PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

ANNUAL REPORT 2024

TLP:CLEAR = Disclosure is not limited.

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.

Contact details and feedback

Feedback about this report is welcome, and should be directed to:

The PaCSON Secretariat: pacson.secretariat@defence.gov.au

ANNUAL REPORT

2024

Table of contents

Chair remarks

Chair remarks

Kia Orana and warm Pacific greetings,

It has been both an honour and a privilege for the Cook Islands, through the Office of the Prime Minister, to serve as Chair of the Pacific Cyber Security Operational Network (PaCSON) for 2023–24. Over the past year, we have witnessed a period of tremendous growth, collaboration and strategic maturing within our network. As we transition this role to our colleagues from Kiribati, we reflect not just on achievements, but on the collective spirit that binds the PaCSON community.

And on a personal note, this Annual General Meeting (AGM) in Rarotonga also marked **my very first week on the job**. Talk about jumping into the deep end! But what a team to connect with, and what an inspiring community to become a part of. From day one, I've seen first-hand the passion and purpose that drives this network, and I couldn't ask for a more dedicated, welcoming and forward-thinking group of regional cyber leaders.

A year of expansion and connection

2024 marked the most significant expansion in PaCSON's history. We proudly welcomed the **Federated States of Micronesia** into our membership, and extended our family through new partnerships with the French cyber security agency ***Agence nationale de la sécurité des systèmes d'information***, the ***Canadian Centre for Cyber Security***, and the ***Pacific Fusion Centre***. These relationships are more than symbolic—they reflect a growing regional and global consensus that **cooperation is our greatest cyber defence asset**.

Together, we are building a network that doesn't just monitor cyber threats, but responds as a resilient and united force across the Pacific. The growing size of our AGM attendees in Rarotonga is testimony to this momentum – indeed, it was the **largest PaCSON AGM to date**.

Cyber resilience in action: AGM highlights

The 2024 PaCSON AGM, held in the heart of our paradise island of Rarotonga, provided the perfect setting to strengthen bonds and deepen our technical capabilities. From the fierce fun of the **Capture the Flag** cyber challenge to the spirited strategic dialogues in our Working Group meetings. Each activity reminded us that cyber security is both a technical endeavour and a human one.

A standout moment for the Cook Islands was the official launch of our **National Cyber Security Strategy**, a key pillar of our broader National Security Framework. This milestone was made even more meaningful as it was shared among regional friends and dignitaries such as the Honourable Tingika Elikana, Minister of Foreign Affairs, and also the Honourable Henry Puna, former Prime Minister.

The AGM also offered a hands-on glimpse into our national digital infrastructure, with site visits to the **Avaroa cable landing station** and the **Vodafone Data Centre** – an opportunity that was both educational and affirming of our digital ambitions.

Progress across Working Groups

The heartbeat of PaCSON lies in its Working Groups, and their 2024 efforts have been nothing short of inspiring. Some notable developments include:

- **Awareness Raising Working Group**: Launch of the vibrant new **Cyber Smart Pacific Campaign**, reinforcing cyber hygiene through familiar Pacific motifs.
- **Capacity Building Working Group**: Plans to relaunch **remote learning initiatives** and welcome **Tonga as co-convenor**.
- **Communications Working Group**: Expansion of the **Cyber Upskill Program** – a flagship training initiative now poised to reach even more of our communities.

These initiatives underscore our belief that everyone in the Pacific – from government officials to grassroots users – must be equipped to face cyber threats with confidence.

Looking ahead with optimism

The challenges before us are real. Ransomware, phishing campaigns, misinformation and geopolitical cyber tensions all threaten our Pacific peace of mind. Yet, through cooperation and shared strategy, we are not standing still – we are moving forward together.

As our term as Chair concludes, we look ahead with optimism and gratitude. To **Kiribati as the incoming Chair**, to **Samoa as Deputy Chair** and to **Papua New Guinea as future Chair**, we pass the baton with full confidence in your leadership and vision.

Final reflections

We offer heartfelt thanks to the PaCSON Secretariat, to our tireless Working Group leads, and to every member who has contributed over the past year. Hosting the AGM in Rarotonga was a privilege, but the real honour was serving this community – one that continues to inspire with its resilience, innovation and deep sense of Pacific solidarity.

This year, we also pause to reflect on the life of **Georgina Kiele of PNG DICT**, a cherished member of our community who sadly passed away. Georgina brought not only technical skill but deep-hearted commitment to our regional work – her contributions to PaCSON will be long remembered. We honour her memory and the positive impact she made in such a short time.

The Cook Islands will always remain a steadfast member of this network and we will continue to champion its mission to secure the digital frontlines of our Blue Continent.

Meitaki maata and thank you.

Cook Islands, Chair, PaCSON Executive Committee

Program overview

Program overview

Established in 2017, PaCSON was created to foster regional cooperation and collaboration, and to ultimately protect the Pacific region's respective information infrastructures and constituents.

PaCSON is an operational cyber security network of regional working-level cyber security experts. PaCSON coordinates activities that aim to benefit the regional network of cyber security incident response professionals. These activities are underpinned by 3 guiding pillars:

- encouraging collaboration on best practice
- increasing threat and information sharing
- supporting and developing incident response capability through training and awareness raising.

The PaCSON network, commonly referred to as the 'PaCSON Community', consists of representatives from eligible Pacific governments and private organisations. Membership of PaCSON includes Australia, the Cook Islands, the Federated States of Micronesia, Fiji, Kiribati, the Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Samoa, the Solomon Islands, Tokelau, Tonga, Tuvalu and Vanuatu.

In support of PaCSON, partners – including government organisations from other nations, not-for-profit organisations and academia – are able to join the network. The partner organisations to PaCSON include:

- Agence nationale de la sécurité des systèmes d'information (ANSSI)
- the Canadian Centre for Cyber Security (CCCS)
- the US Cybersecurity and Infrastructure Security Agency (CISA)
- the US Federal Bureau of Investigation (FBI)
- the Forum of Incident Response and Security Teams (FIRST)
- the Reserve Bank of Fiji (RBF).

In support of PaCSON, friends – including government organisations from other nations, not-for-profit organisations and academia – are able to join the network. The friend organisations to PaCSON include:

- Cyber Safety Pasifika (CSP)
- Global Forum on Cyber Expertise (GFCE)
- Pacific Fusion Centre (PFC)
- Australia's eSafety Commissioner.

PaCSON is not a Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT) and does not provide an incident response capability. Instead, the network maintains operational cyber security points of contact and empowers members to share cyber security threat information; provides opportunities for technical experts to share tools, techniques and ideas; and is an enabler of cooperation and collaboration, particularly where a cyber security incident affects the region.

The direction of PaCSON is guided by the Executive Committee (EC), which provides leadership on behalf of the whole PaCSON community. The EC is empowered to make decisions on behalf of PaCSON and is responsible for the management and direction of PaCSON. All PaCSON members are eligible to nominate for any of the EC positions.

In 2023–24, the structure of the PaCSON EC included:

Chair	Cook Islands
Deputy Chair	Papua New Guinea
Incoming Chair	Kiribati

In 2024–25, the structure of the PaCSON EC is:

Chair	Kiribati
Deputy Chair	Samoa
Incoming Chair	Papua New Guinea

The PaCSON community and the EC are supported in all matters by the PaCSON Secretariat. The function of the PaCSON Secretariat is performed by the Australian Cyber Security Centre (ACSC). The ACSC absorbs all the costs associated with this function. The PaCSON Secretariat supports PaCSON members and PaCSON partners to be part of a cooperative and collaborative community; maintains records and updates documentation; arranges and supports EC meetings; and coordinates arrangements for AGMs, cyber security information exchanges, and cyber security workshops.

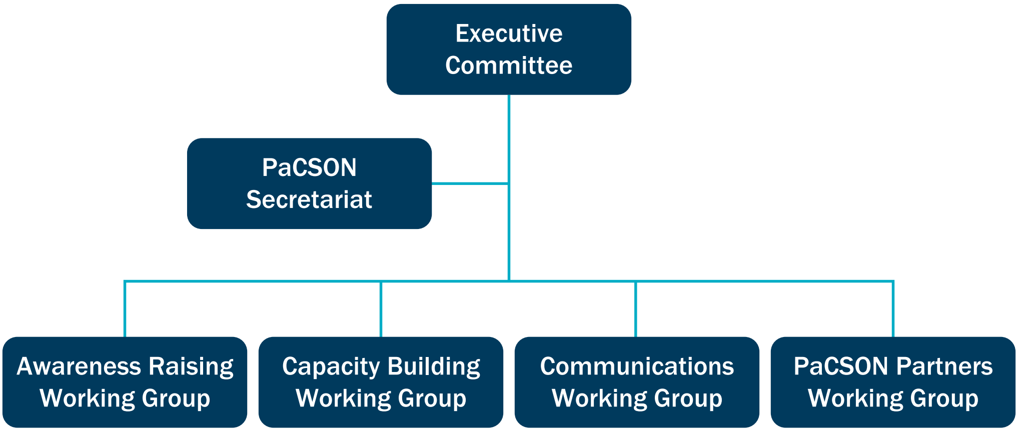

Executive Committee
PaCSON Secretariat
Awareness Raising Working Group
Capacity Building Working Group
Communications Working Group
PaCSON Partners Working Group

Figure 1: PaCSON governance structure

Mission

Work together across the Pacific to cooperatively and collaboratively develop collective cyber security incident response capabilities; enhance technical skills and knowledge; share cyber security threat information; and reflect best practice in order to strengthen our cyber security defences.

Vision

Improve cyber security capabilities and readiness across the Pacific through cooperation and collaboration among those responsible for coordinating national responses to cyber security incidents.

2024 PaCSON Annual General Meeting

2024 PaCSON Annual General Meeting

Overview

The 2024 PaCSON AGM was held from 9 to 12 September in Rarotonga, Cook Islands, at the Edgewater Resort and Spa. The four-day AGM was held in tandem with the half-day intersessional Pacific Cyber Capacity Building and Coordination Conference (P4C). The AGM presented an opportunity for the PaCSON community – members, partners, friends and observers – to come together to share information, learn from one another and collaborate.

The 2024 PaCSON AGM was the largest to date, with over 60 participants from 19 countries – a clear demonstration of the continued growth and development of the community. The opportunity to come together as a group was invaluable and offered a chance to reflect on the work that has been done, while simultaneously looking towards the future.

The AGM program was as follows:

- Day 1: Opening Ceremony and Capture the Flag cyber challenge.
- Day 2: Members-only day with AGM governance proceedings, Working Group meetings, followed by a public launch of the Cook Islands Cyber Security Strategy and a formal dinner.
- Day 3: Working Group updates and community and guest presentations.
- Day 4: Visit to the Avaroa Cable Limited (ACL) landing site and Vodafone Data Centre and community presentations.

Executive Committee election

The AGM serves as a handover between the outgoing and incoming PaCSON EC. The announcement of the new EC came following an open nomination period prior to the AGM. The nominees for the 2024–25 PaCSON EC ran unopposed, rendering a formal vote unnecessary.

PaCSON 2024–25 EC:

- Chair: Kiribati
- Incoming Chair: Papua New Guinea
- Deputy Chair: Samoa.

Priorities discussion 2023–24

PaCSON members revisited the 2023–24 priorities. These priorities are listed and measured in the 2024 outcomes section of this report.

Priorities discussion 2024–25

Following on from the 2023–24 priorities discussion, members moved to discuss the 2024–25 priorities. These priorities are listed in the 2024 outcomes section of this report.

Future plans 2025

2024–25 priorities

Below is a list of the 2024–25 priorities, which will be reported on in the 2025 annual report. These priorities were decided at the 2024 AGM, and were published in the 2024 AGM wrap-up report.

- **Solidify PaCSON's position within the regional architecture by formalising its status as a regional body**

  Building on PaCSON's place in the Boe Declaration Action Plan, use existing and new relationships with regional bodies to increase PaCSON's presence and recognition in the region.

- **Increase engagement opportunities internally and externally**

  Prioritise increasing engagement within and external to PaCSON. Encourage active participation and contribution from members, partners and friends. Externally, increase regional engagement to stop duplicating efforts and also establish engagement mechanisms with industry.

- **Encourage information sharing and confidence to seek assistance**

  Further establish PaCSON as a safe and open environment to share information, enabling members to learn from one another and share key insights to increase the region's capabilities and cooperation.

- **Implement a comprehensive PaCSON monitoring and evaluation framework**

  In the spirit of transparency and maturing the network, establish mechanisms to review and share PaCSON priorities, activities and expenditure with the community.

Member Updates

Australia

Australian Cyber Security Centre

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is the Australian Government's technical authority on cyber security. Through the ACSC, ASD brings together capabilities to improve Australia's national cyber resilience. The ACSC's services include:

- providing the Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, via 1300 CYBER1 (1300 292 371)
- providing technical advice and publishing alerts, advisories and notifications on significant cyber security threats
- monitoring cyber threats and sharing intelligence with partners, including through the Cyber Threat Intelligence Sharing platform (CTIS)
- helping Australian organisations respond to cyber security incidents
- providing exercises and uplift activities designed to enhance the cyber security resilience of Australian organisations
- supporting collaboration between over 119,300 Australian organisations and individuals on cyber security issues through ASD's Cyber Security Partnership Program.

ASD's ACSC encourages every organisation and individual who observes suspicious cyber activity, incidents and vulnerabilities to report them at **cyber.gov.au** and to the hotline. ASD provides free technical incident response advice and assistance, 24 hours a day, 7 days a week.

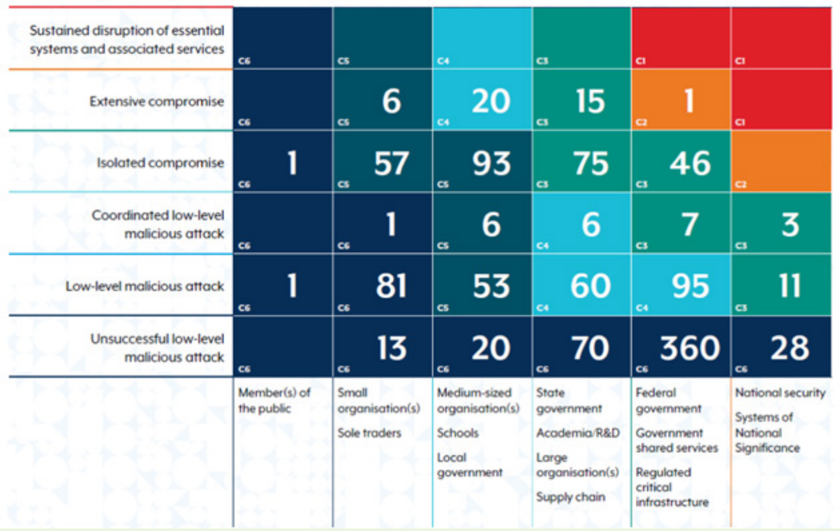
In the 2023–24 financial year (July 2023 to June 2024, ASD's statutory reporting period), the top 3 self-reported cybercrime types for Australian individuals were:

- identity fraud (26%)
- online shopping fraud (15%)
- online banking fraud (12%).

The top 3 self-reported cybercrime types for Australian businesses were:

- email compromise (20%)
- online banking fraud (13%)
- business email compromise (BEC) fraud (13%).

ASD’s ACSC categorises each cyber security incident it responds to on a scale of Category 1 (C1), the most severe, to Category 6 (C6), the least severe. Cyber security incidents are ranked on severity of the incident combined with the significance of the affected organisation to Australia.



Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C1	C1
Extensive compromise	C6	6 C5	20 C4	15 C3	1 C2	C1
Isolated compromise	1 C6	57 C5	93 C5	75 C3	46 C3	C2
Coordinated low-level malicious attack	C6	1 C6	6 C5	6 C4	7 C3	3 C3
Low-level malicious attack	1 C6	81 C6	53 C5	60 C4	95 C4	11 C3
Unsuccessful low-level malicious attack	C6	13 C6	20 C6	70 C6	360 C6	28 C6
	Member(s) of the public	Small organisation(s) Sole traders	Medium-sized organisation(s) Schools Local government	State government Academia/R&D Large organisation(s) Supply chain	Federal government Government shared services Regulated critical infrastructure	National security Systems of National Significance

Figure 2: Cyber security incidents by severity category for FY2023–24

ASD’s ACSC responded to over 1,100 cyber security incidents, around the same as in the previous 2022–23 financial year.

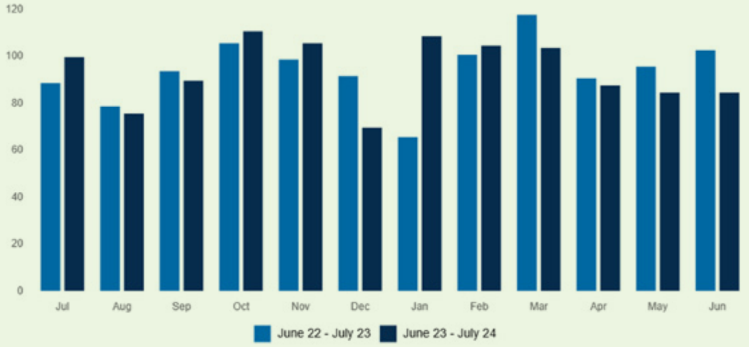


Figure 3: Cyber security incidents by month, 2023–24

Threat landscape

ASD's ACSC provides advice and information about how to protect individuals, families and businesses online. Our role is to help make Australia the most secure place to connect online.

ASD did the following in the 2023–24 financial year:

- notified entities 930 times of potential malicious cyber activity
- Australian Protective Domain Name System blocked customer access to 82 million malicious domains, up 21%
- Domain Takedown Service requested the removal of over 189,000 malicious domains targeting Australian servers, up 49%
- Cyber Threat Intelligence Sharing partners grew by 66% to over 400 partners:
  - shared over 1,372,400 indicators of compromise
- Cyber Hygiene Improvement Program:
  - performed 365 high-priority operational taskings, up 250%
  - distributed around 6,400 reports to approximately 2,000 organisations, up 32% and 48% respectively
- Cyber Uplift Remediation Program:
  - 24 active engagements
  - 17 engagements commenced
- Cyber Maturity Measurement Program:
  - 16 active engagements
- Critical Infrastructure Uplift Program (CI-UP):
  - 10 uplifts completed covering 15 CI assets
  - 5 uplifts in progress
  - 17 uplift information packs sent
  - 42 uplift workshops held
- notified critical infrastructure organisations over 90 times of potential malicious cyber activity
- ASD's Cyber Security Partnership Program grew to around 119,300 partners
- led 16 cyber security exercises involving over 130 organisations to strengthen Australia's cyber resilience
- briefed board members and company directors covering 37% of the Australian Stock Exchange 200

- published or updated 29 PROTECT publications
- updated the Information Security Manual and the Essential Eight Maturity Model
- published 19 joint advisories and publications with international partners to cyber.gov.au
- published 118 alerts, advisories, incident and insight reports on cyber.gov.au and the Partnership Portal.

Case study: Medibank Private and LockBit cyber sanctions

In January 2024, under the Autonomous Sanctions Act 2011, the Australian Government sanctioned Russian national Aleksandr Ermakov for his role in compromising the Medibank Private network in 2022. This was the first use of the Australian Government's autonomous cyber sanctions framework.

Nearly 10 million personal records were stolen during the cyber security incident against Medibank Private, including names, dates of birth, Medicare numbers and sensitive medical information. Some records were published on the dark web.

In May 2024, as part of a separate investigation, the Australian Government imposed Australia's second cyber sanction against Russian national Dmitry Yuryevich Khoroshev, for his senior leadership role in the LockBit ransomware group. LockBit is a prolific cybercriminal ransomware group and works to destabilise and disrupt key sectors for financial gain.

The cyber sanctions that the Australian Government imposed on Ermakov and Khoroshev were targeted financial sanctions and travel bans that acted alongside sanctions that international partners imposed.

Sanctions are an important part of the Australian Government's toolkit in countering cybercrime. Cyber sanctions impose cost on cybercriminals' ability to operate.

- Cyber sanctions reveal the real-world identities of cybercriminals, undermining their credibility.
- For others in the crime ecosystem, affiliating with a sanctioned cybercriminal could be perceived as higher risk.
- Breaching a cyber sanction can be a serious criminal offence, punishable by up to 10 years in prison and/or significant financial penalties.

Limited use obligation for ASD

On 29 November 2024, the Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024 became law. The Act was part of the Cyber Security Legislative Package 2024. The Act amended the Intelligence Services Act 2001 by adding a new division, 1A of Part 6, which legislated a limited use obligation for ASD.

The limited use obligation for ASD adds additional protections to the information that organisations voluntarily provide to ASD, and to the information acquired or prepared by ASD with the consent of an organisation.

Under the limited use obligation, any information about a cyber security incident or potential cyber security incident (including vulnerability information) that is voluntarily provided to, acquired or prepared by ASD in collaboration with an organisation, cannot be used for regulatory purposes.

Living off the land techniques

In February 2024, ASD joined the US and other international partners in releasing the advisory *PRC state-sponsored actors compromise and maintain persistent access to US critical infrastructure*. The US assessed that People's Republic of China (PRC) state-sponsored cyber actors had compromised and kept access to US critical infrastructure networks to be able to conduct disruptive cyberattacks in the event of a major crisis or conflict. US agencies also assessed with high confidence that PRC state-sponsored cyber actor Volt Typhoon, was pre-positioning itself on information and communications technology (ICT) networks. This was to enable lateral movement into operational technology assets so it could disrupt functions. In the advisory, ASD assessed Australian critical infrastructure could be vulnerable to similar activity from these actors.

Also in February 2024, ASD and partners released the advisory *Identifying and Mitigating Living Off the Land Techniques*, which outlines techniques being deployed by the PRC and Russia to compromise and maintain access to critical infrastructure systems.

In March 2024, ASD and international partners released the fact sheet *PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders*, detailing Volt Typhoon's activities and providing defensive actions for critical infrastructure organisations. The fact sheet made several recommendations, including making informed and proactive resourcing decisions, securing supply chains, and driving a cyber security culture within organisations.

Cook Islands

Information and Communications Technology Division, Office of the Prime Minister

The Office of the Prime Minister (OPM) consists of 5 technical staff under the Director of ICT, with these staff reporting directly to the Chief of Staff of the OPM.

People or organisations based in the Cook Islands can report cyber incidents directly to the police, the Financial Intelligence Unit, or to the ICT Division of the OPM.

Threat landscape

The Cook Islands' most prominent cyber security threats are credential theft and phishing attacks. Although not as common, the Cook Islands experienced a man-in-the-middle (MitM) attack last year.

The OPM works collaboratively with New Zealand's National Cyber Security Centre (NCSC NZ) and Cyber CX to assess attacks and respond accordingly. In 2024, there was an increase in cyber incidents, but this was mainly because of increased monitoring.

When launching national initiatives within the civil service and also for the public, cyber security is a core component in our communications and public relations strategy. Security and awareness raising advisories of critical vulnerabilities are also disseminated to government ministries and agencies.

Achievements

The OPM's main accomplishment this year is the establishment of the Cooks Islands Cyber Security Centre which will host the functions of CERT and training.

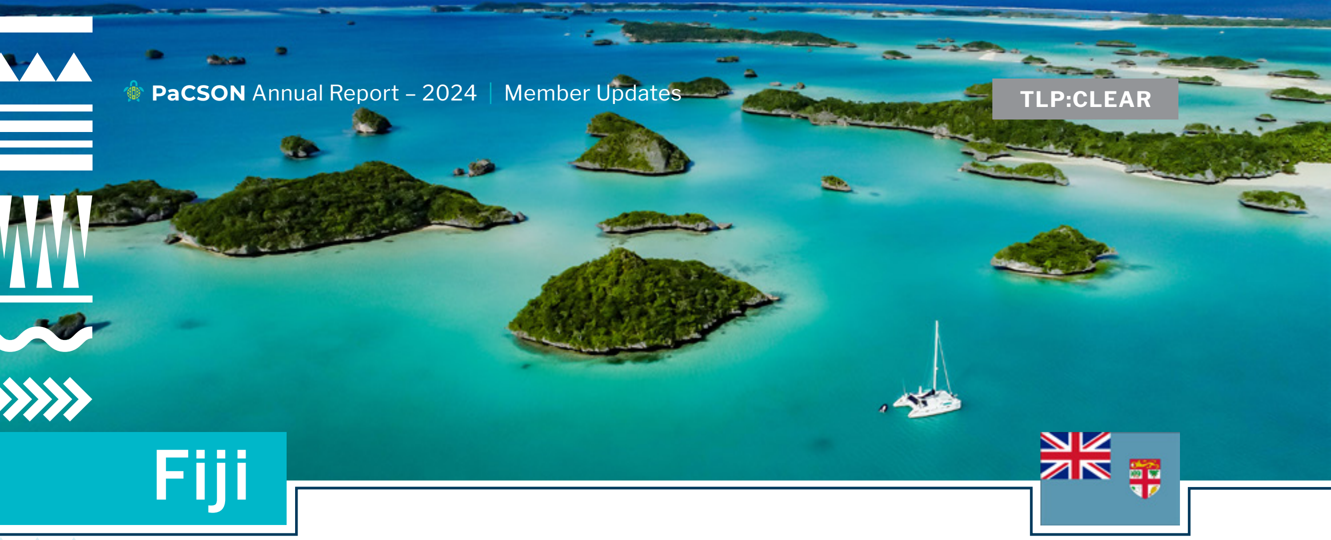
Case study: phishing campaign escalating to MitM attack

The Cook Islands Government recently fended off a significant overseas cyberattack involving a phishing campaign that intercepted multi-factor authentication (MFA) and escalated into a MitM attack. While government firewalls successfully protected central systems, some local hospitality businesses were compromised. This disclosure came during the Financial Transactions Reporting Amendment Bill 2024 being passed, which aims to enhance compliance with international transparency and cyber security standards. The bill supports the Cook Islands' alignment with Global Forum recommendations, including legal reforms, stricter information security, and operational protocols like securing office access and staff ID systems. These changes are crucial for maintaining the country's strong rating in financial information exchange and preparing for a 2025 reassessment. Justice Minister Vaine 'Mac' Mokoroa highlighted that the bill also incorporates updates to the longstanding International Trust Act 1984, reinforcing the Cook Islands' reputation as a global leader in offshore financial services.

- **https://www.rnz.co.nz/international/pacific-news/536567/cook-islands-govt-fends-off-cyberattacks-passes-bill-to-strengthen-financial-transparency**

Figure 4: Cyber security training program in Guam, February 2025, involving Japan's Ministry of Internal Affairs and Communications

Figure 5: Digital Forensic Conference in Tokyo, Japan, March 2025, involving Japan's National Police Agency



Fiji

Ministry of Trade, Co-operatives, Micro, Small and Medium Enterprises and Communications

There are 3 departments under the communications portfolio of the Ministry:

- **Department of Communications:** The department's mission is to provide efficient, competitive, cost-effective and accessible telecommunication and postal services to all Fijians. The department also works closely with the Telecommunications Authority of Fiji to ensure that proper monitoring, compliance and regulatory oversight of the telecommunications sector is maintained. The department is also responsible for the ministry's cyber security mandate, and therefore drives government efforts to protect Fiji's digital space and infrastructure.

- **Digital Government Transformation Office (DGTO):** The DGTO spearheads the digitalFIJI Programme, a digital government transformation initiative which optimises and digitalises key government services. The program is focused on a citizen-centric and business-centric approach using the Govstack platform, which is a common services, data harmonisation, e-payment and e-authentication platform. It is also focused on developing, releasing and maintaining software and mobile applications and systems (such as the digitalFIJI app; careFIJI app; vax check system; Vaccination Registry System; Registrar of Companies services; and Births, Deaths and Marriages Services) to dramatically increase public accessibility to key government services. The DGTO focuses on digitalisation-by-design, data protection-by-design and data security-by-design to enable safe, personalised and seamless service experiences.

- **Department of Information, Technology and Computing Services (ITC):** The department manages, supports and upgrades all government networks and systems on a safe and secured platform. This is to increase the productivity and efficiency of the Fijian Government through the provision of electronic services. The department is also tasked with managing all ICT-related procurement across government ministries via the ITC Steering Committee.

The Minister for Trade, Co-operatives, Micro, Small and Medium Enterprises and Communications is the Honourable Manoa Seru Kamikamica, with Shaheen Ali as the Permanent Secretary, and Tupou'tuah Baravilala as the Director-General for Digital Government Transformation, Cybersecurity and Communications. Our primary constituencies are the Government and nation of Fiji.

Depending on the nature of cyber incident or cybercrime, reports can be made to the following:

- Fiji Police Force: **https://www.police.gov.fj/**
- Fiji Independent Commission Against Corruption (FICAC): **https://ficac.org.fj/**
- Fiji Financial Intelligence Unit (FIU): **https://www.fijifiu.gov.fj/**
- Online Safety Commission (OSC): **https://onlinesafetycommission.com/**

Threat landscape

The 3 most common cyber incidents that occur in Fiji are:

- malware
- phishing
- spam.

Given the increased investments in the Government's cyber security efforts, we have seen a decrease in the number of incidents. This is based on data from the government network only.

To raise awareness in the community, there is an online cyber security awareness tool where the team runs phishing-simulation attacks and push through mandatory training for all users.

Security advisories and awareness on critical vulnerabilities are disseminated to government ministries and agencies.

Achievements

In 2024, the ministry reached several key milestones:

- International cyber security commitments: Fiji formally acceded to the Budapest Convention, therefore strengthening its global collaboration on cybercrime.
- Fiji has also been making notable contributions at the United Nations Open-Ended Working Group (UN OEWG) on the security of, and in the use of, ICT. Fiji also participated in the negotiations for the UN Convention Against Cybercrime.
- Business process simplification: The businessNOW platform's first sub-system—Starting a Business—was launched, integrating 8 e-services from different agencies into a single platform.
- Cyber security advancements: Fiji's second Cybersecurity Maturity Model Assessment was undertaken to guide the development of the upcoming National Cybersecurity Strategy. Fiji's National CERT Action Plan was developed to support the first year of Fiji CERT.
- Digital Transformation Roadmap: The National Digital Strategy 2025–2030, drafted in 2024, was launched in April 2025.
- Expanded connectivity: Starlink officially launched its services in Fiji, after the Government and the Regulatory Authority issued licenses in 2023, significantly enhancing internet access in previously underserved regions.
- National Taskforce to Address Pornography: This taskforce, which convened in 2024, is working towards addressing online child sexual exploitation and abuse materials as its first work stream. It is co-chaired by the Deputy Prime Minister and the Minister for Communications as well as the Minister for Women, Children and Social Protection. It has 3 working groups – Working Group 1: Policy, Legislation, Governance, and Criminal Justice; Working Group 2: Survivor Support, Empowerment, Society, and Culture; and Working Group 3: Industry and Technology Response. The taskforce comprises representatives from Members of Parliament, government ministries and agencies, law enforcement and prosecution, civil society, non-government organisations (NGOs), the telecommunications and technology sector, and academia.

- National Anti-Scam Taskforce: Convened in 2024, this taskforce is an interagency initiative formed to combat the rise of online fraud and scams, focusing on raising awareness, strengthening institutional frameworks, and pursuing legal reforms to create a safer online environment for Fijians. The taskforce is represented by members from the Ministry of Trade, Co-operatives, Micro, Small and Medium Enterprises and Communications; the Ministry of Local Government; the RBF; the Office of the Solicitor-General; the Fiji Police Force; the Consumer Council of Fiji; the Fijian Competition Consumer Commission; the Online Safety Commission; and its co-opted members Vodafone and Digicel Fiji.

In 2024, Fiji took a significant step in strengthening its cyber security framework by acceding to the Budapest Convention. As part of this process, the country's 24/7 Points of Contact were activated in November, marking a key milestone in international cyber cooperation. Fiji is now working towards signing the Second Additional Protocol of the Convention, further enhancing its commitment to combating cybercrime.

Fiji and Australia signed a Memorandum of Understanding (MoU) on Cyber Security Cooperation in April 2024. The MoU strengthens the bilateral partnership on cyber security and incident response, governance, cyber safety and critical infrastructure cyber security. Fiji is receiving support from Australia to establish and operationalise Fiji CERT through technical assistance and advice, and collaborating to develop Fiji's National CERT Action Plan.

As part of its global commitments, Fiji also communicated its UN Diplomatic and Technical Point of Contact to the UN OEWG on security of, and in the use of, ICT. Fiji actively participated at the UN OEWG in 2024 to support the development of norms and rules of responsible state behaviour in cyberspace.

A two-day National Conference on Cybercrime and E-evidence for Prosecutors was organised in Fiji by the Office of the Director of Public Prosecutions (ODPP) with the support of the GLACY-e joint project of the European Union, the Council of Europe and also support from the United Nations Office on Drugs and Crime (UNODC). The conference aimed to increase mutual understanding of the needs and challenges faced by criminal justice authorities, particularly when dealing with cybercrime and electronic evidence.

Figure 6: Three-day Validation Workshop for the National Digital Strategy

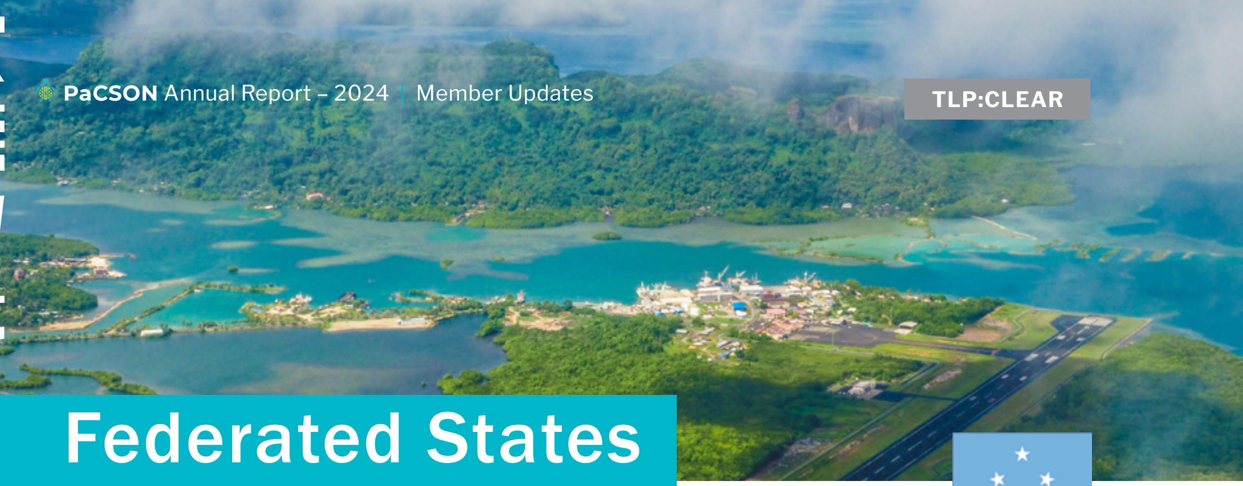
Figure 7: Deputy Prime Minister and the Minister for Trade, Co-operatives, Micro, Small and Medium Enterprises and Communications the Honourable Manoa Kamikamica (centre right); Director-General Digital Government Transformation, Cybersecurity and Communications Tupou'tuah Baravilala (centre left); and Digital Government Transformation Office Team at the businessNOW eServices Launch

Figure 8: Director-General Digital Government Transformation, Cybersecurity and Communications Tupou'tuah Baravilala, Deputy British High Commissioner Nicola Noble, Acting Director of the Office of the Director of Public Prosecutions John Rabuku, Cybersecurity Maturity Model Expert Associate Professor James Boorman, with stakeholders at the Welcome Ceremony for Fiji's Cyber Security Capacity Maturity Model for Nations Review

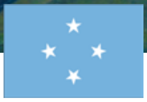
Ministry of Trade, Co-operatives, Small and Medium Enterprises and Comm
UK Government
Welcome Ce
Fiji Cybersecurity Review
Model for Nations (CMM)
OCSC
Oceania Cyber Security Centre

Figure 9: Director-General Digital Government Transformation, Cybersecurity and Communications Tupou'tuah Baravilala delivering her remarks at the Welcome Ceremony for Fiji's Cyber Security Capacity Maturity Model for Nations Review

Figure 10: First official meeting of the National Taskforce to Address Pornography



Federated States of Micronesia



The Cyber Security and Intelligence Bureau

The Cyber Security and Intelligence Bureau (CSIB) is a division within the Department of Justice in the Federated States of Micronesia (FSM), and currently has 6 staff members.

People and organisations report cyber incidents and cybercrime to their local law enforcement agency. The agency then reports to CSIB.

Threat landscape

The 3 most common cyber incidents that occur in FSM are phishing, ransomware and cyber espionage. With regards to phishing, email advisories have been able to deter further exploitation. Ransomware attacks have been mitigated through full backups using the Veeam Backup and Replication ICT solution with weekly full backups and daily incremental backups. Cyber espionage has been addressed using end-to-end encryption communication application software.

Awareness raising

CSIB held the country's first cyber security symposium and, during the reporting period, CSIB travelled to all the FSM states to conduct cyber safety and hygiene awareness exercises at the elementary and high schools.

During the reporting period, CSIB released an intelligence report every quarter.

This year saw many achievements by CSIB including, the first FSM cyber security symposium, the launch of the National Cybersecurity Strategy, and the creation of FSMCERT.

Figure 11: a school group using the Cyber Up campaign materials

Figure 12: Sharing Cyber Up campaign materials with the community

Kiribati

Ministry of Information, Communications and Transport

The Digital Transformation Office (DTO) within the Ministry of Information, Communications and Transport (MICT) is made up of 6 units, one of which is the National Cybersecurity and CERT which has 3 permanent staff: the Chief Information Security Officer, the Senior Information Security Analyst, and an Information Security Analyst.

The National Cybersecurity and CERT is run by the Government's National ICT Director, who also oversees the DTO. The DTO was established under a restructuring of all Government ICT personnel who are now under the DTO. The Government Chief Information Security Officer leads the National CERT and reports to the National ICT Director. The National ICT Director reports to the Secretary of the MICT and the Honourable Minister of the MICT.

Our primary constituencies are the government ICT sector, critical national infrastructure providers, local businesses, civil societies, academia and the public.

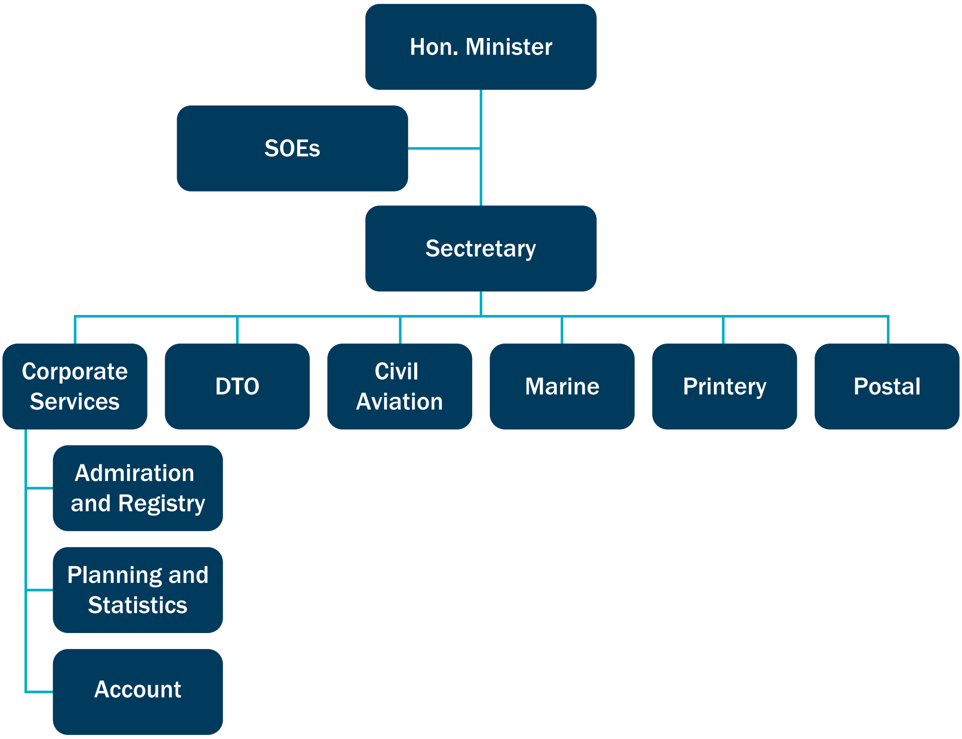


Figure 13: Organisational structure

Projects

Kiribati Connectivity Project

This project will finance the construction of a fibre-to-the-premises network, targeting coverage of 80% of homes, businesses and all government entities and schools. In addition, the project will support the establishment of a Starlink community gateway to provide interim high-speed internet connectivity prior to the landing of the East Micronesia Cable (EMC) system in the capital. The Project Development Objective is to reduce the cost and improve the availability of internet services in Kiribati. The project is funded and led by the World Bank.

Cybersecurity Bill 2025

The Cybersecurity Bill is a proposed legislation to promote the development and awareness of cyber security, designate institutions, and provide processes to anticipate, prevent, manage and respond to cyber security incidents. It also aims to ensure that operators of critical infrastructure adopt cyber security measures and practices and collaborate on matters of cyber security. The bill is planned for its first reading in November 2025.

Kiribati Digital Government Project

This project aims to support the implementation of Kiribati's Digital Government Master Plan 2021, focusing on governance, technical infrastructure and e-government applications. Funded by a USD 12 million grant through a partnership between the Government of Kiribati, MICT and the World Bank, the project seeks to strengthen digital services and systems across government.

East Micronesia Cable

This project's objective is to facilitate social and economic benefits for the people of FSM, Kiribati and Nauru by providing faster, higher quality and more reliable internet connectivity via a submarine cable, replacing the current, less reliable satellite services.

Threat landscape

Currently, cyber incidents in Kiribati are reported on an ad hoc basis. Individuals or organisations usually report incidents directly to CERT-KI via email, phone calls or in person at the DTO or the cybercrime unit at the Kiribati Police Service. There is no standard operating procedure yet, but efforts are underway to establish a standardised reporting and response process. The most common cyber incidents occurring in Kiribati are ransomware, phishing, scams, fraud attempts, cyberbullying and online harassment.

CERT-KI responds by assisting digital forensic investigations in their analysis, identifying root causes and recommending preventive measures. Incidents include:

- phishing and scams
- malware and ransomware attacks
- cyberattacks.

During the reporting period, there was an increase in the number of incidents compared to 2023. Most were phishing attempts, scam cases and fraud attempts targeting the fisheries sector.

Awareness raising

CERT-KI actively raises awareness of cyber threats and the importance of cyber security among citizens and organisations through the following activities:

- conducting awareness visits to schools, communities and outer islands
- sharing cyber safety tips regularly on social media platforms
- distributing educational materials and merchandise during public events, such as school athletics
- running cyber drills for the national ICT Taskforce
- organising cyber security boot camps for students and youth to build their knowledge and practical skills
- participating in regional and global cyber drills
- collaborating with partners like PaCSON to promote best practices and strengthen community awareness.

Achievements

MICT achievements in 2024 included:

- advanced from Tier 5 to Tier 3 in the Global Cybersecurity Index 2024 5th Edition
- established a CERT under Kiribati's Digital Government Act 2023 legalised and empowered it with its roles and responsibilities
- accession to the European Union's Budapest Convention on Cybercrime.

Figure 14: Sharing Cyber Up materials with the community

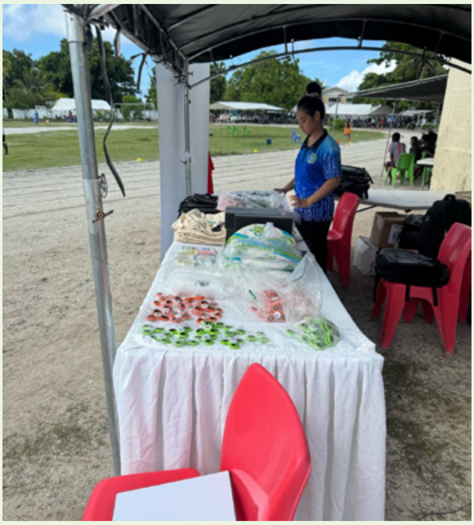


Figure 15: Sharing Cyber Up materials with the community

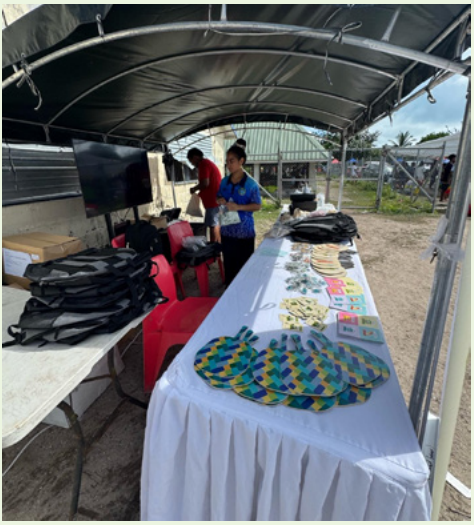


Figure 16: Sharing Cyber Up materials with the community

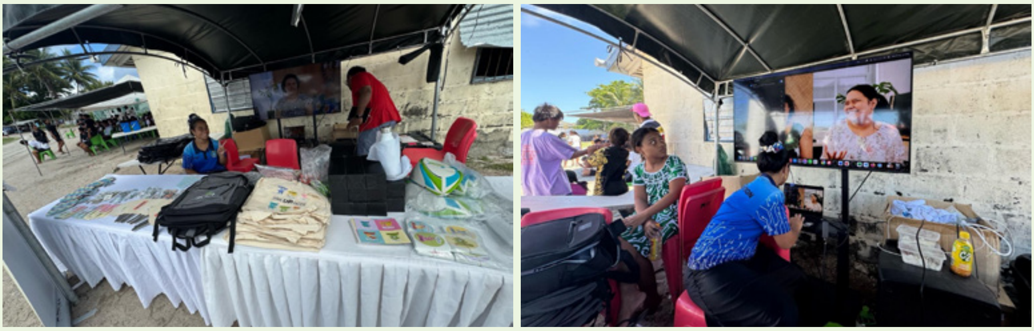


Figure 17: Sharing Cyber Up materials with the community

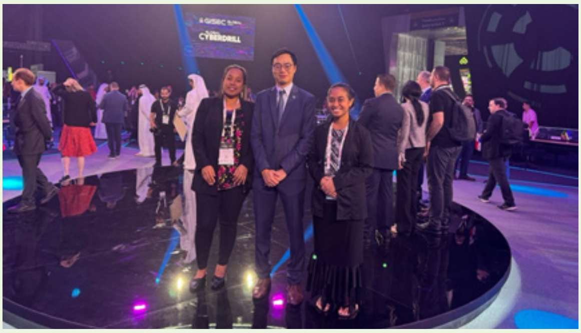


Figure 18: MICT representatives at the GISEC Global Cyberdrill

Figure 19: MICT representative at the GISEC Global Cyberdrill

Figure 20: MICT representative at the GISEC Global Cyberdrill

Figure 21: Cyber awareness raising in the community

Figure 22: Cyber awareness raising in the community

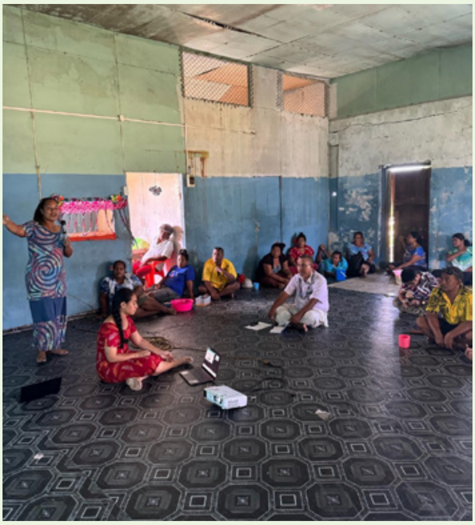


Figure 23: Cyber awareness raising in the community

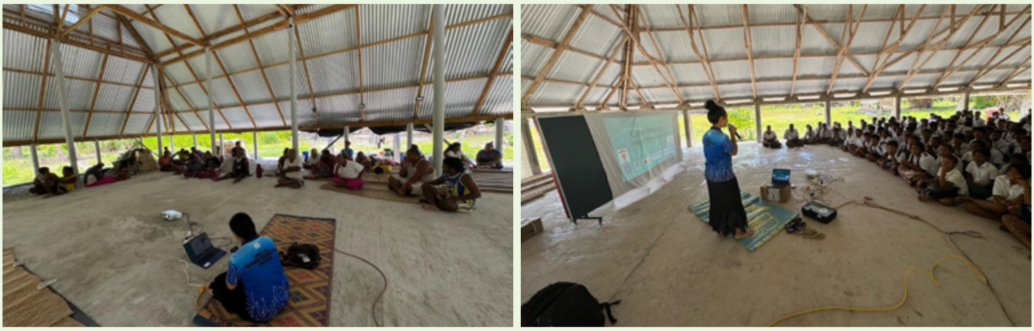


Figure 24: Cyber awareness raising in the community

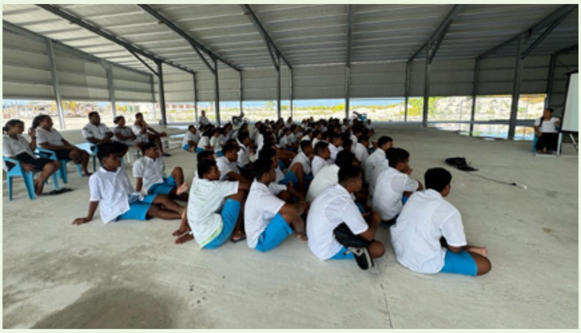


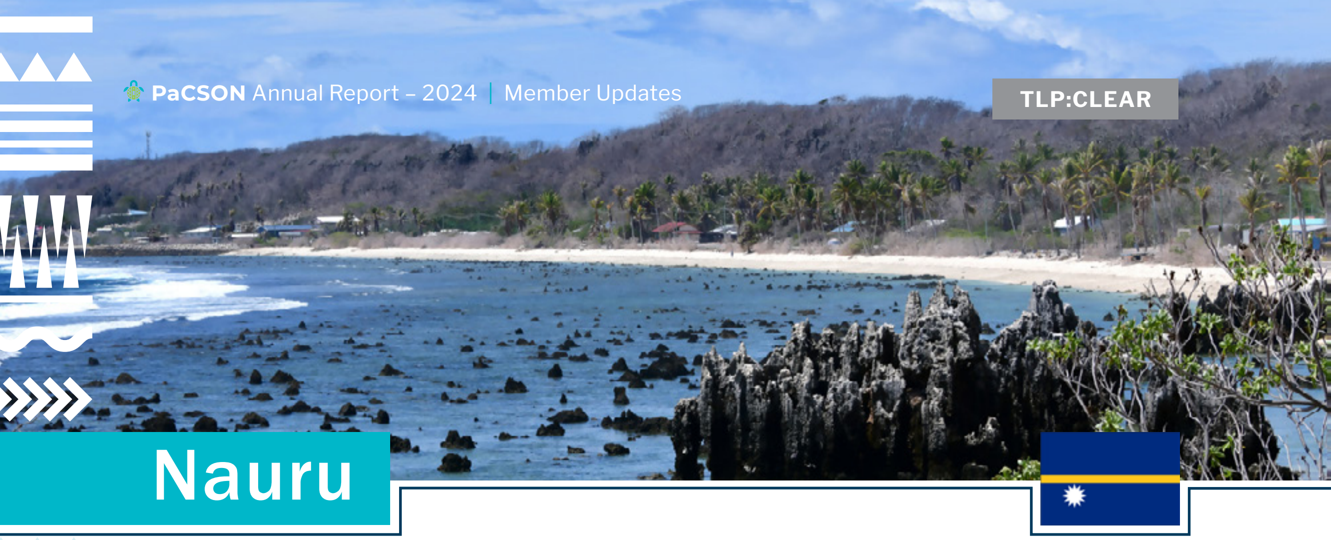
Figure 25: Cyber awareness raising in the community

Marshall Islands

Marshall Islands Police Department

The Marshall Islands Police Department (MIPD) is part of the Ministry of Justice. Headed by the Police Commissioner, the force is responsible for serving a population of 70,000 people populating 34 coral atolls and more than 1,000 islands, and is made up of approximately 200 sworn police officers.

The MIPD supports government, business and small enterprises, private industry and the Marshall Islands public as its primary constituency.



Nauru

Department of Information, Communication and Technology, Ministry of Telecommunications

The Government of Nauru has a large investment in computing resources and has encouraged the government departments to use these resources effectively to share information and knowledge in support of the government's mission. The computer facilities are a shared system made available to promote atmosphere for the government, create a sense of commitment to the local and global community, and assist in preparation for living in a complex technological society. The network infrastructure, access to the internet and online resources, powerful servers and an increasing number of personal computers are assets in which we may take pride. Their value increases the more we take advantage of them.

The Cyber Security Awareness Team (CSAT) was established in 2019 and provides cyber safety awareness to all Nauruan government departments.

Most of the people of Nauru report directly to the Nauru Police Force through either walk-ins, phone calls or Facebook chat. Public service workers report to the Department of ICT through either phone calls or emails.

The top security incidents in Nauru include phishing, identity theft (copying Facebook accounts in order to impersonate), and hacked accounts (Facebook, IMO, etc.).

Awareness raising

Awareness raising is conducted via the radio; translating content from PaCSON into local language; travelling around and training and spreading awareness in person; and using PaCSON Cyber Up materials. Awareness raising is also done through the Department of ICT Facebook page.

The PaCSON Cyber Up Campaign was held in 4 schools in Nauru over a one-week period in July where ICT staff presented to school staff and students on the importance of being cyber safe and on the Cyber Up tips and suggestions on increasing cyber security.

A major accomplishment this year was the launch of the Nauru National Digital Transformation Strategy.

New Zealand

National Cyber Security Centre, New Zealand

The National Cyber Security Centre (NCSC), a part of the Government Communications Security Bureau (GCSB), is Aotearoa New Zealand's lead operational cyber security agency.

In 2024, New Zealand's CERT was transferred from the Ministry of Business, Innovation and Employment (MBIE) to the NCSC NZ. The integration process, when completed, will result in an agency that provides cyber security services to all New Zealanders – from individuals and small to medium enterprises, through to nationally significant organisations.

Since the integration, anyone in New Zealand can report a cyber security incident to the NCSC NZ. We also receive incident notifications from our international incident response counterparts when they identify affected New Zealand organisations in their investigations.

NCSC NZ also has a dedicated Pacific Partnership Team that works closely with Pacific incident response counterparts and the wider regional cyber community. The Pacific Partnerships program focuses on 4 core pillars of support as well as responsive activities.

The 4 core pillars are:

- institution building (supporting the development of CERT or CERT-like functions)
- workforce development
- capacity-building activities
- engagement in regional and international forums.

Responsive activities since January 2024 has included:

- Chair of the PaCSON Capacity Building Working Group (CBWG)
- Participating in the PaCSON Awareness Raising Working Group (ARWG) – collaborating on developing and delivering the Cyber Smart Pacific (Cyber Up) annual regional awareness raising campaign
- in-country bilateral meetings and training with the Solomon Islands, Fiji and Tuvalu
- partnering with SamCERT for cyber security support for the Commonwealth Heads of Government Meeting (CHOGM)
- sharing CERT NZ reporting templates
- continuing collaboration with CERT Tonga on a Cyber Security Workforce Development Program.

Incidents can be reported to NCSC NZ through an online reporting tool, by phone or through our referral partners.

Reporting incidents of potential national significance:

- **Report an incident and request support | National Cyber Security Centre**

Reporting all other incidents:

- individuals and businesses: **https://www.cert.govt.nz/individuals/report-an-issue/**
- IT specialists: **https://www.cert.govt.nz/it-specialists/report-an-incident/**

Full contact details: **https://www.cert.govt.nz/about/contact-us/**

CERT NZ also has a Coordinated Vulnerability Disclosure Policy and process:

- **https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/**

Threat landscape

In 2024, the top 3 cyber security threats recorded by NCSC NZ were:

- phishing and credential harvesting
- scams and fraud
- unauthorised access.

NCSC NZ responds to cyber security threats and issues in New Zealand. NCSC NZ's core business is supporting nationally significant organisations, government agencies, businesses, IT specialists and members of the public with any form of cyber security incident. This may include:

- ransomware incidents
- phishing and credential harvesting
- malware
- scams and fraud
- unauthorised access
- website compromise.

NCSC NZ reviews and assesses any threats reported, and uses the information provided to develop mitigation advice that we can share with those reporting an incident and with the rest of the community.

When NCSC NZ receives a report, we also assess whether it is best investigated by a partner agency and can refer the incident to them. Information provided to NCSC NZ is confidential and consent is sought before sharing any details of a report.

The NCSC recorded 7,122 cyber security incidents in the year to 30 June 2024 – its first year as New Zealand's lead operational cyber security agency.

As this was the first reporting year since CERT NZ was transferred to the NCSC, an overview of cyber threats in New Zealand was able to be presented in a single report.

NCSC NZ's Deputy Director-General Cyber Security Lisa Fong noted,

> While the report draws from separate data sets, we can begin to see the extent of malicious cyber activity. Of the 7,122 incidents, 6,779 were handled through the NCSC's general triage process, often affecting individuals or small to medium businesses, resulting in $21.6 million NZD of reported losses.
>
> The other 343 incidents were triaged for more specialist technical support because of their potential national significance. These are incidents that affect the systems and data of organisations in key sectors or where NCSC's understanding of the malicious actor responsible for the incident means there is additional risk.

Of these 343 incidents (up from 316 in 2022–23), 110 could be linked to state-sponsored actors and 65 were likely caused by criminal or financially motivated actors – which was consistent with the past few years.

Awareness raising

In October 2024, NCSC NZ delivered its first annual Cyber Smart Week as a combined agency. The Public Awareness Campaign – imagined as a 'Scamathon' played on the idea of a Telethon – raised awareness about the importance of being vigilant of scammers.

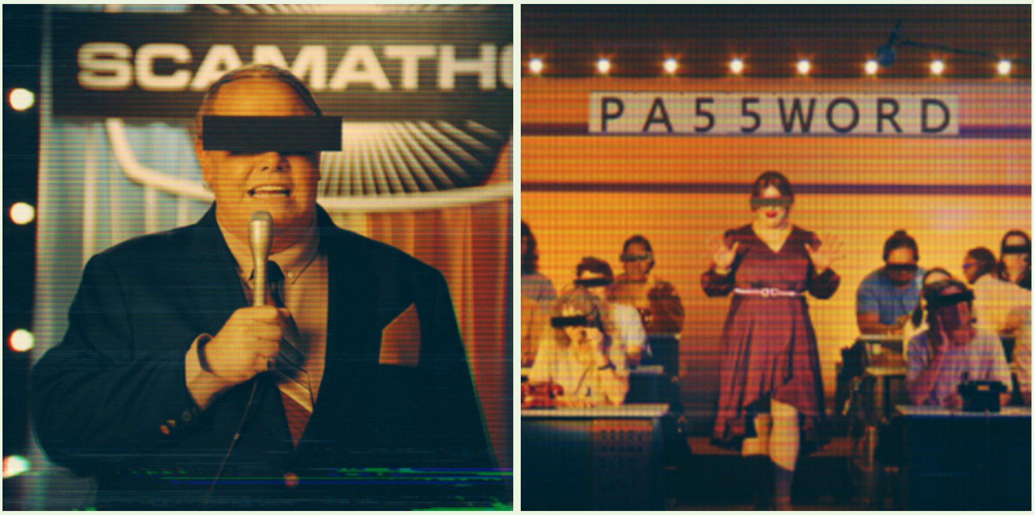
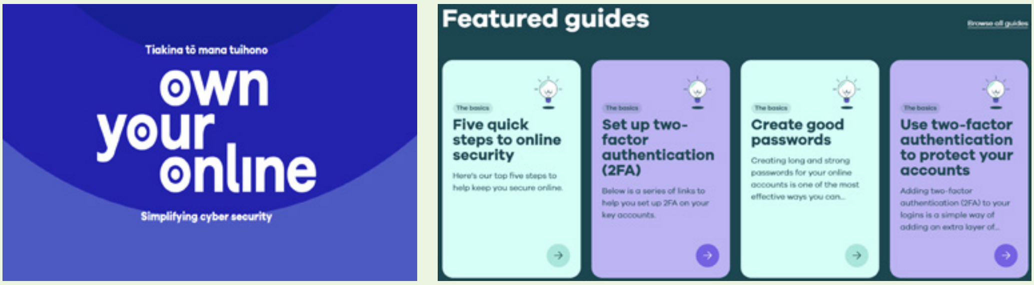


Figure 26: An awareness raising campaign

In 2024, NCSC NZ also launched the consumer-facing website 'Own Your Online' to share key cyber security advice to New Zealanders.



Featured guides

Browse all guides

The basics
Five quick steps to online security
Here's our top five steps to help keep you secure online.

The basics
Set up two-factor authentication (2FA)
Below is a series of links to help you set up 2FA on your key accounts.

The basics
Create good passwords
Creating long and strong passwords for your online accounts is one of the most effective ways you can...

The basics
Use two-factor authentication to protect your accounts
Adding two-factor authentication (2FA) to your logins is a simple way of adding an extra layer of...

Figure 27: Online materials from 'Own your Online'

NCSC NZ also supported the development and refresh of the collaborative Cyber Up Pacific initiative, through the ARWG.

This year, the ARWG developed 'Cyber Starter Packs' containing hardcopy resource packs for schools, community groups and businesses.

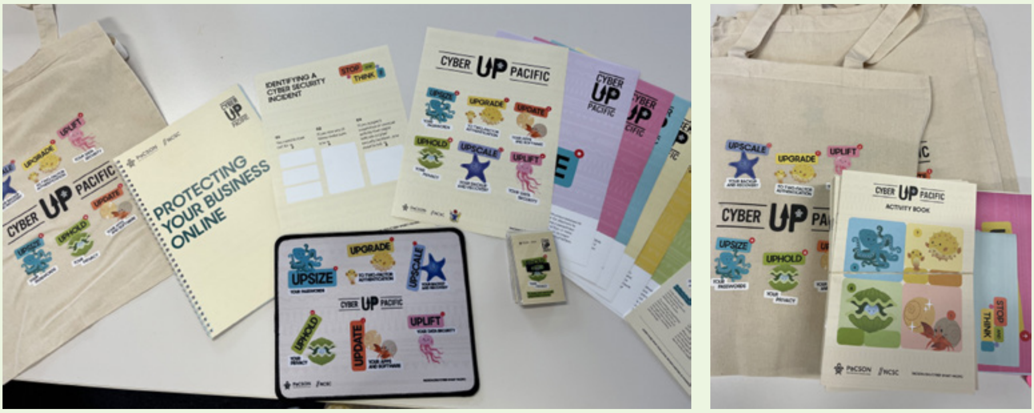


Figure 28: Materials from the 2024 Cyber Up campaign

NCSC NZ hosts resources including cyber resilience guidance, technical documents and guidelines on the website.

NCSC NZ publishes advisory bulletins on social media channels and distributes these to organisations and individuals on their mailing list.

NCSC NZ website: **ncsc.govt.nz**

Significant achievements in 2024 included:

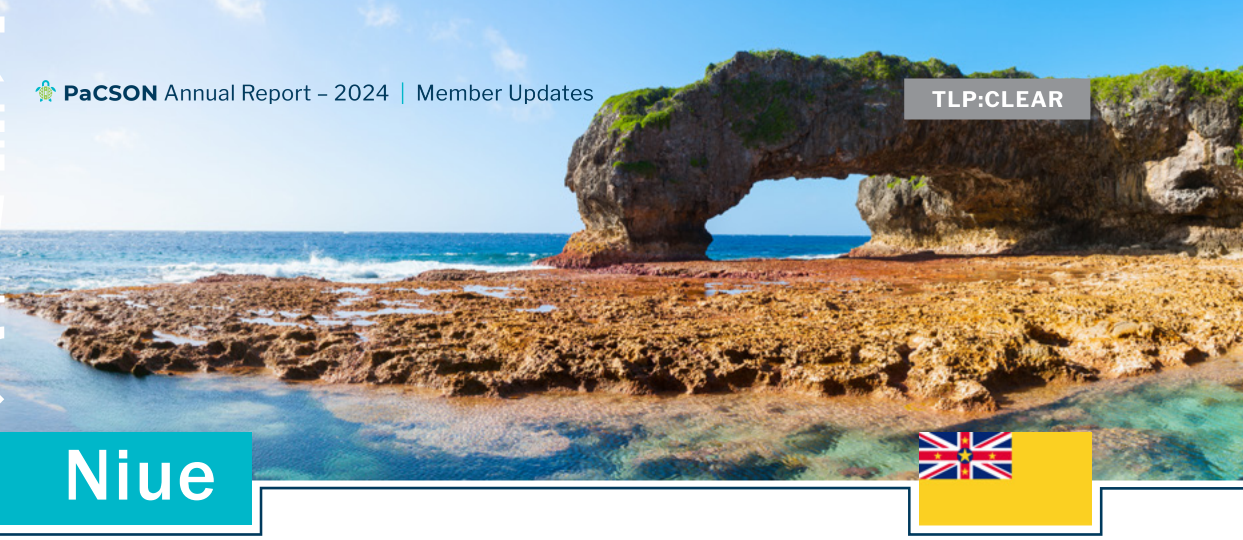
- integrating CERT NZ into the NCSC NZ to form one leading cyber agency
- responding to 7,122 incidents
- disrupting 10.3 million malicious cyber events via malware-free networks
- delivering a new awareness raising platform – Own Your Online
- delivering the awareness campaign 'Cyber Smart Week'
- supporting Samoa MCIT and SamCERT in delivering cyber security support to CHOGM.

Case studies: compromised parliamentary networks

In August 2021, the NCSC NZ provided support to the compromise of computer networks associated with New Zealand's' Parliamentary Counsel Office and the Parliamentary Service by malicious cyber actors attributed to the PRC, known as APT40. During the last 3 years, the PRC has demonstrated ongoing targeting of democratic institutions globally, and the targeting of critical infrastructure networks in the US.

Following the March 2024 public announcement of the APT540 activity against Parliament, in July 2024 the NCSC NZ joined partners to highlight evolving tactics, techniques and procedures of APT40. The actors had been observed using compromised small-office/home (SOHO) devices as operational infrastructure, and exploiting newly public vulnerabilities in applications and devices such as Microsoft Exchange, Atlassian Confluence and Apache Log4j. Many of these SOHO devices, including in New Zealand, are unpatched or end-of-life devices left vulnerable to exploitation. Once compromised, SOHO devices can be used for attacks while blending in with legitimate traffic, subsequently presenting challenges for network defenders. APT40 continues to make use of compromised infrastructure and use available exploits within hours or days of public release.

This joint advisory served to raise awareness of and resilience to the tactics associated with a significant cyber threat to New Zealand and like-minded nations.



Niue

Telecom Niue Limited

Telecom Niue Limited is a company incorporated in Niue and owned by the Government of Niue. Telecom Niue employs a moderate workforce, including administrative officials, technicians and contractors.

Telecom Niue supports government, business and small enterprises, private industry and members of the public as its primary constituency.

- People can report cyber incidents via **https://telecomniue.com/support/contact-us**
- Email: **support@telecomniue.com**
- Local toll-free number: 015

Threat landscape

The 3 most common cyber incidents are phishing attacks, insider threats and social engineering.

Telecom Niue has processes in place to identify and respond to phishing emails, including user reporting channels, email filtering systems, and incident response playbooks for containment and analysis. There are incident response protocols to investigate, report and contain data breaches, along with encryption and access controls to minimise data exposure. Role-based access controls, activity logging and user-behaviour analytics help us identify and manage risks from within the victim organisation.

Telecom Niue has collaborated with CEIT, Niue Police, and the Office of the Secretary of Government (SOG) to support cyber security awareness initiatives. While progress has been gradual, we recognise the importance of educating staff and stakeholders about cyber threats. Efforts are ongoing, and we are committed to strengthening our awareness programs and building a more cyber-resilient culture over time.

Telecom Niue does not issue any official news, publications or advisory bulletins. Instead, we provide relevant cyber security advice and updates directly to SOG, who is responsible for disseminating such information as needed.

In the reporting period, notable achievements included the completion of the government network upgrade and standardisation of hardware and software throughout the whole of government.

Palau

Bureau of Public Safety

As its primary constituency, the Bureau of Public Safety provides support to government, law enforcement, business and small enterprises, private industry and members of the public.

The bureau receives cyber-related reporting through formal reporting frameworks. Additionally, the bureau uses social media to engage with the public.

Papua New Guinea

Department of Information and Communications Technology

The Department of Information and Communications Technology (DICT) is a government agency established through Ministerial Determination Gazettal No. 145/2007. It is responsible for providing timely policy advice to the Minister for ICT on communications and information matters, coordinating digital government programs and initiatives, raising awareness and disseminating government development information.

The mission of DICT is to harness the potential of ICT to make PNG become a smart, networked and knowledgeable society. This will bring the Government closer to the people through effective governance, improved service delivery and socioeconomic growth.

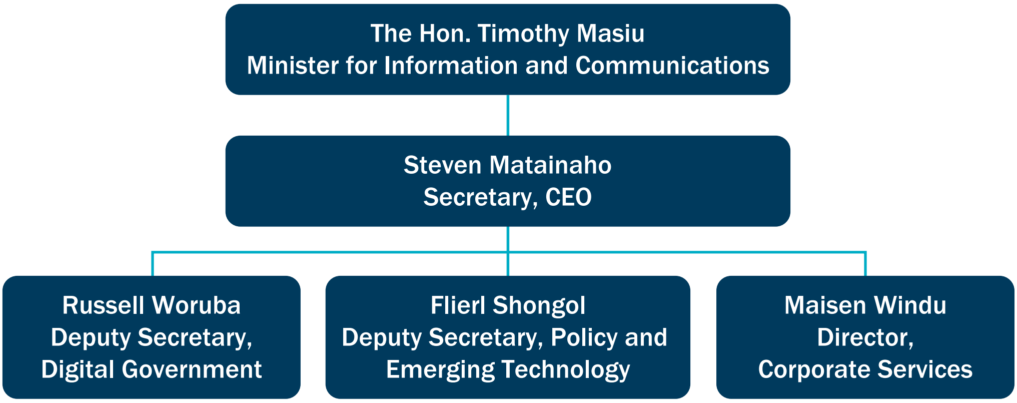
DICT achieves its mission by providing all agencies with the tools, methods, practices and policy guidance they need to deliver effective and accessible digital services to all PNG residents. This ensures the use of appropriate and affordable digital technologies through a transformative and inclusive approach across sectors of the economy for the benefit of all.

At DICT we are committed to improving people's experience of government services by putting people first, improving skills both within government and outside government. We focus on:

- customer-focused services
- innovation and change
- standards
- teamwork and collaboration
- transparency
- listening
- professionalism
- employees
- honesty.

We are committed to working as one team at all government levels of our operations to ensure the effective and efficient delivery of digital services to the government, business and the citizens of the country.

The current DICT organisational structure includes:



The Hon. Timothy Masiu
Minister for Information and Communications

Steven Matainaho
Secretary, CEO

Russell Woruba
Deputy Secretary,
Digital Government

Flierl Shongol
Deputy Secretary, Policy and
Emerging Technology

Maisen Windu
Director,
Corporate Services

Figure 29: DICT organisational structure

Staff in organisations that experience a cyber incident can report it directly to DICT via the website: **www.ict.gov.pg** or directly to the PNG National Cybersecurity Centre (PNG NCSC).

Threat landscape

Some of the common cyber security threats are:

- malware
- ransomware attacks
- phishing attacks
- distributed denial-of-services (DDoS) attacks
- identity theft and fraud.

DICT are equipped to deal with the following cyber incidents:

- malware incidents: PNG NCSC uses its own security information and event management system to monitor endpoints and firewalls, enabling them to respond to detected threats at any time.
- phishing and social engineering attacks: DICT uses all its social media platforms to provide guidance on containment and prevention, as well as conduct public awareness campaigns.

Awareness raising

DICT provides awareness raising via its social media pages, mainly Facebook and LinkedIn. DICT also supports the PNG Government, and spreads awareness through official communication channels. DICT provides printed materials and graphics online to the community, and also raises awareness through local talk-back radio shows.

DICT regularly supports awareness raising initiatives, promoting cyber security awareness materials for communities and government users. This is done through the website **www.ict.gov.pg**.

Achievements

In 2024, DICT and PNG NCSC achieved significant cyber security progress. PNG dramatically improved its global cyber security ranking, implemented its National Cybersecurity Strategy 2024, and actively enforced its Cybersecurity Operations Centre. DICT launched the National Data Governance & Data Protection Policy and the DICT Corporate Plan. Public awareness campaigns were conducted, and collaborations with international partners were strengthened to build cyber forensics capabilities and expand CERTs.

Case study: ransomware against the Internal Revenue Commission

In late January 2025, PNG's Internal Revenue Commission (IRC) suffered a major ransomware attack. This caused a system outage affecting their tax system (SIGTAS), internet, phones and email for weeks. While the IRC claimed taxpayer data was secure, the incident underscored the growing cyber threats in PNG and the Government's commitment to improving cyber security resilience.

National Information & Communications Technology Authority

PNGCert operates within the National Information & Communications Technology Authority (NICTA) under the Ministry of ICT, which serves the whole of PNG.

Members of the public, businesses and organisations can report cyber security incidents directly to PNGCert by reaching out to us via our email address, or through our website.

- Email: **report@pngcert.org.pg**
- Website: **https://www.pngcert.org.pg**

PNGCert provides advisories on how be safe online; it is up to each entity to implement safeguards, based on their budget.

Threat landscape

In 2024, NICTA faced these common cyber threats:

- Ransomware

  During the past year, we saw dramatic ransomware attacks impacting PNG companies. Usually, ransomware attacks happen for 2 reasons:

  - bad configuration of systems at the perimeter of company networks
  - phishing emails being opened by company users.

  Ransomware is definitely one of the biggest threats in PNG. At least 90% of the hacking attacks seen in PNG are ransomware or phishing-related.

- Social media, such as Facebook and Tiktok, issues with fake accounts and cyber bullying.

  This is also a huge issue in PNG. In particular, stealing Facebook accounts is rampant for various reasons (e.g. a weak password that can easily be guessed).

  Cyberbullying happens a lot too. Sadly, victims rarely report this to the police because they feel ashamed or because they simply don't know that cyber bullying is now a crime according to the Cyber Security Act.

- Website defacing

  This issue particularly affects public agencies and authorities. Website attacks are very common in PNG.

Awareness raising

NICTA raises cyber awareness of the people of PNG through strategies like:

- the Safer Internet Day, which is an awareness raising initiative conducted by NICTA to encourage cyber safety
- advice to internet users in our country to practise safer behaviours when using the internet
- publishing updates on the NICTA website and NICTA Facebook account
- using the awareness raising materials provided by PaCSON as part of our community engagement activities.

Samoa

Samoa Computer Emergency Response Team

Samoa Computer Emergency Response Team (SamCERT) is a division of the Ministry of Communications and Information Technology, Government of Samoa. SamCERT is an initiative aimed at cyber security, and its focus is monitoring and delivering a safe cyberspace to users. SamCERT's key activities are cyber security, cyber safety and cyber inclusion. It is for all citizens of Samoa, tourists, businesses and Government so they may enjoy the full benefits of a secure and resilient cyberspace.

The SamCERT team consist of 5 staff: the Deputy Chief Executive Officer, the Principal Cyber Awareness Officer, the Principal Cyber Emergency Handling Officer, the Senior Officer and the IT Officer.

Individuals and organisations in Samoa can report cyber incidents via an online form at **samcert.gov.ws**.

Solomon Islands

Solomon Islands Government Information & Communication Technology Services

Solomon Islands Government Information Communication Technology Services (SIG ICT Services) falls under the Ministry of Finance Corporates Services. SIG ICT Services is mandated to provide ICT service delivery to the Solomon Islands Government. This includes all ministries, provincial governments and related agencies. SIG ICT Services has 32 staff – including technical, management and administration positions.

SIG ICT Services provides technical operational and development support through the following teams: Information Systems, Client Support Services, Infrastructure, Digital Transformation and Strategic Projects, Cyber Security, and Admin/Finance and Management.

Threat landscape

In the Solomon Islands, people and organisations can report cyber incidents to the Solomon Islands Computer Emergency Response Team (SICERT) or SIG ICT Services. Reports can be made by:

- emailing SIG ICT Services
- calling the SIG ICT Services helpdesk
- raising tickets to the SIG ICT Services helpdesk
- visiting the SIG ICT Services office during working hours.

The 3 common cyber security threats in the Solomons include:

- phishing attacks
- malware
- brute-force attacks.

SIG ICT Services is equipped to respond to a variety of cyber security incidents affecting government ministries and agencies. These include:

- **Phishing and social engineering attacks:** This involves investigating and mitigating email-based attacks where users are tricked into revealing sensitive information or clicking malicious links.
- **Malware infections:** SIG ICT Services detects and responds to infections by viruses or malicious software on government systems and networks.
- **Unauthorised access and account compromise:** SIG ICT Services identifies and seeks to contain incidents where user accounts or systems are accessed without permission, often due to weak passwords or credential theft.
- **Insider threats:** SIG ICT Services investigates security breaches by employees or contractors with legitimate access who misuse their privileges.
- **Endpoint security alerts:** SIG industrial control systems handles alerts from security tools such as antivirus, firewalls, or endpoint detection platforms (e.g. CrowdStrike) to take immediate remediation actions.

Awareness raising

SIG ICT Services is dedicated to enhancing cyber security awareness through ongoing campaigns for staff and communities. We have established awareness training in collaboration with the Institution of Public Administration and Management (IPAM) for government officers. These ongoing campaigns aim to ensure employees are well-informed and vigilant, fostering a strong culture of cyber safety.

SIG ICT Services primarily promotes cyber security awareness through a dedicated Cyber Safe Campaign, which includes regular email communications to all staff. These emails serve as our main channel for sharing timely insights, advice and updates on cyber security best practices, emerging threats and protective measures. While we do not produce a broad range of formal publications or advisory bulletins, these carefully crafted messages help ensure that all employees remain informed and proactive in protecting against cyber threats.

Achievements

Major accomplishments include:

- an enhanced Security Events Incidents Management System
- strengthened endpoint security with deployment of CrowdStrike EDR
- a revised and updated Incidents Response Plan and Incidents Communication Plan.

Case study: launching the SICERT Project

This year, a major cyber development in the Solomon Islands was the official launch of the SICERT project. The project was introduced by the Ministry of Communication and Aviation in collaboration with the governments of Australia, the UK and New Zealand. It marks a significant step under our National Cybersecurity Policy, particularly in achieving the goal of strengthening our national cyber security structures.

SICERT will serve as our country's first line of defence against cyber threats, helping government agencies, businesses and the public to prevent, detect, respond to and recover from cyber incidents. It will also raise awareness, coordinate incident response, support digital forensic investigations, and connect us to regional and global CERTs.

With the growing risks in our digital environment, the launch of SICERT is a key move to ensuring the security and resilience of our national digital systems and infrastructure.

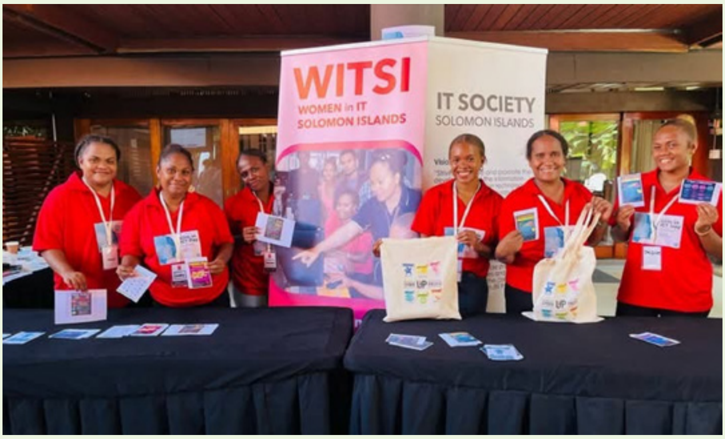


Figure 30: SIG ICT Services staff joined Women in IT Solomon Islands (WITSI) to raise cyber awareness during the Girls in ICT event on 24 April 2025 at the Solomon Kitano Mendana Hotel, Honiara, Solomon Islands

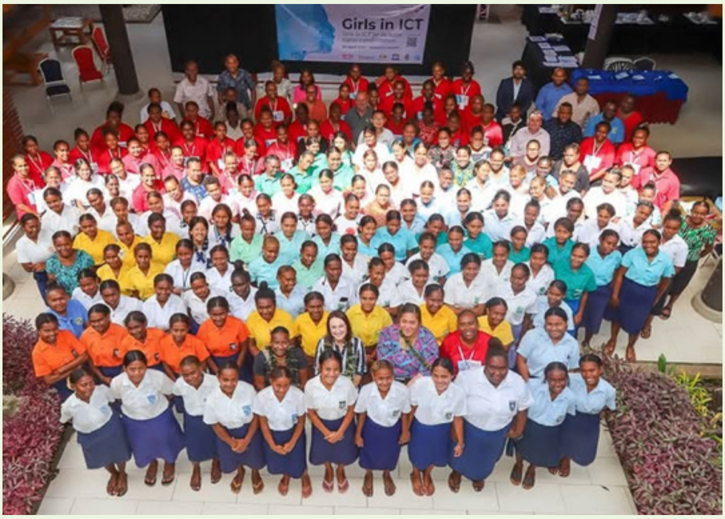
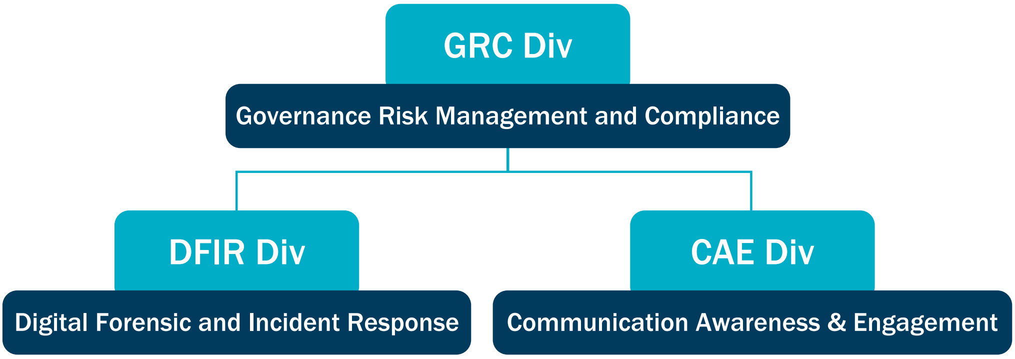


Figure 31: Group photo of WITSI members and students from various schools attending the Girls in ICT event, on 24 April 2025, at the Solomon Kitano Mendana Hotel, Honiara, Solomon Islands

Tonga

Tonga Computer Emergency Response Team

CERT Tonga is the Kingdom of Tonga's National Computer Emergency Response Team and point of contact for cyber security issues (incident response, awareness raising, training, digital forensics and cyber security bulletins and advisory). The CERT Tonga Department is one of the departments operating under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (MEIDECC). CERT Tonga's amended organisational structure consists of 4 established staff members, and 2 contracted staff members under the CERT Tonga Cybersecurity Workforce Development Program (CWDP) capacity-building project, funded by CERT NZ from November 2021 to December 2025.



GRC Div

Governance Risk Management and Compliance

DFIR Div

Digital Forensic and Incident Response

CAE Div

Communication Awareness & Engagement

Figure 32: CERT Tonga divisional organisation structure

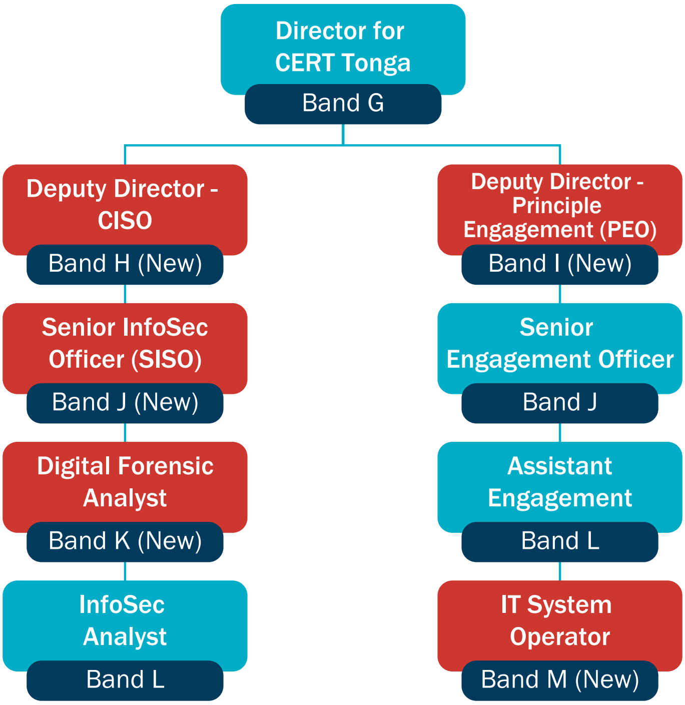


Figure 33: Updated organisation structure with new positions

The CERT Tonga Department consists of 3 divisions: Governance Risk Management and Compliance Division; Communication Awareness and Engagement Division; and Digital Forensic and Incident Response Division. Previously, there were only 2 divisions – the Engagements and Technical divisions.

There are now 4 established positions: the Director, the Senior Engagement Officer, the Assistant Engagement Officer and the Information Security Analyst. There are supplementary positions currently filled by CWDP-contracted staff: the IT System Operator (apprentice) and the Security/Forensic Analyst. The CWDP was extended for another 7 months up to the end of August 2025. The newly proposed positions are still in draft and submitted with the budget proposal for FY2025–26. These positions are Deputy Director (Chief Information Security Officer), Deputy Director (Principal Engagement Officer), Senior Information Security Analyst, Digital Forensic Analyst and IT System Operator.

CERT Tonga's constituents are government ministries, departments and agencies; the private sector; public enterprise; and NGOs.

People or organisations in Tonga can report cyber incidents via email, telephone, the social media platform (CERT Tonga Facebook page), CERT Tonga website or face to face during office hours.

The 3 most common cyber threats Tonga faces are:

- hackers (including state actors)
- malware (infostealer and ransomware)
- international malicious actors (professionals exploiting vulnerable IP address and DNS).

Threat landscape

CERT Tonga is equipped to respond to:

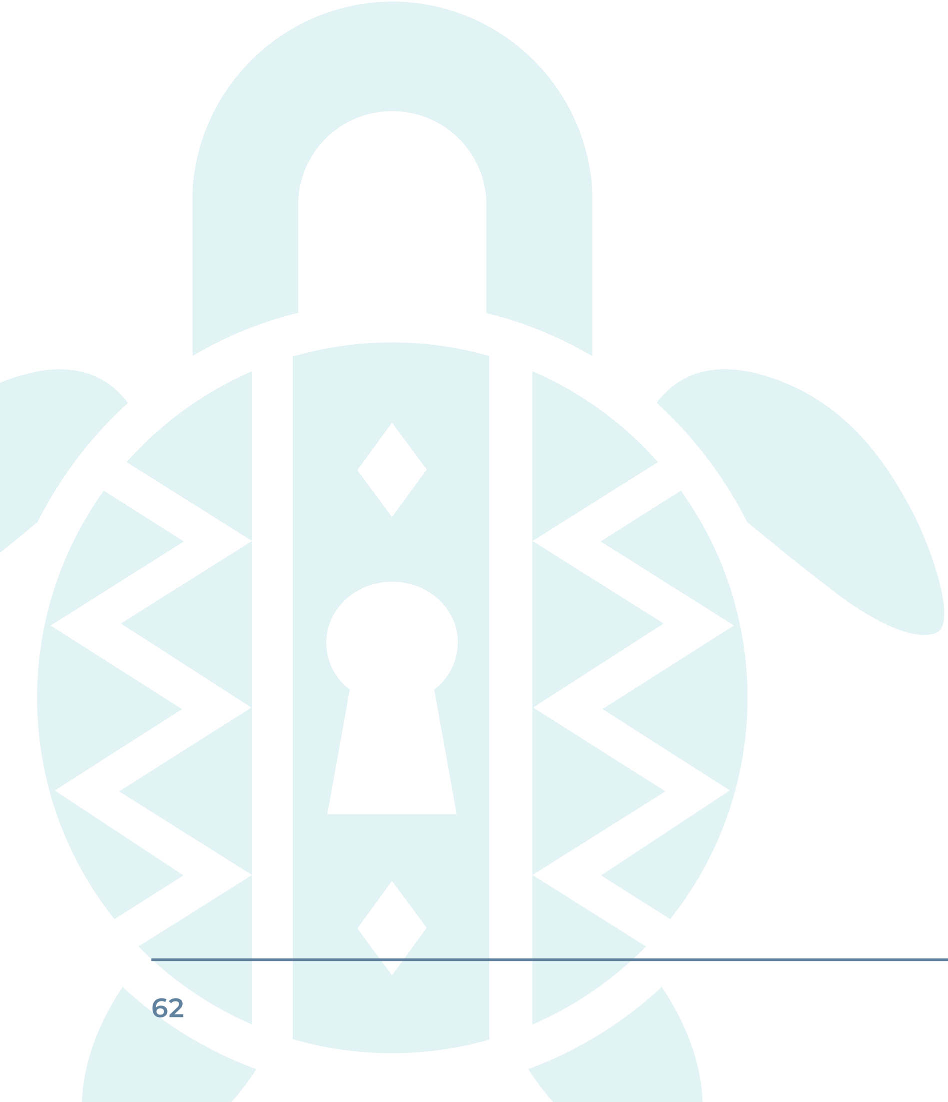
- phishing emails (scam emails)
- ransomware (to a limited extent, mainly coordinating stakeholders and third parties)
- fraud emails (coordination and collaboration with stakeholders and third parties)
- requests from the Cybercrime Working Group (Attorney General's Office and Tonga Police) to assist with cases of social media driving electronic-communications abuse (misinformation, disinformation and malinformation) regarding government officials and high-profile cases.

There was a slight increase in the number of incidents with new variations of scams and fraud. There were mainly domestic reports of information leaks, cyber-harassment and hate speech on social media aimed at key government officials. There were also new scams promising free online education and courses translated in Tongan (most likely using AI), and one major fraud transaction involving one of the public enterprises, with several occurrences of mishandled transfer of funds. Incidents also included web defacement and compromised business emails systems.

Awareness raising

CERT Tonga raises awareness through:

- providing awareness and community outreach, including to outer islands, for government ministries, the private sector, NGOs and schools. CERT Tonga has used the awareness raising materials provided by PaCSON as part of our outer islands outreach and domestic awareness campaigns
- providing joint radio broadcasts to raise awareness of cyber threats and the importance of security
- introducing and hosting training on cyber security and the countermeasures that could be used to mitigate such risk. This has included cyber hygiene training to the IT system administrators and operations at the end of FY2023–24.



Case study: developing the PIF Cyber Risk Assessment and Incident Response Plan

The Cyber Risk Assessment (July 2024) and Cyber Incident Response Plan (August 2024) were developed following the Cyber Taskforce collaboration with cyber experts from Australia's Cyber Rapid Team prior to and during the 53rd Pacific Islands Forum Leaders Meeting (PIFLM53). These documents supported the playbook and guidance for the Command Post battle rhythm and routines during PIFLM53, which the Government of Tonga hosts once every 18 years. The PIFLM53 was held successfully with no cyber incident or cyberattack.

CERT Tonga also published a Monthly Security Bulletin and Advisory (ongoing) and the CERT Tonga Weekly Report Analysis of Shadowserver Scan Reports.

CERT Tonga also completed the Outer Island Outreach Program that started in April 2023. In October 2024, CERT Tonga deployed to the Northern Islands of Vava'u (the second largest of the island groups in Tonga) and conducted 11 awareness sessions, including at 7 high schools and colleges. In September 2024, CERT Tonga was selected for, and won, the 2024 Information Society Innovation Fund (ISIF) Asia Award for Outstanding Digital Development Contributions in protecting Tongan internet users online during the APNIC58 conference, back-to-back with the Pacific Internet Governance Forum 2024 (PacIGF2024) in Wellington, New Zealand.

The Defensive Readiness and Cyber Security Exercise Program to strengthen Tonga's emergency response capacity and preparedness was held from 16 to 20 September 2024. More than 50 participants from line ministries, internet service providers and the private sector attended the training program, co-hosted by CERT Tonga under the Ministry of MEIDECC and Retrospect Labs through Australia's Department of Foreign Affairs and Trade (DFAT). The program focused on several fundamental principles and common protocols for responding to cyber security incidents, and there was an interactive cyber security exercise where participants were required to be part of an incident response team dealing with a ransomware case at a fictional company. A realistic scenario was designed and crafted to simulate an actual incident response operation, providing offline files and live elements for the participants to interact with.

Case study: cyber hygiene training – 20 June 2024

CERT Tonga was also grateful for the support given by the US Agency for International Development (USAID) for Pacific Islands through USAID Digital Connectivity and Cybersecurity Partnership Pacific Activity. This helped CERT Tonga equip participants with practical knowledge and best practices for safeguard against cyber threats.

Figure 34: Opening of the USAID DCCP Workshop

Figure 35: Cyber hygiene training on 20 June 2024, at Fe'ao Moe Ngalu, Customs Building, Ma'ufanga

CERT Tonga's Contact Detail
Q&A
Tonga's National Computer Emergency Response Team

Figure 36: Cyber security awareness training for the Ministry of Internal Affairs Social Protection & Disability Division, February 2024

UPGRADE TWO-FACTOR AUTHENTICATION
UPDATE DEVICES AND APPS
UPSIZE
UPDATE
www.bsp.to
BSP
"A Safe and Secure Digital Environment for the Kingdom of Tonga and its citizens"
CERT TONGA

Figure 37: Tonga Women in ICT (TWICT) ICT Expo, Queen Salote Memorial Hall, 21–22 March 2024

Figure 38: Outer Island outreach to Vava'u Islands: Cybersecurity Awareness Raising Campaign, 8–14 October 2024

Figure 39: Drills and exercises, for the Cyber Task Force RAPID Team Risk Assessment and Incident Response Plan (drill) implementation, 24–26 July 2024, prior to and during the PIFLM53, 19–31 August 2024

Figure 40: Defensive Readiness and Cyber Security Exercise Program to strengthen Tonga's emergency response capacity and preparedness, 16–20 September 2024

CERT Tonga

{retrospect_labs}

Figure 41: Participants at the CERT Tonga and Retrospect labs training

Tuvalu

Department of Information and Communications Technology

The Department of Information and Communications Technology underwent a transition in February 2024, shifting from the Ministry of Justice, Communications, and Foreign Affairs to the Ministry of Transport, Energy, Communication, and Innovation. Responsible for overseeing the government's technological landscape, ICT plays a pivotal role in various sectors. While certain government departments employ IT specialists tailored to specific requirements, the broader spectrum of technological affairs falls under the purview of ICT.

Under the leadership of the Director and 2 senior officers, ICT is organised into key teams such as networking and database management. These teams are further subdivided to also address critical areas such as cyber security. These teams collaborate closely with the virtual CERT, plays a role in regulatory compliance, and spearheads the Government of Tuvalu's ambitious digital transformation objectives.

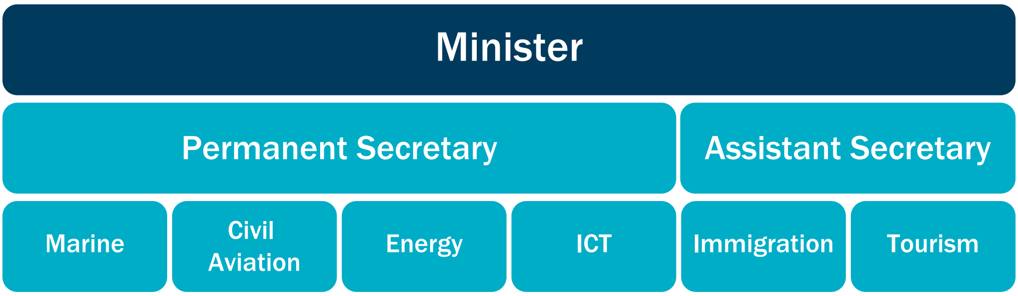


Figure 42: Ministry of Transport, Energy, Communication and Innovation structure

As mentioned above, our CERT team is virtual and involves collaboration between the Department of ICT, Tuvalu Telecom, Tuvalu Police and the Attorney General's Office. This collaboration extends the reach of our awareness programs – which includes input form partners like Cyber Security, Pasifika, PaCSON, Get Safe Online and PILON – to primary school students, as well as to the wider community.

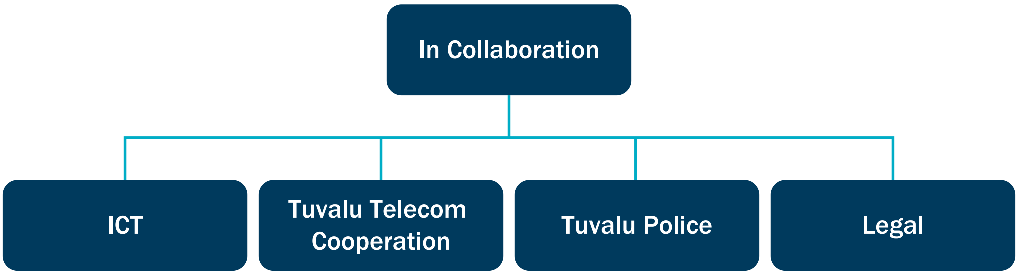


Figure 43: Virtual CERT team collaboration

The World Bank is funding a submarine cable project for Tuvalu and, while that is happening, further collaboration to expand satellite internet bandwidth is also in progress, with the timely introduction of Starlink satellite services to boost connectivity speed and reliability. Our virtual CERT will continue to educate the general public on how to stay safe online. There have been a few workshops held in the capital and some on the outer islands by the Cyber Safety Pasifika team from Tuvalu Police.

Threat landscape

In Tuvalu, cyber incidents can be reported to the police, the Department of ICT or the Office of the Peoples' Lawyer, who is the major legal aid service for the general public.

Generally, Tuvalu shares many similarities regarding cyber security threats with the broader Pacific region. Some common types of cyber threats to Tuvalu include:

- malware
- phishing attacks
- scams
- identity theft and fraud
- ransomware.

Awareness raising

The Department of ICT, in collaboration with the Tuvalu Police, supported various community engagement and awareness raising efforts during the reporting period, including through community outreach, visits to schools and engagement via social media. Our office and the police office are always open to the public if there are any cyberattacks or any online issues.

The Department of ICT uses our social media accounts as a platform to share cyber security and cyber safety updates. The Department of ICT tries to share the security advisories from PaCSON partners – like Tonga CERT, Vanuatu CERT, NZ CERT and the US' CISA – on various social media outlets like the Government's Facebook pages and Tuvalu news pages.

Vanuatu

CERT Vanuatu (CERTVU)

CERTVU is Vanuatu's national CERT, established under the Department of Communication and Digital Transformation (DCDT) – which was formerly known as the Office of Government Chief Information Officer (OGCIO) – within the Ministry for the Prime Minister, Vanuatu Government. CERTVU currently has 4 dedicated staff members, 3 of whom are employed on a full-time basis and one on a contracted basis.

As the Vanuatu national CERT, CERTVU provides services to the entire nation – the Government, businesses and civil society.

Services are provided through:

- visiting CERTVU's online incident report portal via CERTVU's website
  - **https://cert.gov.vu/index.php/services/incident-resolution**
- calling our phone contact
- visiting our social media platform
- coming into the office to report any cyber incident. CERTVU is operating an open-door policy, meaning there is no need to make an appointment to come to the office. People can come in at any time during working hours.

Threat landscape

The 3 most common cyber threats in Vanuatu are:

- phishing
- online scam and fraud
- malware.

Awareness raising

Awareness raising activities by CERTVU include:

- participating in national radio talk show
- participating in national events
- producing cyber security awareness videos
- conducting a Cyber Smart Pacific, Cyber Up Campaign
- conducting a one-to-one community awareness program
- conducting a cyber awareness campaign in schools
- conducting a business house awareness campaign
- encouraging public and private awareness and intelligence sharing
- producing flyers, brochures and guides on cyber security.

Publications by CERTVU include:

- security bulletins – **https://cert.gov.vu/index.php/resources/bulletins**
- security advisories – **https://cert.gov.vu/index.php/services/online-advisories-alerts**
- news and press releases – **https://cert.gov.vu/index.php/news**
- the Vanuatu Digital Transformation Master Plan – **https://cert.gov.vu/index.php/resources/policies-and-strategies**

Achievements

Achievements by CERTVU in 2024:

- hosted Senior Secondary School Cybersecurity Boot Camp
- introduced Cybersecurity Defence Readiness, capacity-building program
- conducted Cyber Smart Pacific, Cyber Up Campaign
- delivered ongoing radio talk show program on cyber security
- established the Vanuatu Cyber Incident Response community
- held ‘a Day with CERTVU’ event.

Case study: cyber bootcamps for secondary schools

May 2024 marked another milestone in CERTVU's cyber security journey as we teamed up with 8 senior secondary schools in Port Vila to deliver the first Vanuatu Senior Secondary School Cybersecurity Boot Camp. We had over 50 senior students participating in 2 days of intensive cyber security lectures. Topics ranged from the basics of cyber security to identifying threats and security best practices, while also focusing on the good use of ICT. The boot camp finished with a Capture the Flag session, where students put all their learning into problem solving different challenges. There was also a career path session where we invited individuals from different sectors to talk about their respective educational journeys in the fields of ICT and telecommunications. The primary objective of this boot camp was to develop future cyber experts in different focus areas. We believe that involving students as early as high school will help shape and guide them into pursuing a career in the field of cyber security.

Figure 44: Cybersecurity Boot Camp participants

Figure 45: Students during the cyber security boot camp

Figure 46: CERTVU delivering training during boot camp

Figure 47: Cybersecurity Defence Readiness course participants

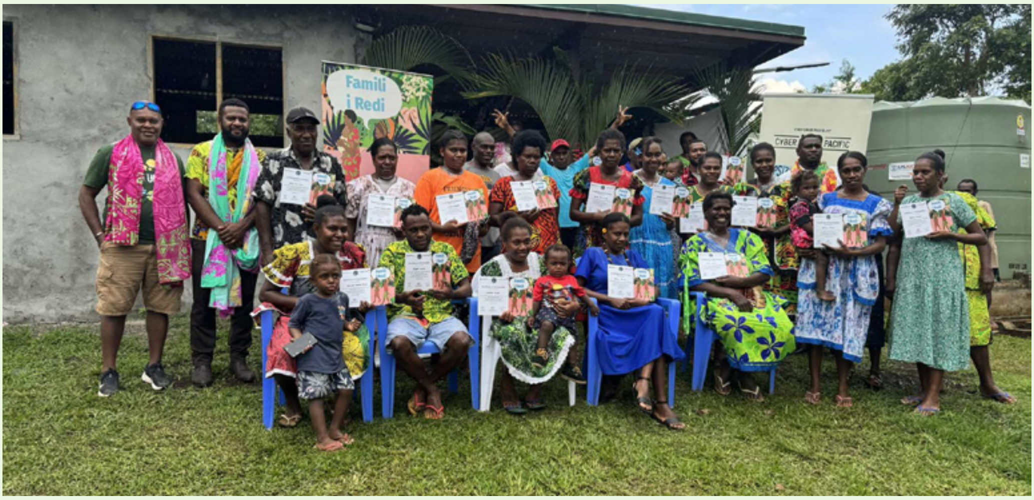


Figure 48: Teuoma Fork Road community participants in the Cyber security awareness for Family I Redi workshop

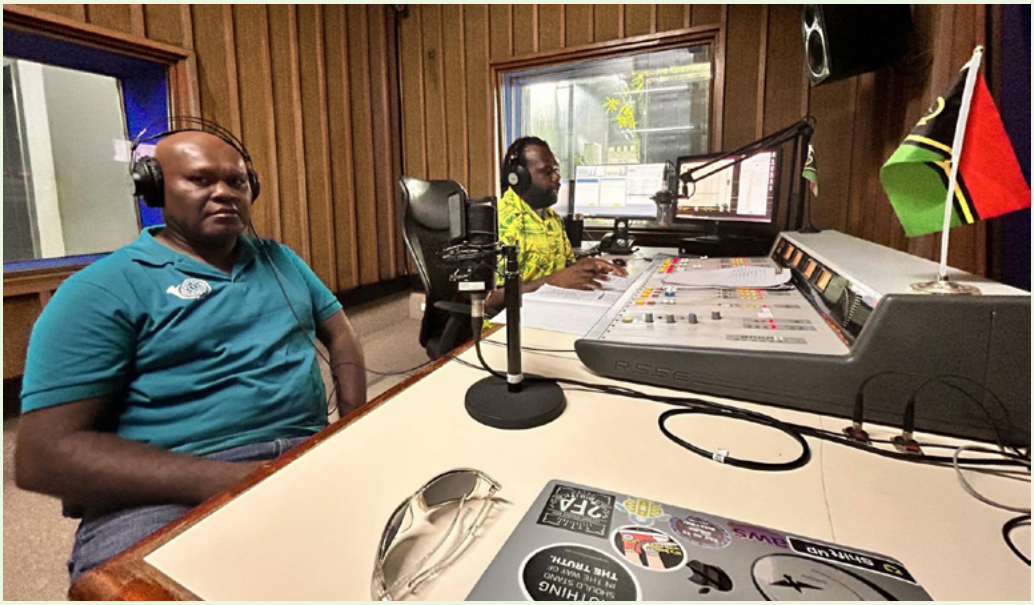


Figure 49: CERTVU delivering a one-hour session on ICT and cyber security on a talk show on Radio Vanuatu every Friday

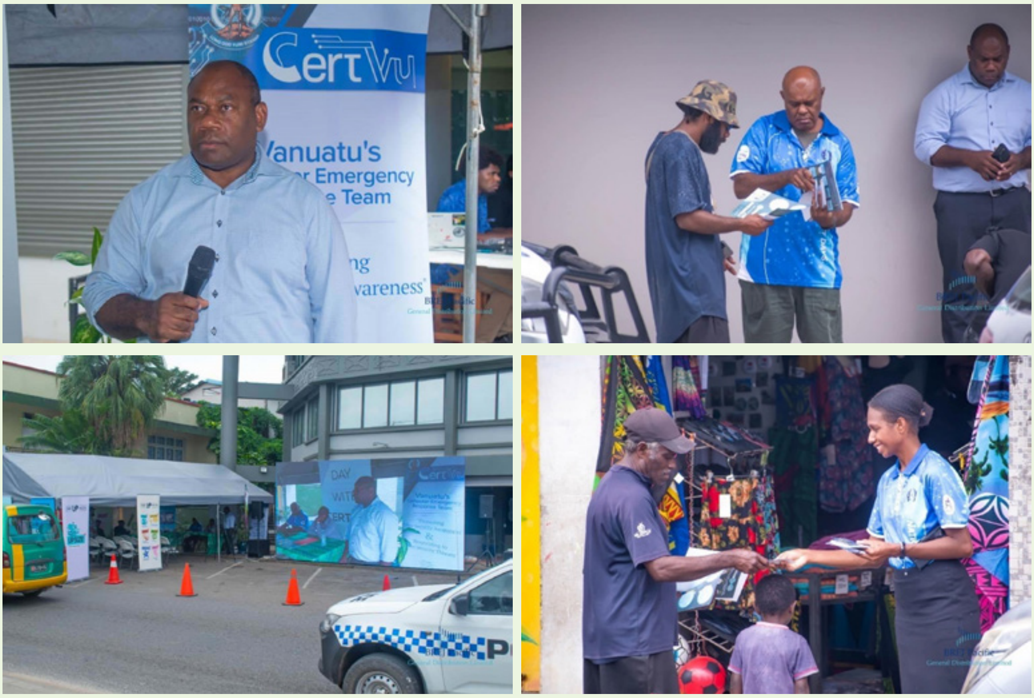


Figure 50: 'A day with CERTVU' event in town, stepping out of the office comfort zone to meet the public and provide insightful information on cyber security

Figure 51: The first meetup session for our Vanuatu Cybersecurity Incident Response community brought together different volunteers from all their respective fields to collaborate under the community's banner

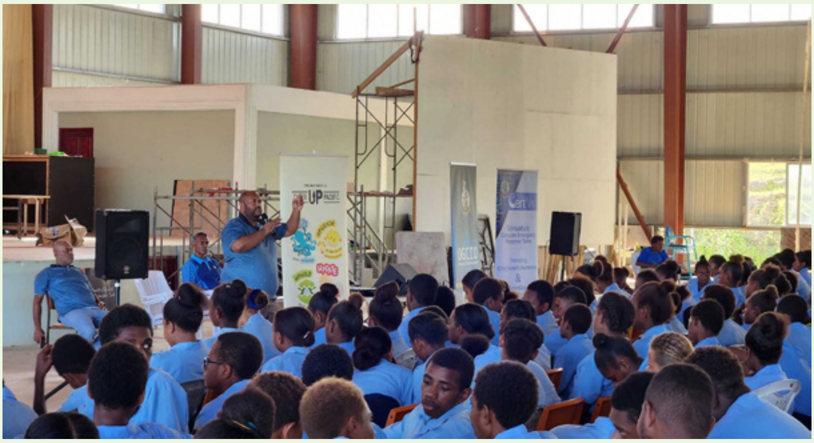


Figure 52: CERTVU delivers a cyber security awareness session for the Epauto Adventist Senior Secondary School

Figure 53: Participants is the Vanuatu National Cybersecurity Agency consultation workshop

Partner Updates

Agence nationale de la sécurité des systèmes d'information

Agence nationale de la sécurité des systèmes d'information (ANSSI) is a French government agency, specialising in cyber security. It has cyber threat intelligence (CTI) teams, a CERT team (CERT-FR), regulation and certification teams, regulatory teams, an expert team and so on. ANSSI's mission is to defend France's national information systems, but it is also responsible for advising and supporting administration and critical French companies. ANSSI comes under the General Secretariat for Defence and National Security (SGDSN), which is in the Prime Minister's Department.

Last year, ANSSI saw 3 major common cyber security threats:

- opportunistic attacks (vulnerability exploits, mostly)
- destabilisation attacks (DDoS, defacement and so forth)
- targeting of supply chains.

In 2024, ANSSI attended the PaCSON AGM in the Cook Islands for the first time. The head of operational cooperation attended members' calls, when invited, and partners calls.

Incident reports were posted on the PaCSON portal until a better system could be put in place.

In the context of the 2024 Paris Olympic and Paralympic Games, ANSSI took the lead on cyber security initiatives. To this end, the framework put in place by ANSSI and the different entities involved in organising the Games – including the Interdepartmental Olympic and Paralympic Delegation (DIJOP), the Ministry of the Interior and of the Overseas (MIOM), and the Paris 2024 Organising Committee – was structured around 5 main objectives:

- perfecting our knowledge of the cyber threats facing the Games
- ensuring the security of critical information systems
- protecting sensitive data
- raising awareness and understanding of the Olympic ecosystem
- preparing for a potential intervention in the event of a cyberattack impacting the Games.

With the support of the MIOM's *Coordination Nationale pour la Sécurité des Jeux* (CNSJ), ANSSI delineated an Olympic and Paralympic ecosystem of almost 500 entities, categorised into 3 different groups defined by their level of criticality. Events for the Olympic and Paralympic Games were held both in mainland France and French Polynesia.

The entities within this ecosystem were encouraged to use ANSSI's automatic auditing tools.

From 2023, an awareness-building plan was implemented across the Olympic and Paralympic ecosystem. This plan allowed easier communication of information about the cyber threats faced by large-scale sporting events as well as distribution of cyber security recommendations and best practices.

In cooperating with the different state services involved in the preparation, the agency established a framework of cyber incident monitoring, alerting and processing. The framework entailed adopting a specific stance intended to withstand intensified operational activity.

Several crisis response drills were organised in 2023 to collectively prepare for any prospective cyberattacks. ANSSI also offered 'drill kits' to entities within the Olympic and Paralympic ecosystem who may have wished to practise independently. These kits were used by around 100 entities.

Exceptional interdepartmental coordination measures were put into place – notably in the *Centre National de Commandement Stratégique* (CNCS) – in order to centralise cyber information. Detected cyber security events were all reported to ANSSI – the sole entry point of cyber reports – by the organiser, the ministries, and the wider ecosystem, in order to consolidate a common appraisal of the cyber situation during the Olympic and Paralympic periods.

Close coordination with the organiser of the Games was arranged, via the presence of one of ANSSI's liaison officers with Paris 2024's cyber teams. This facilitated the transmission and qualification of cyber security events. The agency's national and international partners were also regularly mobilised prior to the Games, in order to guarantee cooperation during the event. Over the duration of the Games, cyber information pertaining to the event was consistently shared with international partners, bilaterally and within the framework of specific structures – particularly with the International Cooperation Centre and the EU-CyCLONe European crisis-management network.

Between 8 May and 8 September 2024, there were 548 cyber security events were reported to ANSSI that impacted entities involved in running the 2024 Paris Olympic and Paralympic Games. These events were brought to the agency's attention and were subsequently processed by its operational teams.

Out of all of these reported cyber security events, close to half resulted in non-availability – and a quarter of these cases were caused by DDoS attacks. The rest of the events were characterised by the report of vulnerabilities, by data leaks or by attempted or successful compromises. The sectors of activity most affected by these events were governmental, sports, transportation, entertainment (Paris 2024 and Game locations) and telecommunication entities.

Though the agency and its national partners assisted several victims in resolving incidents, no cyber security events disrupted the opening and closing ceremonies, or running the competitions. All of the cyber security events that occurred during this period generally had a rather minor impact.

ANSSI publications in 2024:

- Cyber Threat Overview 2024 (annual report): **https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-004/**
- Security alerts: **https://www.cert.ssi.gouv.fr/alerte/**
- CTI threat reports: **https://www.cert.ssi.gouv.fr/cti/**
- Security notices: **https://www.cert.ssi.gouv.fr/avis/**
- IOCs: **https://www.cert.ssi.gouv.fr/ioc/**
- Recommendation: **https://www.cert.ssi.gouv.fr/dur/**
- CERT-FR's news bulletin: **https://www.cert.ssi.gouv.fr/actualite/**
- Reflex cards: **https://www.cert.ssi.gouv.fr/fiche/**

Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security (CCCS) is part of the Communications Security Establishment (CSE), Canada's national cryptologic agency, and reports directly to the Minister of National Defence. As Canada's technical authority on cyber security, CCCS is responsible for safekeeping the information and systems that Canadians rely on daily. CCCS protects and defends Canada's valuable cyber assets and leads Canada's federal response to cyber security events. Simultaneously, CCCS collaborates with international partners to mitigate and respond to cyber events. Cumulatively, CCCS raises Canada's cyber security bar so Canadians can live and work online safely and with confidence.

Ransomware is the largest threat to Canadian businesses and citizens. Common cyber security threats include social engineering and phishing, unauthorised access and malicious code deployment.

CCCS attended the 2024 PaCSON AGM in Rarotonga. Several valuable conversations were had with PaCSON members during the AGM and their insights have influenced future engagements in the region. Towards the end of 2024, CCCS began working with Global Affairs Canada to craft the 2025 GeekWeek participation opportunity for PaCSON members.

In 2024, CCCS shared 3 items with the PaCSON community:

- CCCS November Roundup of Incidents (TLP:AMBER Level)
- Canada's new National Cyber Threat Assessment (TLP:CLEAR)
- Canada's Cyber Readiness Goals & Implementation Toolkit (TLP:CLEAR)

CCCS publications include:

- **https://www.cyber.gc.ca/en/alerts-advisories**
- **https://www.cyber.gc.ca/en/guidance**
- **https://www.cyber.gc.ca/en/news-events**

Cybersecurity and Infrastructure Security Agency

The Cybersecurity and Infrastructure Security Agency (CISA) is part of the US Department of Homeland Security. As the US's cyber defence agency and as the National Coordinator for the security and resilience of US critical infrastructure, CISA leads the national effort to understand, manage and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. Our primary stakeholders are US critical infrastructure owners and operators; US federal, state, local, territorial and tribal governments; the private sector; and the American people.

CISA's 3 most common cyber incidents are:

- ransomware
- malware (information stealers)
- supply chain exploitation.

In 2024, CISA contributed to PaCSON in the following ways:

- Two CISA representatives attend the 2024 PaCSON AGM and facilitated a workshop on Secure-by-Demand to support PaCSON members, when selecting vendors, to assess the software manufacturers' approach to product security.
- CISA worked with other US government partners to support the attendance of some PaCSON partners at the AGM.
- CISA shared information with PaCSON through the portal and community calls.

CISA regularly releases cyber security alerts and advisories on specific cyber security and industrial control systems issues, as well as in-depth publications on cyber security and critical infrastructure security. CISA also maintains the Known Exploited Vulnerabilities Catalog, the authoritative source of vulnerabilities that have been exploited in the wild. These resources can be found at **cisa.gov.**

Forum of Incident Response and Security Teams

The Forum of Incident Response and Security Teams (FIRST) brings together incident response and security teams from across the world to share knowledge and insights, ensuring a safer internet for all. Founded in 1990, FIRST consists of teams from over 770 corporations, government bodies, universities and other institutions. Participants represent over 110 countries in the Americas, Asia, Europe, Africa and Oceania.

FIRST gives the global incident response community a place to build trust and work together. It also provides valuable opportunities to build capability, such as:

- technical conferences for security experts
- hands-on classes
- annual incident response conference
- advisory publications and web services
- special interest groups and
- community and capacity building.

FIRST has been a PaCSON partner since 2023 and enjoys strong membership and mutual engagement across our events and activities.

FIRST has collaborated with PaCSON and its community through various channels. Some examples are:

- In 2024, FIRST continued engagement with CERT Tonga and CERTVU as participants in the FIRST Suguru Yamaguchi Fellowship Program.
- In June 2024, FIRST was excited to support the PaCSON Secretariat to welcome a strong delegation of Pacific participants to the 2024 FIRST Annual Conference in Fukuoka, Japan.
- In September 2024, FIRST collaborated with Asia Pacific Network Information Centre (APNIC) to host a Technical Colloquium (TC) as part of the APNIC 58 Conference held in Wellington, New Zealand. The TC including speakers from CERT NZ, CERT Tonga, Kiribati CERT and CyberSafe Samoa. The event was held in conjunction with the Pacific Internet Governance Forum) and the Wellington Forum on Pacific Internet Capacity Building. Together these events engaged diverse stakeholders across the Pacific cyber security ecosystem, including many PaCSON members.
- As part of the November 2024 APCERT-FIRST Asia Pacific Regional Symposium, FIRST organised the Asia Pacific (APAC) Incident Response Fellowship Program. The program welcomed 9 participants from the Asia Pacific including from Kiribati, the Solomon Islands and Papua New Guinea. The fellowship was generously supported by the APNIC Foundation.

FIRST continues to work with the Pacific cyber security community through formal and informal mentorship, information sharing, training, advisory support, and community engagement and looks forward to building even stronger collaboration and engagement with PaCSON and the wider community in 2025.

- FIRST webpage: **https://www.first.org**
- FIRST newsletter: **https://www.first.org/newsroom/newsletters/**

Figure 54: APAC Incident Response Fellows at the November 2024 APCERT-FIRST Regional Symposium

Figure 55: Speakers at the FIRST TC held during the September 2024 APNIC58 Conference

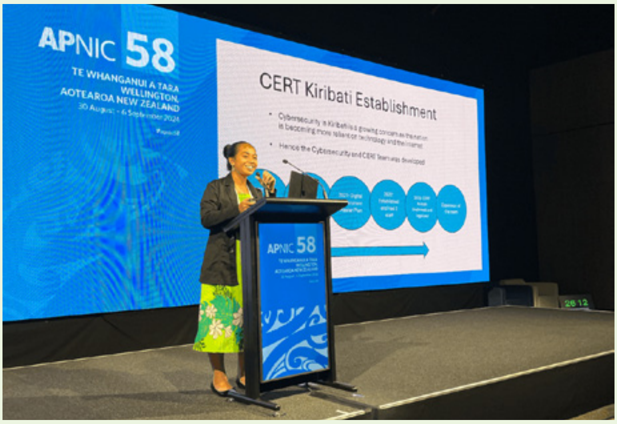


Figure 56: CERT Kiribati presenting during the FIRST TC at the APNIC58 Conference

Figure 57: Some Pacific delegates at the FIRST TC during the September 2024 APNIC58 Conference

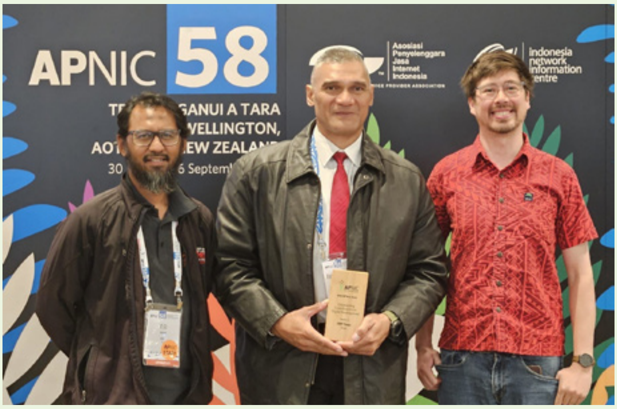

APNIC 58
Asosiasi Penyelenggara Jasa Internet Indonesia
Indonesia network information centre

Figure 58: CERT Tonga awarded the ISIF Asia Award for Outstanding Contributions to Digital Development at the APNIC58 Conference

Friend Updates

eSafety Commissioner

The eSafety Commissioner (eSafety) is Australia's independent online safety regulator, governed by the Online Safety Act 2021.

Except for the Commissioner, all staff employed to undertake the functions of eSafety are staff of the Australian Communications and Media Authority (ACMA). In 2023–24, eSafety averaged 164 staff, with some additional contractor employees. eSafety sits within the Infrastructure, Transport, Regional Development, Communications and the Arts portfolio, with the Honourable Michelle Rowland MP, the Minister for Communications, being the responsible minister. Further information about eSafety's structure can be found **here**.

eSafety focuses on online safety and online harms, rather than cyber security threats. Priorities in 2024–25 included:

- technology-facilitated gender-based violence (TFGBV)
- terrorism and violent extremist content and youth radicalisation
- sexual extortion
- impacts of generative AI on online safety (for example, deepfakes and nudify Apps)

eSafety has largely focused on bilateral relationships with PaCSON members on a range of online safety topics, but looks forward to engaging at a regional level over 2025.

eSafety has a range of publicly available resources, including **tech trends and challenges papers**, **advisories and blog posts**, resources for **industry** and **research products**. Key research undertaken in 2024 includes the digital lives of young LGBTIQ+ people, and the risks and benefits of online gaming for children and young people.

Case study: 'Train of Trainers Program' to build Pacific experts' capacity to provide online safety education in their communities

In November 2024, eSafety delivered a training of trainers (TOT) for frontline workers in the Pacific about TFGBV. The TOT aimed to build capacity among identified gender-based violence trainers from across the Pacific on best practice approaches to identifying and responding to TFGBV. Over 5 days, 20 trainers and government representatives from 9 Pacific Island Countries gathered in Fiji to discuss incidents of TFGBV in their local contexts, and learn how to upskill frontline workers on safely identifying TFGBV and supporting survivors.

Cyber Safety Pacifika

Cyber Safety Pacifika (CSP) is a Pacific Chiefs of Police program, sponsored and delivered by the Australian Federal Police (AFP) and its strategic partners to small core teams (1 Team leader, 4 team members), noting activities are collaboratively delivered.

CSP delivers cyber prevention and investigation capability development to Pacific police.

The 3 most common cyber security threats reported during CSP training are phishing, scams, and misinformation and disinformation

CSP has contributed to PaCSON by providing capability development opportunities to Pacific police, thereby enhancing cyber resilience in Pacific communities and complementing broader regional cyber security efforts.

In the last 12 months, CSP has run regional training programs in Palau, Australia, Niue and the Cook Islands, training 82 police from 18 Pacific nations. CSP also helped establish and train the Tonga Police Cybercrime Team (12 members) in July 2024.

Further information can be found on the website **www.cybersafetypasifika.org**, and articles in Pacific Community for Law Enforcement Cooperation newsletters.

Global Forum on Cyber Expertise Pacific Hub

The Global Forum on Cyber Expertise (GFCE) Pacific Hub team has 3 members: a Director and 2 Senior Advisers.

The GFCE Pacific Hub is an impartial and independent, but pragmatic, action-oriented and responsive platform that focuses on empowering and upskilling Pacific communities and structures. This is done through ongoing collaboration with both donors and actors, including those who can build cyber capacity that is tailored to the uniqueness of the Pacific at the national, sub-regional and regional levels.

The Hub offers practical advice, expertise and assistance that aligns with donor development programs in an effort to ensure that a demand-driven approach is at the forefront of activities.

Furthermore, the Hub provides timely access to the global network of expert members and partners who deliver on the requirements of their respective countries. This Hub collaboration is done with a view to ensuring that each of the Pacific Island Countries and territories involved has adequate levels of capacity, expertise, skillsets and resources to address cyberattacks in an effective and timely manner.

The common cyber security threats that the Hub is observing in the region are:

- **Phishing and social engineering attacks:** Cybercriminals use deceptive emails or messages to trick individuals into revealing sensitive information, such as passwords or financial details.
- **Ransomware and malware:** Malicious software is used to encrypt or steal data, often demanding payment for its release. This can disrupt businesses, governments and individuals.
- **Weak cyber security infrastructure:** Many Pacific nations face challenges in implementing strong cyber security frameworks, making them vulnerable to cyber threats and attacks.

The GFCE Pacific Hub fully supports and continues to complement the work of PaCSON in the region by strengthening cyber capacity-building efforts, connecting PaCSON's member countries with global cyber expertise and resources and facilitating collaboration through a platform for networking and trusted connections.

Pacific Fusion Centre

The Pacific Fusion Centre (PFC) consist of 8 full-time staff:

- Director of the PFC (Pacific official)
- Assistant Director of the PFC (Pacific official)
- Special Adviser (Australian embed)
- Technical Adviser (Australian embed)
- Corporate Adviser (Australian embed)
- Executive Assistant (Vanuatu)
- Business administrator (Vanuatu)
- Cleaner (Vanuatu).

There are also 3 cohorts of 5 analysts participated per year (15 total), comprising officials from across the Pacific.

There are also 2 short-term embedded technical advisers from NZ and the UK per year.

The PFC looks at cyber security issues for the region from a strategic perspective. Our top 3 threats reflect the analysis in the PaCSON Annual Report.

The PFC participates in some PaCSON community calls. Our Assistant Director (AS equivalent) attended some elements of the 2024 PaCSON AGM but had to leave early. In September 2024, we held a roundtable with PaCSON in Canberra. PaCSON reviewed the PFC's Pacific Regional Security Outlook Report 2024–25. However, monthly calls between PFC and PaCSON dropped off late last year

The Pacific Security Outlook Report 2024–25 was just released on the Pacific Islands Forum (PIF) website. The PFC also has its beneficiary only website (available to all PIF members and Council of Regional Organisations of the Pacific - CROP - agencies).

Working Group Updates

Awareness Raising Working Group

We would like to begin this update by congratulating everyone at PaCSON for their dedication and hard work in advancing our awareness efforts throughout 2024. The Cyber Up and Cyber Up Pacific campaigns faced unique challenges in reaching and educating Pacific communities spread across the vast, blue Pacific. Despite these obstacles, the Awareness Raising Working Group (ARWG) is pleased with the progress made, building on previous years' activities and continuing to plan new initiatives for PaCSON.

At the 2024 AGCM in the Cook Islands, the ARWG shared updates on Pacific cyber security efforts and introduced the 'starter packs' initiative, designed to reinvigorate existing campaigns. A key goal of these packs is to empower stakeholders to launch their own awareness activities using the Train the Trainer model.

As Co-Convener of the ARWG with the Solomon Islands, Samoa managed the dual challenge of leading these efforts, while also preparing for CHOGM in October 2024. CHOGM, with its significant Pacific representation, provided an excellent opportunity to showcase all Cyber Up themes to Commonwealth leaders and delegations. To maximise impact, billboards featuring the campaign themes in both English and Samoan were set up, cyber hygiene videos were produced and shared online, and a special newspaper wrap highlighting all Cyber Up concepts was published. This was especially well received, coinciding with the arrival in Samoa of Their Majesties The King and Queen, which drew widespread attention to the publication given the two events were on pages next to each other.

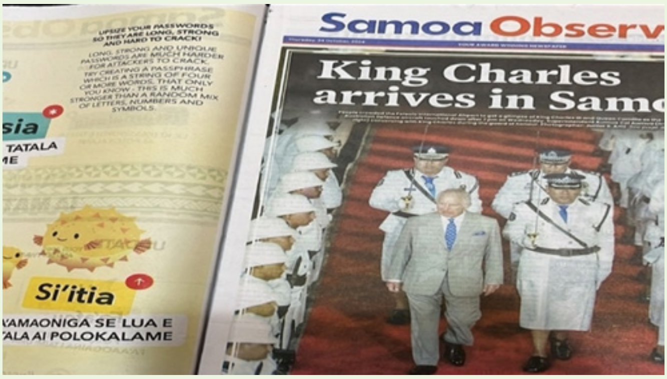
While these initiatives were mainly based in Samoa, they also represented a collective effort by the entire ARWG to raise awareness of cyber hygiene and security among all CHOGM participants. Members from other CERTs joined the Pacific Response Team, supporting the protection of CHOGM and demonstrating strong regional coordination in incident response.

A Security Operations Centre (SOC) was established to oversee both CHOGM activities and the daily operation cyber needs of the Samoan Government, ensuring the safety of the event and government functions. The awareness campaign was further enhanced by support from NCSC NZ, whose staff provided training before and after the event, and the RAPID Team from Australia, who managed the 24/7 SOC operations.

In summary, the ARWG dedication to the Cyber Up Campaign showed outstanding commitment in expanding the campaign's reach. By introducing new themes and leveraging high-profile events such as CHOGM for outreach, the team successfully delivered cyber security messages across the region. From developing practical 'starter packs' to executing large-scale, multilingual outreach and operation models, these efforts have significantly contributed to building a safer digital environment in the Pacific.

Figure 59: First Day: CERT and IT Team after the 7 am briefing

Figure 60: Team SOC operations



UPSIZE YOUR PASSWORDS SO THEY ARE LONG, STRONG AND HARD TO CRACK!

LONG, STRONG AND UNIQUE PASSWORDS ARE MUCH HARDER FOR ATTACKERS TO CRACK. TRY CREATING A PASSPHRASE WHICH IS A STRING OF FOUR OR MORE WORDS, THAT ONLY YOU KNOW - THIS IS MUCH STRONGER THAN A RANDOM MIX OF LETTERS, NUMBERS AND SYMBOLS.

sia

TATALA ME

Si'itia

AMAONIGA SE LUA E ALA AI POLOKALAME

Samoa Observ

King Charles arrives in Samo

Figure 61: Their Majesties The King and Queen arrive; Cyber Up newspaper wrap was a hit during CHOGM

Figure 62: Final day of the CHOGM meeting with Samoan traditional wear. The photo pose says it all. A great opportunity to collaborate, build great teams and learn together for a greater purpose. Chewooo!!!

Capacity Building Working Group

The goal of the Capacity Building Working Group (CBWG) is to identify the practical steps that PaCSON members can take to build their cyber security capability and capacity, and identify ways in which other members of PaCSON may be able to contribute support.

A key goal for this group is to support PaCSON members to have mechanisms, contacts and plans in place so that if a serious cyber security event were to occur, each member could receive and share information, and take steps to protect or recover from it.

2024 activities

In 2024, the CBWG focused on tangible efforts to bring PaCSON members together. New Zealand, with agreement from the Government of Samoa, funded the first Cyber Regional Technical Team to support Samoa's CERT and IT functions during CHOGM.

New Zealand thanks the representatives from Kiribati, Nauru, Palau, Papua New Guinea, the Solomon Islands, Tonga, Tokelau, Tuvalu and Vanuatu who were embedded within the local virtual teams. This was the first time a contingent of cyber security experts from across the Pacific were brought together to support a large-scale event. CBWG members have expressed positive sentiments about the deployment and would like to continue this vision for future initiatives.

At the 2024 PaCSON AGM, New Zealand recommended that a co-convenor be established to support Pacific leadership within the CBWG. After a vote, Tonga was nominated as the new co-convenor and New Zealand's role was re-confirmed. Over the last 12 months, New Zealand and Tonga have worked on building a CBWG Action Plan in preparation for the2025 PaCSON AGM. This will outline PaCSON's ambition in capacity building, providing actions for implementation, measuring mechanisms to review implementation, and providing structure to the CBWG moving forward. CBWG convenors look forward to presenting the final work plan, for release, at the 2025 AGM.

We are looking forward to continuing this momentum and developing new and exciting projects in the coming year.

Capacity Building Working Group membership

- Australia
- Fiji
- Niue
- Tokelau
- Nauru
- Papua New Guinea
- Solomon Islands
- Tuvalu
- Vanuatu
- Cook Islands
- Samoa
- Federated States of Micronesia
- New Zealand – Working Group Co-Convenor
- Tonga – Working Group Co-Convenor

Communications Working Group

The aim of the Communications Working Group (CWG) is to improve information sharing and the communication tools for the PaCSON community. CWG members work towards building and providing a collection of tools and processes that enable better communication and information sharing within the PaCSON community.

The CWG is responsible for improving the communication outlets and information sharing processes on behalf of the PaCSON community.

2024 activities

In 2024, the CWG was proud to publish the *PaCSON Annual Report 2023* for distribution to our members, partners and stakeholders. The annual report is the CWG's major delivery each year, and the Working Group would like to thank members, partners and friends for their contributions that enable the annual report to be a valuable resource for the community.

In addition to publishing the annual report, the CWG is also pleased to have published 2 news articles during 2024. The articles focused on the PaCSON delegation that attended the 2024 Annual FIRST Conference in Fukuoka, Japan, and the 2024 AGM. These articles served the dual purpose of publicising the important work that PaCSON does, and promoting awareness of key initiatives delivered by our members and partners.

The CWG also continues to maintain the PaCSON website, **pacson.org**.

In 2024, the website continued to be a central source of cyber security news and information. The website provides the PaCSON community with an online identity and has the ability to amplify awareness, share information and develop capacity. Viewership during the reporting period was steady, with a high number of visitors discovering it through organic searches. The website continues to serve as an effective means of communication for PaCSON members, partners and friends, and for disseminating a number of alerts and advisories, including the first Pacific-authored advisory from SamCERT.

Additionally, the PaCSON Signal chat platform transitioned from a website updates-only chat to a more general communication channel. This encouraged the PaCSON community to message each other not only with alerts and advisories, but also with questions, advice or anything else that they thought the chat could be used for. This more informal means of interaction has promoted increased cooperation and communication within the community.

The CWG enjoyed engaging with the ARWG and CBWG in their efforts to uplift PaCSON members throughout 2024, and looks forward to continuing its collaborations in 2025.

PaCSON Partners Working Group

The PaCSON Partners Working Group (PPWG) was established with the aim of providing PaCSON partners with opportunities to support and collaborate with the PaCSON Working Groups (ARWG, CBWG and CWG) on their activities. The PPWG is driven by the aspiration to provide a 'whole-of-community benefit' to PaCSON – working with all PaCSON members to increase their knowledge, capacity and resilience in matters of cyber security. Partners add value to the PaCSON community through their knowledge, resources, experience and capabilities.

In 2024, PaCSON was fortunate to have 2 new partners become a part of the community.

France's ANSSI and Canada's CCCS joined the PPWG in 2024. The PaCSON community gladly welcomed them into the network. This increase in PaCSON partner organisations demonstrates the growth and influence that the network has in the region. By leveraging the great work and advice of PaCSON partners, the PaCSON community is able to continue to uplift and upskill the region.

Throughout 2024 and beyond, the PPWG will continue to support the PaCSON community to deliver against their missions of working together across the Pacific and to cooperatively and collaboratively develop collective cyber security incident response capabilities; enhance technical skills and knowledge; share cyber security threat information; and reflect best practice in order to strengthen our cyber security defences. Support from PaCSON partners to help realise these goals is highly valued, and is an effective mechanism for success.

2024 Outcomes

Progress reporting

At the governance session of the 2024 AGM, the PaCSON community committed to measuring and tracking progress against community priorities. A list of the 2023–24 priorities is outlined below, along with the status of each priority and actions taken to achieve these in the reporting period.

2023–24 priorities

1. General

- Formalise PaCSON's status as a regional body, such as by forming an official relationship with the PIF, and seeking member buy-in.
- Restructure Working Groups by clearly defining roles and responsibilities and encouraging the appointment of co-chairs.
- Grow Working Groups by making them more focused on outcomes and achieving this by developing working plans.
- Review the topics and scope of the Working Groups.
- Align AGMs with other relevant conferences and workshops.

2. Capacity building

- Increase hands-on training opportunities at future AGMs.
- Commit to working with partners and other players in the region to deconflict training offerings.

3. Communications

Increase traffic to, and use of, the portal by:

- setting up automatic notifications about new forum posts to a WhatsApp or Signal group in order to leverage platforms that members are already using, and allow them to click the link on their mobile
- using community-wide emails to notify of forum updates
- encouraging members, partners and friends to post updates in the forum to centralise communications
- creating a downloadable template for forum posts.

Progress against 2023–24 priorities

PaCSON continues to progress action items to do with the 2023–24 priorities as follows.

Table 1: Progress against the 2023–24 PaCSON priorities

Priority	Status	Actions
1. General	On track, ongoing	**Formalise PaCSON's status as a regional body, such as by forming an official relationship with the PIF, and seeking member buy-in.** ▪ PIF Secretariat consulted with the EC about the final draft of the Pacific Partnerships for Prosperity and asked the Chair to officially sign the final document. **Restructure Working Groups by clearly defining roles and responsibilities and encouraging the appointment of co-chairs.** ▪ Co-convenors were appointed to Working Groups. ▪ Break-out sessions at the AGM allowed Working Groups to discuss work plans and the remit of Working Groups. **Grow Working Groups by making them more focused on outcomes and achieving this by developing working plans.** ▪ The Working Group member lists and contact details were updated. ▪ The Working Group frameworks and responsibilities were recirculated. **Review the topics and scope of the working groups.** ▪ Working Group convenors were invited to attend every other Executive Committee call. **Align AGMs with other relevant conferences and workshops.** ▪ The 2024 AGM was aligned with the P4C intersessional to reduce travel and time out of the office for participants.

Priority	Status	Actions
2. Capacity building	Achieved	**Increase hands-on training opportunities at future AGMs** ▪ The Capture the Flag event ran again at the AGM with a high level of participation. ▪ At the request of members, there was a new session on how to deliver your own Capture the Flag. ▪ Commit to working with partners and other players in the region to de-conflict training offerings ▪ The PaCSON Secretariat coordinate cyber training opportunities with KrCERT.
3. Communications	Achieved	**Increase traffic to, and use of, the portal** ▪ A Signal group was established to share alerts, advisories and other posts made on the PaCSON portal. ▪ The Signal group was expanded from a website updates-only chat, to a general PaCSON communications channel to increase ease of communication. ▪ The Secretariat and community shared alerts and advisories to the Signal group to allow members to click the link on their mobile. ▪ The Secretariat used community-wide emails to notify members of alerts and advisories on the portal. ▪ The CWG convenors encouraged members, partners and friends to post updates in the portal to centralise communications. Some examples of these include updates from SamCERT, CCCS and ANSSI. ▪ CWG convenors created and shared a how-to guide for making portal posts.

Financial Reporting

Financial Reporting

As outlined in the 2024–25 priorities, PaCSON members and the EC wished to make public the financial commitments made by members, partners, friends, the Secretariat and other relevant stakeholders. The intention behind this action is to increase the transparency of the network and enable members to understand the commitments made by those who are invested in the network.

The following is a list of stakeholders and their financial contributions to PaCSON for the calendar year of 2024. Please note, some stakeholders were unable to publish their financial commitments due to internal organisational constraints.

Table 2: 2023–24 Cost commitments of major events (in chronological order)

Activity/event	Paid for by	Cost	Notes
FIRST Conference 2024 Fellowship	PaCSON Secretariat	$44,724.00	Support 4x PaCSON members to attend FIRST Conference in Fukuoka, Japan
Additional Solomon Islands attendance at FIRST 2024	Australia-Solomon Islands Partnership in Governance (ASIP-Gov), a DFAT initiative	$11,808.49	1 x attendee from Solomon Islands to attend the FIRST Conference in Fukuoka Japan
PaCSON 2024 AGM	PaCSON Secretariat	$135,717.88	Delivery and facilitation of PaCSON 2024 AGM in Rarotonga, Cook Islands
PaCSON 2024 AGM official dinner	Cook Islands	$8,197.00	Cook Islands hosted dinner as Chair at PaCSON AGM
PaCSON 2024 AGM- ACL site visit	Cook Islands	$1,108.00	Cook Islands facilitated visit to the ACL site

Activity/event	Paid for by	Cost	Notes
PaCSON 2024 AGM and P4C	DFAT	$58,485.18	Support for PaCSON members to attend PaCSON AGM and P4C events
KR CERT APISC Training	Korea’s Internet and Security Agency (KISA) and KR CERT/CC	$12,682.00	3x PaCSON members funded by KISA/KrCERT/CC to attend APISC training in South Korea
Merchandise shipments	PaCSON Secretariat	$444.90	Shipment of PaCSON merchandise
Account subscriptions	PaCSON Secretariat	$1,051.90	Communications and feedback services
PaCSON website management (Jan-June 2024)	PaCSON Secretariat	$130,000	Content updates, enhancements and security updates to pacson.org
PaCSON website management (July-Dec 2024)	PaCSON Secretariat	$25,200	Content updates, enhancements and security updates to pacson.org
PaCSON CUP	PaCSON Secretariat	$65,670	Final payment for PaCSON CUP

Acknowledgements

Acknowledgements

PaCSON acknowledges the valuable contributions made by all of our partners. The PaCSON community is very grateful for the advice, contributions and support of all the government organisations, not-for-profit organisations, private enterprises and academic bodies who work with our network.

This report and the activities of PaCSON are made possible thanks to the support and advice of many individuals and organisations. The EC, on behalf of the entire PaCSON community, would like to thank everyone who contributed to PaCSON in 2024, with special thanks to:

ASIA PACIFIC NETWORK INFORMATION CENTRE

APNIC is an open, member-based, not-for-profit organisation, whose primary role is to distribute and manage internet number resources (IP addresses and AS numbers) in the Asia Pacific region's 56 economies. These number resources are the building blocks needed for the internet to operate and grow. As part of this service, APNIC is responsible for maintaining the public APNIC Who Is Database, and managing reverse DNS zone delegations.

APNIC also provides forums for internet policy development that are bottom-up and open to everyone.

Furthermore, APNIC helps build essential technical skills across the region, supports internet infrastructure development, produces insightful research and is an active participant in the multi-stakeholder model of internet cooperation and governance.

APNIC performs these activities as part of its commitment to a global, open, stable and secure internet that serves the entire Asia Pacific region.

To learn more, please visit **https://www.apnic.net/**

ASIA PACIFIC COMPUTER EMERGENCY RESPONSE TEAM

APCERT cooperates with CERTs and CSIRTs to ensure internet security in the Asia Pacific region that is based around genuine information sharing, trust and cooperation.

APCERT works to help create a safe, clean and reliable cyber space in the Asia Pacific region through global collaboration.

To learn more, please visit **https://www.apcert.org/**

CYBER SAFETY PASIFIKA

CSP is a program led by the AFP and is aimed at increasing cyber safety awareness and education of vulnerable communities in the Pacific region. It is also aimed at upskilling Pacific police officers in cybercrime investigations.

To learn more, please visit Cyber Safety Pasifika **https://www.cybersafetypasifika.org/**

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE

DFAT leads Australia's international engagement on cyber and critical technology across the Australian Government. This work is coordinated by Australia's Ambassador for Cyber Affairs and Critical Technology.

PaCSON acknowledges the support and funding provided by DFAT.

To learn more, please visit **https://www.dfat.gov.au/international-relations/themes/cyber-affairs-and-critical-technology**

GLOBAL CENTRE FOR CYBER EXPERTISE PACIFIC HUB

The GFCE Pacific Hub endeavours to enhance cyber security capacity and capabilities within the Pacific region by facilitating and coordinating initiatives for cyber capacity building. The aim is to ensure that such initiatives are effective, purpose-driven, and sustainable by promoting the sharing of knowledge and expertise, and fostering coordination among diverse stakeholders, including donors, governments, private sector organisations and civil society groups.

To learn more, please visit **https://thegfce.org/**

PACIFIC ISLANDS LAW OFFICERS NETWORK

PILON is a network of senior law officers from 19 Pacific Island Countries, including Australia and New Zealand. PILON contributes to a safe and secure Pacific by addressing key law and justice issues across its 3 strategic priorities: corruption, cybercrime and sexual and gender-based violence. Through regional collaboration, knowledge-sharing and capacity building, PILON works to strengthen justice systems and uphold the rule of law across the Pacific. The PILON Annual Meeting provides an opportunity for members review progress across all work streams, share best practice and plan future initiatives.

To learn more, please visit **https://pilonsec.org/**

Abbreviations

Abbreviations

ACSC	Australian Cyber Security Centre
AGM	Annual General Meeting
ANSSI	Agence nationale de la sécurité des systèmes d'information
APAC	Asia Pacific (FIRST Incident Response team)
APCERT	Asia Pacific Computer Emergency Response Team
APNIC	Asia Pacific Network Information Centre
APSIC	Asia Pacific Society of Infection Control
ARWG	Awareness Raising Working Group
ASD	Australian Signals Directorate
BEC	business email compromise
CBWG	Capacity Building Working Group
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CERT NZ	Computer Emergency Response Team New Zealand
CERTVU	Computer Emergency Response Team Vanuatu
CHOGM	Commonwealth Heads of Government Meeting
CISA	Cyber Security Infrastructure & Security Agency (US)
CROP	Council of Regional Organisations of the Pacific

CSA	Cyber Security Advisories
CSAT	Cyber Security Awareness Team
CSD	Cyber Security Division (CISA, USA)
CSIB	Cyber Security and Intelligence Bureau
CSIRT	Computer Security Incident Response Team
CSP	Cyber Safety Pasifika
CTI	Cyber threat intelligence
CUP	Cyber Upskill Program
CWDP	Cyber Security Workforce Development Program (Tonga)
CWG	Communications Working Group
DDoS	distributed denial-of-service
DFAT	Department of Foreign Affairs and Trade (Aust)
DGTO	Digital Government Transformation Office (Fiji)
DHS	Department of Homeland Security (US)
DICT	Department of Information and Communications Technology (Papua New Guinea)
DIJOP	Olympic and Paralympic Delegation (France)
DNS	Domain Name System
DOJ	Department of Justice (US)
DTA	Digital Transformation Authority (the Solomon Islands)

DTO	Digital Transformation Office (Kiribati)
EC	Executive Committee (PaCSON)
ECD	Emergency Communications Division (CISA, US)
ECIA	Economics, Consumer and International Affairs (PNG)
EMC	East Micronesia Cable
ERPD	Engineering & Resource Planning Department (PNG)
FBI	Federal Bureau of Investigation (US)
FICAC	Fiji Independent Commission Against Corruption
FIRST	Forum of Incident Response and Security Teams
FIU	Fiji Financial Intelligence Unit
FSM	Federated States of Micronesia
GBV	gender-based violence
GCSB	Government Communications Security Bureau (New Zealand)
GFCE	Global Forum on Cyber Expertise
ICT	information and communications technology
IPAM	Institution of Public Administration and Management (the Solomon Islands)
IR	incidence response
IRC	Internal Revenue Commission (PNG)
IRFS	International Revenue Fraud Services

ISD	Infrastructure Security Division (CISA, US)
IT	information technology
ITCS	Department of Information Technology and Computing Services (Fiji)
JCDC	Joint Cyber Defence Collaborative (CISA, US)
KDGP	Kiribati Digital Government Project
LGBTIQ+	Lesbian, Gay, Bisexual, Transgender, Intersex, Queer Community
MBIE	Ministry of Business, Innovation and Employment
MCIT	Ministry of Communications and Information Technology (Samoa)
MEIDECC	Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (Tonga)
MFA	multi-factor authentication
MIC	Ministry of Internal Affairs and Communications (Japan)
MICT	Ministry of Information, Communications and Transport (Kiribati)
MIOM	Ministry of the Interior and of the Overseas (France)
MIPD	Marshall Islands Police Department
MiTM	man-in-the-middle
MoU	Memorandum of Understanding
MSP	managed service providers
NCF	National Critical Functions (CISA, USA)
PNG NCSC	National Cyber Security Centre, Papua New Guinea

NCSC NZ	National Cyber Security Centre, New Zealand
NGO	non-government organisation
NICTA	National Information and Communications Technology Authority
NPA	National Police Agency (Japan)
NRMC	National Risk Management Center (CISA, USA)
OCSC	Oceanic Cyber Security Centre
ODPP	Office of the Director of Public Prosecutions
OGCIO	Office of the Government Chief Information Officer (Vanuatu)
OPM	Office of the Prime Minister (the Cook Islands)
OSC	Online Safety Commission (Fiji)
OT	operational technology
PaCSON	Pacific Cyber Security Operational Network
PILON	Pacific Islands Law Officer's Network
PMO	Prime Minister's Office (Tonga)
PMU	Project Management Unit
PNG	Papua New Guinea
PNGCERT	Papua New Guinea Computer Emergency Response Team
PPWG	PaCSON Partners Working Group
RBF	Reserve Bank of Fiji
SamCERT	Samoa Computer Emergency Response Team

SED	Stakeholder Engagement Division (CISA, US)
SGDSN	General Secretariat for Defence and National Security
SIG	Solomon Islands Government
SIG ICTS	Solomon Islands Government (SIG) Information Communication Technology Services (ICTS)
SIG SOC	Solomon Islands Government Security Operations Centre
SMMD	Social Media Management Desk (PNG)
SOG	Secretary of Government (Niue)
SOHO	small-office/home
UAS	Universal Access Scheme Secretariat (PNG)
UNODC	United Nations Office on Drugs and Crime

PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

Disclaimer

The contents of the membership, partnerships and friend updates are written by each PaCSON member, partner or friend based on their individual analysis and experience. Responsibility for the information and views expressed in each update lies entirely with the member, partner or friend.

PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

pacson.org