-2029 & Vision 2050

National Digital Strategy 2025-2030

National Security Strategy 2025-2029

National Security & Defence Review 2024

Foreign Policy White Paper 2024

National E-Commerce Strategy 2025-2029

National MSME Strategic Plan 2025-2030

Fiji Cybersecurity Maturity Model for Nations Review 2024

REGIONAL AND INTERNATIONAL FRAMEWORKS

2023 Pacific ICT Ministers' Lagatoi Declaration on Digital Transformation in the Pacific

2025 Lagatoi Declaration Action Plan

2025 Blue Pacific Ocean of Peace Declaration

2018 Boe Declaration on Regional Security

2050 Strategy for the Blue Pacific Continent

2001 Budapest Convention on Cybercrime of the Council of Europe

2021 Second Additional Protocol to the Budapest Convention

United Nations General Assembly, '24 July 2025 Final Report of the Open-ended working group on the security of and in the use of information and communications technologies 2021-2025' (A/80/257)

United Nations Convention against Cybercrime (A/RES/79/243)

REFERENCES

[i] Pacific Information Communication Technology Ministerial Dialogue 2023, 'Pacific ICT Ministerial Declaration 2023', 28 August 2023.

[ii] World Economic Forum, 'Global Risks Report 2025'.
www.weforum.org/publications/global-risks-report-2025/

[iii] Estefania Vergara Cobos and Selcen Cakir. 'A Review of the Economic Costs of Cyber Incidents', World

Bank, 2024.
documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf

[iv] IBM, 'Cost of a Data Breach Report 2024'.
www.ibm.com/reports/data-breach

[v] An overview of the SolarWinds cyber attack is available at the SolarWinds website.
www.solarwinds.com/blog

[vi] An overview of the Qantas cyber incident is available on the Qantas website.
www.qantasnewsroom.com.au/qantas-responds/update-on-july-cyber-incident/

[vii] ISC2 Cybersecurity Workforce Study, '2024 ISC2 Cybersecurity Workforce Study', 31 October 2024.
www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study. Global Cybersecurity Forum & Boston Consulting Group, '2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap', 2 October 2024. gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap/

[viii] National Center for Missing and Exploited Children, 2024 Cyber Tipline Report.
www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

[ix] Ministry of Trade, Co-operatives, Micro, Small and Medium Enterprises and Communications, 'Online Safety Commission joins forces with WeProtect Global Alliance to advance child protection online', 29 November 2023.
www.mctt.gov.fj/online-safety-commission-joins-forces-with-weprotect-global-alliance-to-advance-child-protection-online/

[x] Permanent Mission of Germany to the United Nations and the Australian Government Department of Foreign Affairs and Trade, 'Gender Perspectives on Cyber Capacity Building at the OEWG and Beyond', UN OEWG Side Event - Ninth Substantive Session, 5 December 2024.
https://unodaweb-meetings.unoda.org/public/2024-11/OEWG%20Side%20Event%20Gender%20Perspectives%20in%20CCB_Concept%20Note.pdf.

[xi] Microsoft, 'Digital Defense Report 2023'.
www.microsoft.com/en-sg/security/security-insider/microsoft-digital-defense-report-2023

[xii] UN Capital Development Fund, 'Assessing Digital and Financial Literacy in Fiji: A Survey on Knowledge, Skills and Access', 23 July 2023.
www.uncdf.org/article/8317/assessing-digital-and-financial-literacy-in-fiji-a-survey-on-knowledge-skills-and-access

[xiii] Ministry of Foreign Affairs, 'Foreign Policy White Paper 2024', 23 September 2024.
https://www.foreignaffairs.gov.fj/foreign-policy-white-paper-2/

[xiv] Pacific Islands Forum Secretariat, 'Fifty-Fourth Pacific Islands Forum Communiqué Annex 3: Blue Pacific Ocean of Peace Declaration', 12 September 2025.
https://forumsec.org/publications/leaders-communique-54th-pacific-islands-forum-leaders-communique

[xv] Pacific Islands Forum Member States, 'Working Paper: Strengthening Cyber Capacity Building in the Pacific – Connecting Regional Priorities with the UN OEWG Framework', May 2025.
https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/PIF_Working_Paper_on_ICT_capacity_building.pdf

Ministry of Policing and Communications