



PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

ANNUAL REPORT 2025





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 shared 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



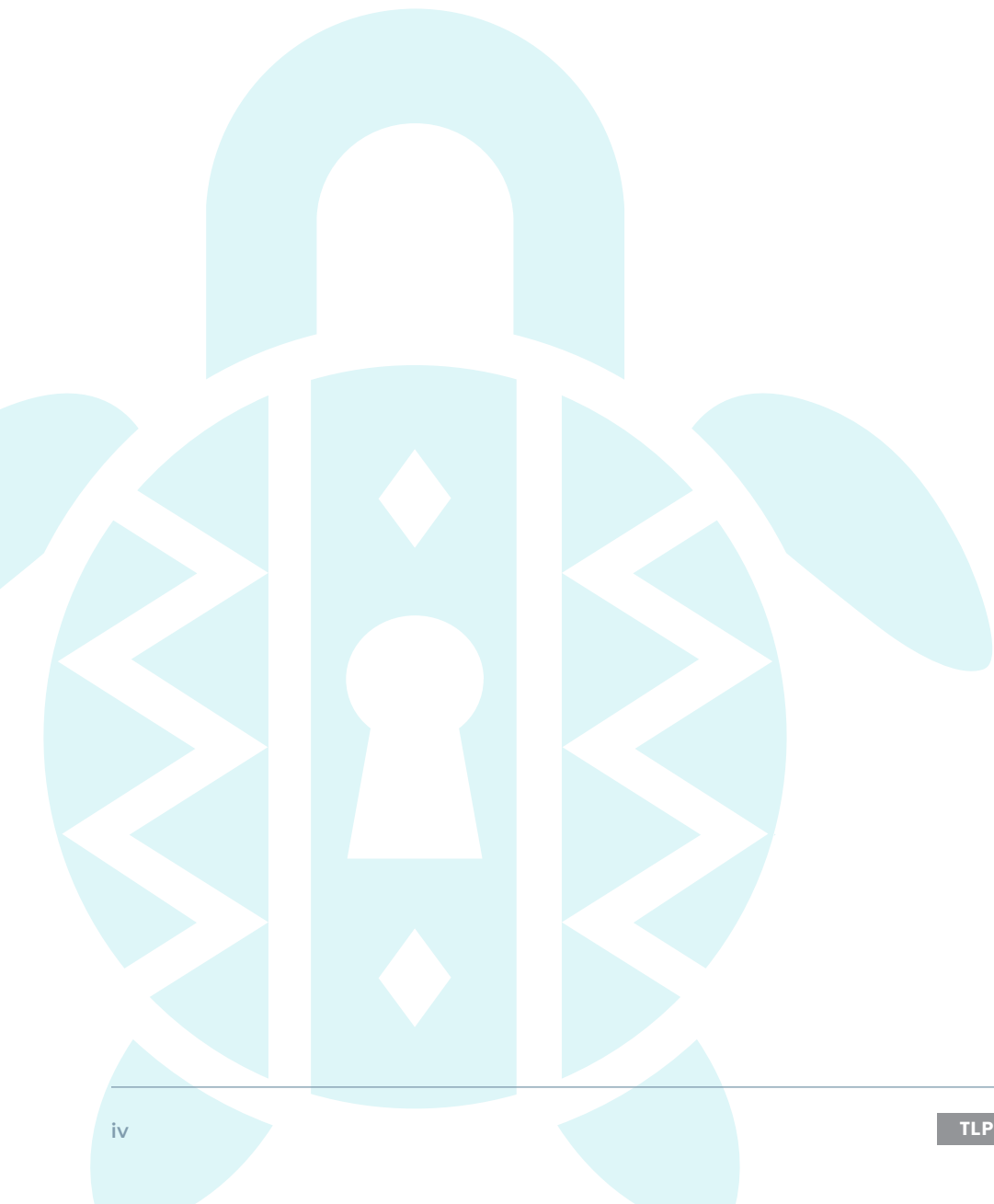
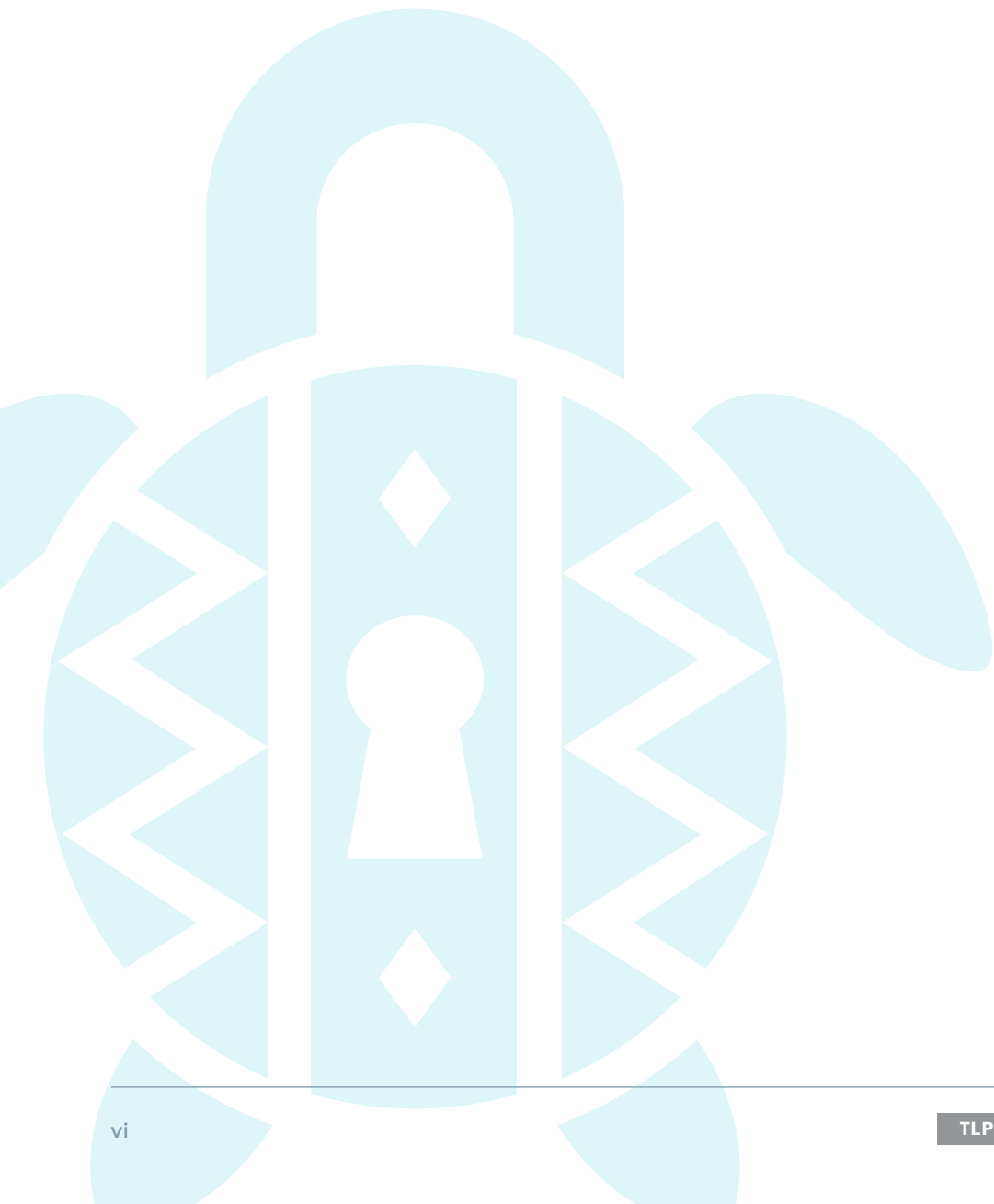


TABLE OF CONTENTS

From the Chair	1
PaCSO ^N 2025 Annual General Meeting	7
Member Updates	11
Australia	12
Cook Islands	18
Federated States of Micronesia	20
Fiji	22
Kiribati	34
Nauru	38
New Zealand	42
Palau	48
Papua New Guinea	50
Samoa	61
Solomon Islands	69
Tokelau	76
Tonga	79
Tuvalu	96
Vanuatu	98
Partner Updates	105
Friends Updates	115
Working Group Updates	123
Progress Reporting	131
2025 Financial Statement	135
Acknowledgements	137
Abbreviations	141





From the Chair



Chair remarks

A unified vision for a resilient Blue Continent

Mauri and warm Pacific greetings,

It has been a profound honour for Kiribati to serve as the Chair of the Pacific Cyber Security Operational Network (PaCSO^N) for the 2024–25 term. As we reflect on the achievements this last term, we are reminded that our strength lies not in isolation, but in the enduring spirit of regional solidarity, cooperation, and collective responsibility that continues to define our Pacific family.

The term marked a period of strategic maturity for PaCSO^N. Our efforts remain firmly anchored in the 2050 Strategy for the Blue Pacific Continent, particularly under the ‘Technology and Connectivity’ theme. For our Pacific small island developing states, cyber security is not merely a technical issue; it is intrinsically linked to sovereignty, economic resilience, social stability, and protecting our people and cultures in an increasingly digital world. The PaCSO^N mission embodies this commitment by strengthening our cyber security defences through coordinated regional cooperation across the Pacific.

Building resilience through connection

A defining highlight of this year was the 2025 PaCSO^N Annual General Meeting (AGM), held on the beautiful Kiritimati Island. Hosting our community in one of the most remote parts of our region was both a deeply humbling opportunity, which underscores the very essence of the United Nations Development Programme (UNDP) Small Island Digital States manifesto that focuses on efforts that ensure that no island, no matter how distant, is left vulnerable in the digital age. The discussions held in Kiritimati moved beyond policy, focusing on the operational realities of protecting critical infrastructure and the information it holds against an evolving landscape of ransomware and phishing threats.

2025 key achievements

Throughout the year, our PaCSO^N working groups have turned the aspirations of the Lagatoi Declaration into tangible action. Publishing the PaCSO^N Capacity Building Action Plan 2025–28 was a significant milestone for the period. This action plan signals the focus areas for partners who want to build capacity in the Pacific – the actions are the initiatives members want to see implemented.

- **Capacity-building:** We have successfully expanded our remote learning initiatives: the increased support of member-to-member training has been a stand-out effort for 2025. This effort is ensuring that our local technical experts have the tools needed to defend their networks in real time.

- **Awareness-raising:** The refreshed Cyber Smart Pacific Campaign has reached deep into our communities, using familiar Pacific motifs to simplify complex security concepts for all citizens. This more targeted campaign gave some of our most pervasive digital consumers training and awareness materials, which demonstrates how working together using one uniting campaign can have big impacts in protecting us all against cyber security threats.
- **Regional representation:** Undertaking efforts to enhance and promote our status within the regional architecture, PaCSO has strengthened its voice in global forums, ensuring the unique challenges of Pacific small island states are heard and addressed. This activity is a priority that we look forward to continuing to support into future years.
- **Women in cyber security:** A step in recognising the influence of women and diverse identities, the newly established PaCSO Women in Cybersecurity Working Group (PWCS) was endorsed at the PaCSO 2025 AGM. This new working group has many exciting plans, and we look forward to supporting it to support the role and impact of women in cyber security for PaCSO and our region.

Gratitude to our members, partners, and friends

Our progress would not be possible without the unwavering dedication of all our participants. I wish to extend my deepest gratitude to our members, partners and friends, and to the PaCSO Secretariat for its tireless support that remains the bedrock of our network. To our international partners, your expertise and resource mobilisation have been vital in bridging the digital divide. We thank you all.

Looking forward

As we look towards 2026, the cyber security landscape will continue to evolve alongside emerging technologies, geopolitical cyber tensions, and increasingly sophisticated cyber threats. However, the 2025 AGM demonstrated that, when we speak with 'One Voice', we are a resilient force. We remain committed to the vision of a 'Smart Pacific', where technology serves as a catalyst for prosperity while remaining safe, secure, and inclusive for every Pacific Islander.

To our incoming leadership and the entire community, let us continue to move forward with the same solidarity and cooperation that has brought us this far. Together, we are not just navigating the digital frontier; we are securing a prosperous future for the generations to follow.

Kam rabwa and thank you.

Kiribati

Chair, PaCSO Executive Committee



Program overview

Established in 2017, PaCSO^N was created to foster regional cooperation and collaboration, and to protect the Pacific's respective information infrastructures and constituents. The availability of internet connectivity presents significant opportunities, but also exposes users within the Pacific to increased threats from malicious cyber actors.

PaCSO^N is an operational cyber security network of regional working-level cyber security experts in the Pacific. PaCSO^N coordinates activities which 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 oversight.

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

In support of PaCSO^N, our partners – including other government organisations, not-for-profit organisations (NGOs) and academia – are able to join the network. Partner organisations to PaCSO^N currently include:

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

In support of PaCSO^N, our friends – including other government organisations, NGOs and academia – are able to join the network. Friend organisations to PaCSO^N include:

- Cyber Safety Pasifika (CSP), Pacific Islands Policing Community
- Global Forum on Cyber Expertise (GFCE), international
- Pacific Fusion Centre (PFC), Pacific islands
- the eSafety Commissioner, Australia.

PaCSON is not a Computer Emergency Response Team (CERT) nor a Computer Security Incident Response Team (CSIRT) and does not provide an incident response capability. The program 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 managing and directing PaCSON. All PaCSON members are eligible to nominate for any of the committee positions.

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

Chair	Kiribati
Deputy Chair	Samoa
Incoming Chair	Papua New Guinea

In 2025–26, the structure of the PaCSON EC is:

Chair	Papua New Guinea
Deputy Chair	Tonga
Incoming Chair	Naura

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

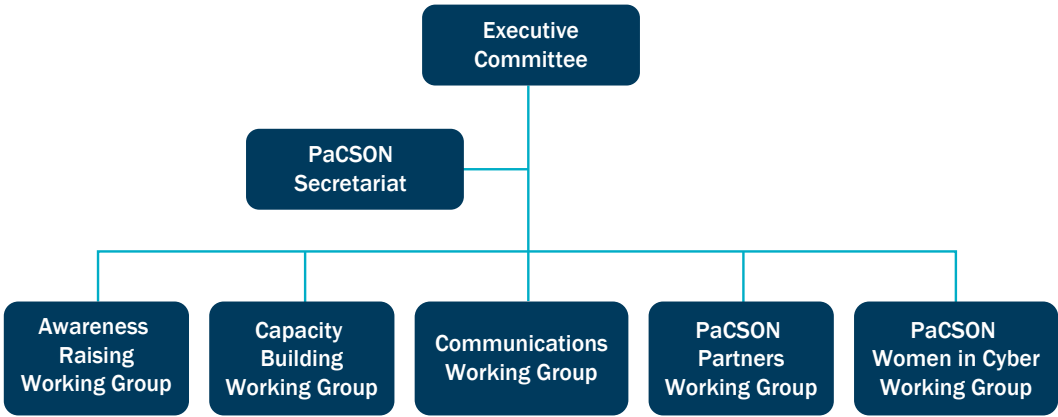


Figure 1: PaCSO governance structure

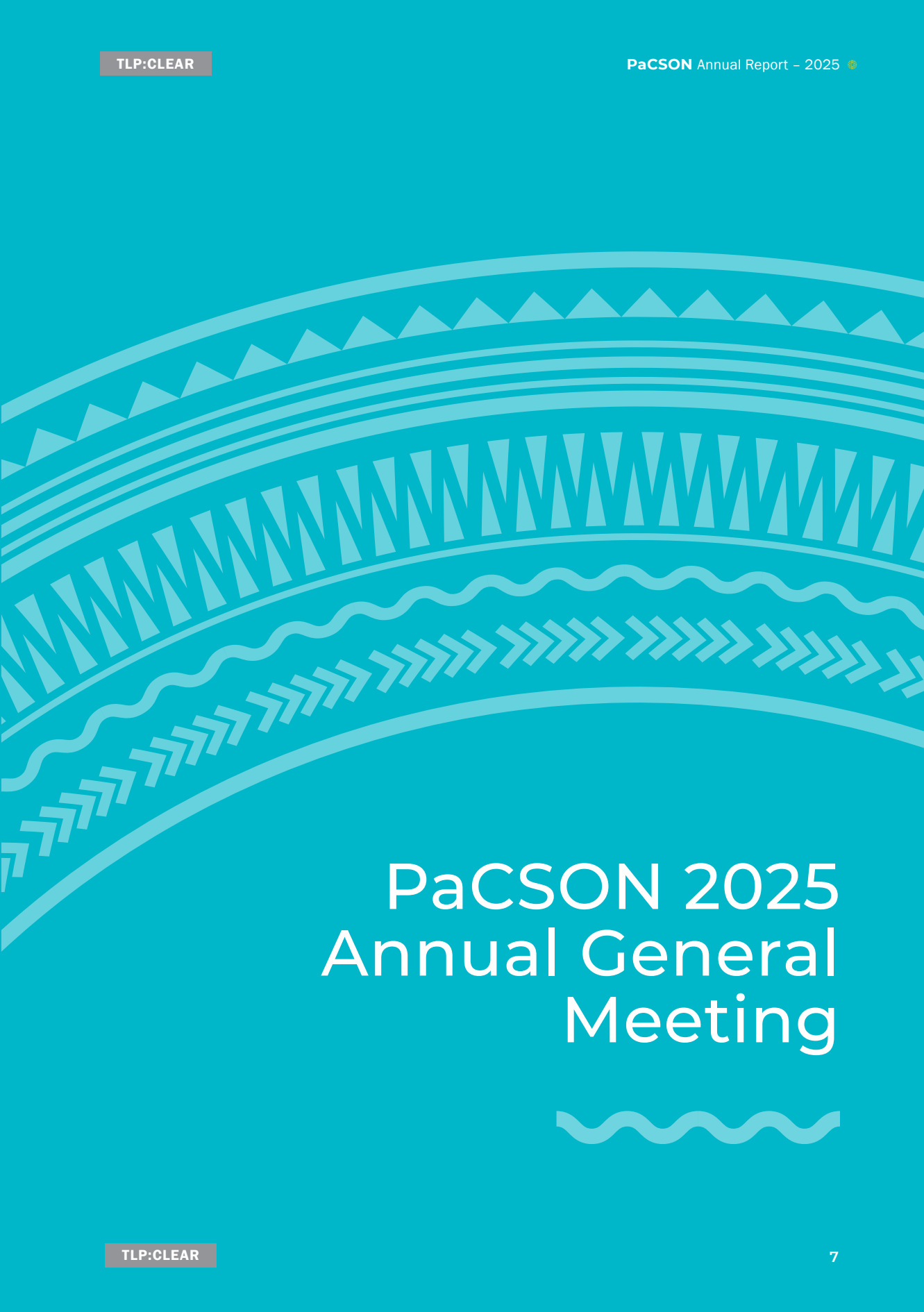
Vision

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



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..



PaCSON 2025 Annual General Meeting



PaCSO^N 2025 Annual General Meeting

Overview

The 2025 PaCSO^N Annual General Meeting (AGM) took place from 16 to 21 October on Kiritimati Island, Kiribati. This year's AGM stretched over the weekend, providing members with opportunities to connect in person through sessions that strengthened members' collective expertise in cyber security, information sharing, networking, and capacity-building. Beyond the formal program, the AGM also offered attendees the chance to catch up with familiar faces in person and experience the untouched beauty of Kiritimati Island.

The AGM program was as follows:

- **Day 1 (16 October):** Opening Ceremony and annual cyber challenge
- **Day 2 (17 October):** Members-only day with AGM governance proceedings, working group meetings and TLP:RED Cyber Security Information Exchange
- **Day 3 (20 October):** Community workshops and presentations
- **Day 4 (21 October):** Site visit to the Southern Cross NEXT cable landing site.



Figure 2: Images from PaCSO^N 2025 AGM

Executive Committee election

The AGM serves as a handover between the outgoing and incoming PaCSO Executive Committee. The announcement of the new committee came following an open nomination period prior to the AGM.

In 2025–26, the structure of the PaCSO Executive Committee will be:

Chair	Papua New Guinea
Deputy Chair	Tonga
Incoming Chair	Nauru

As the Chair for 2024–25, the Ministry of Information, Communications and Transport’s (MICT), Kiribati, served as the host of the AGM. During the closing session, Kiribati farewelled its position and graciously handed over the role to Papua New Guinea, who will serve as Chair for 2025–26.

Throughout its term serving on the EC, Kiribati played a leading role in the community’s collective efforts to share information and strengthen relationships, as well as guiding decision-making for the PaCSO community.



Figure 3: Images from PaCSO 2025 AGM

Future plans

2025–26 priorities

Below are the 2025–26 priorities for PaCSO^N. Progress against these will be reported on in the 2026 annual report. These priorities were decided on at the 2025 AGM, and were published in the wrap-up report.

1. Strengthen PaCSO^N's position within the regional architecture and global cyber forums through formal coordination and regional alignment.

Building upon last year's priority of solidifying PaCSO^N's presence in the regional architecture, as well as increasing efforts to promote visibility of PaCSO^N at global cyber forums, PaCSO^N will:

- advocate for the alignment of the 2026 PaCSO^N AGM alongside other regional cyber events
- encourage members to utilise interventions within regional forums to attract the attention of senior leaders and ICT ministers in the region
- continue to advocate for the Pacific at key global forums to advance PaCSO^N objectives and provide opportunities for PaCSO^N members to share Pacific issues and solutions from the region.

2. Further develop a PaCSO^N monitoring and evaluation framework.

Building upon last year's priority of establishing a monitoring and evaluation framework, expanding the evaluation function to measure progress, identifying challenges, and sharing outcomes across the network, PaCSO^N will:

- understand the priorities and work programs of all elements of the PaCSO^N program, including working groups, partner engagement, and fellowship opportunities
- assess PaCSO^N functions and provide recommendations for Executive Committee consideration.

3. Strengthen and streamline capacity-building efforts in the region.

Leveraging the Capacity Building Action Plan, facilitate and deconflict capacity-building efforts in the region to work towards a more capable and self-sufficient Pacific cyber environment, PaCSO^N will:

- promote the Capacity Building Action Plan with regional partners encourage partners and friends to take a more active role and highlight the value their expertise brings to PaCSO^N.

4. Promote a safe and secure environment to enable members to share information and increase confidence to ask for assistance.

Prioritising an increase in members sharing information through existing or new methods of communication, PaCSO^N will:

- enable an increase in the number of member-produced advisories, alerts and updates
- encourage initiatives that assist with the growth of information-sharing within the PaCSO^N community.



Member Updates



Australia



The Australian Cyber Security Centre (ACSC)

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

- providing the Australian Cyber Security Hotline, which can be called 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 (CTIS) platform
- 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 133,000 Australian organisations and individuals on cyber security issues through ASD's Cyber Security Partnership Program.

ASD is a statutory agency within the Defence portfolio, which reports directly to the Minister for Defence. ASD brings together capabilities from partner agencies and works closely with partners across government organisations, including the Department of Home Affairs, Australian Federal Police (AFP), Department of Foreign Affairs and Trade (DFAT), and industry.

ASD encourages every organisation and individual who observes suspicious cyber activity, incidents and vulnerabilities to report them at cyber.gov.au, and to the Australian Cyber Security Hotline 1300 CYBER1 (1300 292 371). ASD provides free technical incident response advice and assistance, 24 hours a day, 7 days a week.

ASD encourages every organisation and individual who observes suspicious cyber activity, incidents and vulnerabilities to report at cyber.gov.au, and to the Australian Cyber Security Hotline 1300 CYBER1 (1300 292 371). ASD provides free technical incident response advice and assistance, 24 hours a day, 7 days a week.

Threat landscape

In the FY2024–25 (financial year), where July 2024 to June 2025 is ASD's statutory reporting period), the top 3 self-reported cybercrime types for Australian individuals were:

- identity fraud (30%)
- online shopping fraud (13%)
- online banking fraud (10%).

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

- email compromise resulting in no financial loss (19%)
- business email compromise (BEC) resulting in financial loss (15%)
- identity fraud (11%).

The 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 categorised on severity of impact and significance of the organisation to Australia.

Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C1	C1
Extensive compromise	C6	7	10	7	2	C1
Isolated compromise	C6	52	79	51	28	C2
Coordinated low-level malicious attack	C6	1	2	2	3	1
Low-level malicious attack	C6	1	128	65	109	94
Unsuccessful low-level malicious attack	C6	33	12	183	334	40
	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 4: Cyber security incidents by severity category for FY2024-25 (total 1,253)

Overall, there was an 11% increase in incidents reported to the ACSC in FY2024–25. Compared to FY2023–24, there was a notable increase in both successful and unsuccessful low-level malicious attacks.

In FY2024–25, the ACSC received over 42,500 calls to the Australian Cyber Security Hotline, a 16% increase on the previous year. On average, the ACSC received 116 calls per day, an increase from 100 calls per day in the previous year. The ACSC also responded to over 1,200 cyber security incidents, an 11% increase on the previous year.

Critical infrastructure is, and will continue to be, an attractive target for state-sponsored cyber actors, cybercriminals, and hacktivists, primarily due to large holdings of sensitive data and the critical services that they provide to Australia’s economy. Incidents against critical infrastructure made up 13% of all incidents for the reporting period.

The ACSC responded to over 1,200 cyber security incidents, an 11% increase on the previous reporting period. A breakdown by month is below.

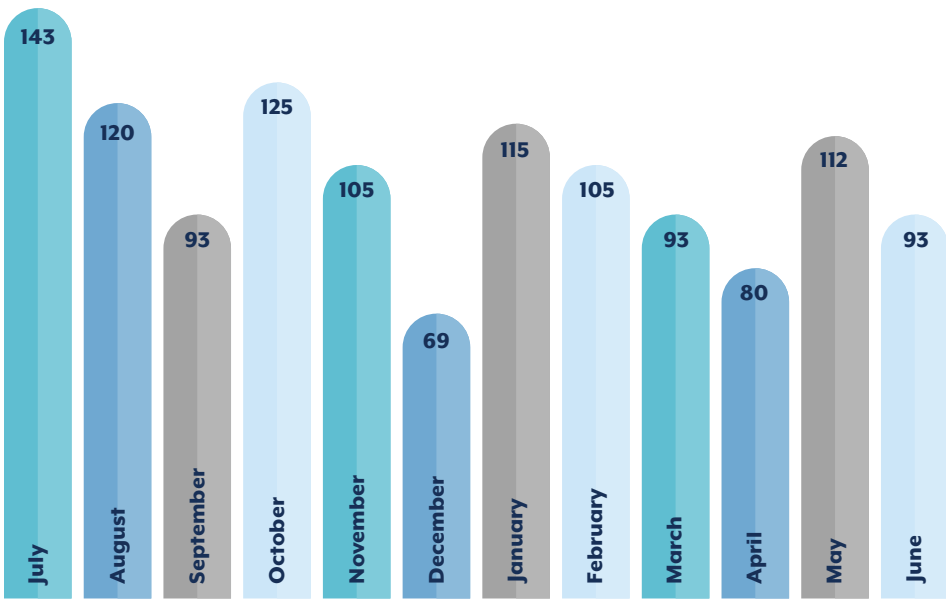


Figure 5: Cyber security incidents responded to by month

Awareness-raising

The ACSC also 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 achieved the following in FY2024–25:

- made 1,700 notifications of potential malicious cyber activity
- Australian Protective Domain Name System blocked customer access to 334 million malicious domains, up 307%
- Cyber Threat Intelligence Sharing partners grew by 13% to over 450 partners
 - shared over 2,984,000 indicators of compromise (IOCs).
- Cyber Hygiene Improvement Program:
 - performed 478 high-priority operational tasks, up 31%
 - distributed around 14,400 reports to approximately 3,900 organisations, up 125% and 95% respectively
 - distributed around 11,000 notifications of IOCs to approximately 2,160 organisations.
- Cyber Uplift Remediation Program:
 - 26 active engagements
 - 4 engagements commenced.
- Cyber Maturity Measurement Program:
 - 7 active engagements.
- Critical Infrastructure Uplift Program:
 - 8 uplifts completed, covering 38 CI assets
 - 4 uplifts in progress, covering 5 CI assets
 - 7 tech-to-tech workshops held.
- notified critical infrastructure organisations, over 190 times, of potential malicious cyber activity, an increase of 111%
- grew ASD's Cyber Security Partnership Program to around 133,000 partners
- led 17 cyber security exercises, involving over 120 organisations, to strengthen Australia's cyber resilience
- briefed board members and company directors covering 41% of the ASX 100 (Australian Stock Exchange).

In FY2024–25, the ACSC:

- published or updated 26 PROTECT publications, updated the Information Security Manual every 3 months, and updated the Essential Eight Maturity Model
- published 20 joint advisories and publications, with international partners, to cyber.gov.au
- published 108 alerts, advisories, incident and insight reports on cyber.gov.au and the Partnership Portal.

Achievements

ACSC hosted the 2025 APCERT AGM and Conference from 25 to 27 November. The theme ‘Cyber Horizons: Strengthening Regional Resilience – Together’ reflected our shared commitment to collaboration in an evolving cyber threat landscape.

The event brought together 21 CERTs and CSIRTs from 18 of APCERT’s 24 economies, 3 APCERT partners, plus industry representatives and Australian government agency officials. Over 3 days, participants engaged in strategic discussions, technical presentations, and team-building activities designed to strengthen operational trust and resilience across the region.

On 30 May 2025, the Australian Government introduced a mandatory ransomware reporting regime for businesses with annual turnovers of \$3 million or more and for entities responsible for CI. This regime aims to enhance the Government’s visibility of ransomware and cyber extortion threats, enable tailored advice to industry, inform policy and legislation, and improve operational responses to disrupt ransomware activity across Australia.



Figure 6: Images from APCERT 2025 AGM and Conference, 25 to 27 November 2025

The ransomware payment reporting obligation established under the Cyber Security Act 2024 enhances Australia's visibility of ransomware and cyber extortion activity by requiring entities above the reporting threshold to notify the Australian Government of any ransom payments made. Throughout 2025, stakeholders were engaged through Town Hall sessions, published detailed guidance materials, and an industry survey to assess sector understanding and the usability of the reporting form.

Case study: ZServers

On 12 February 2025, the Australian Government imposed sanctions, under the Autonomous Sanctions Regulations 2011, on a cyber infrastructure entity – ZServers – and 5 of its Russian employees. The individuals are ZServers' owner, Aleksandr Bolshakov, and employees Aleksandr Mishin, Ilya Sidorov, Dmitriy Bolshakov and Igor Odintsov. The sanctions were in response to ZServers' role in providing bulletproof hosting services to host and disseminate data stolen from compromises of Australian and other organisations in 2022. Australia's cyber sanctions against this entity are strengthened by a trilateral sanctions approach, which includes the US and UK imposing the same sanctions. This approach demonstrates our collective resolve to combat cybercrime.

These latest sanctions make it a criminal offence to provide assets to ZServers or the 5 sanctioned individuals, or to use or deal with their assets, with penalties of up to 10 years' imprisonment and/or heavy fines. These sanctions also ban the individuals from entering Australia. Cyber sanctions impose cost and consequence on the ability of cybercriminals to operate.

These sanctions follow on from Australia's first ever cyber sanctions, which were issued against Aleksandr Gennadievich Ermakov in January 2024 for his role in the Medibank Private data breach.

Malicious cyber actors continue to target Australian government agencies, critical infrastructure, businesses and individuals. This threat will continue to be met by the collaborative sanctions work of the whole government and the AFP, the ACSC, and DFAT in particular. Cyber sanctions are a key tool in disrupting and deterring malicious cyber actors and protect Australians from this threat.

Cook Islands



Information, and Communications Technology (ICT) Division

The organisational structure of ICT Division includes a small technical team, the Chief Data and Privacy Officer, and the Chief Digital Officer under the Director of ICT, with all functions reporting directly to the Chief of Staff in the Office of the Prime Minister (OPM).

Those wishing to report a cyber security incident can do so directly to the police, the Financial Intelligence Unit or to ICT Division via email or phone:

Email: pmoffice@cookislands.gov.ck

Phone: 29300

Threat landscape

For the Cook Islands, common cyber security threats include

- account and credential theft
- phishing attacks
- BEC.

To respond to the cyber threats we face, ICT Division works with the New Zealand National Cyber Security Centre (NCSC NZ) and Cyber CX to assess and respond to attacks accordingly.

For the reporting period, we observed an increase in cyber threats resulting in an increase in monitoring for them.

Awareness-raising

Within the civil service and also for the public, the launch of national initiatives for cyber security is a core component in our communications and public relations strategy. Security advisories and notifications on critical vulnerabilities are also disseminated to government ministries and agencies via email.

The OPM Facebook page is another means for disseminating alerts and advisories, but we do not make this approach a common practice.

The other way we raise awareness is that we have a program called 'Au vaine'. For this program, we send one of our female ICT staff out to our small islands to teach women and children about how to be safe online.

Our Office of the Public Service Commissioner (OPSC) has an orientation program for all new government employees and, in this program, ICT Division has been given 15 minutes to talk about ICT issues, cyber security and how to be safe online.

We did not publish any news, publications or advisory bulletins for the reporting period. Rather, all advice was shared via email with our direct stakeholders.

Continuing on efforts established in 2024, ICT Division is in the process of setting up the Cooks Islands Cyber Security Centre, which will host the functions of CERT and support offerings of cyber security training.

Achievements

In March 2025, a cyber safety presentation was provided by the Cook Islands Police to Year 9 and 10 students at Tereora College. It followed a case where a student became the victim of online blackmail. This presentation was an opportunity for students to better understand the impacts of cyberbullying and the online threats they may face.



Figure 7: presentation to school students - March 2025

<https://www.cookislandsnews.com/internal/national/local/crime/cyber-safety-presentation-empowers-online-blackmail-victim-to-speak-out/>

This year, 27 Cook Islanders have fallen victim to a recent Facebook scam using fake celebrity endorsements and Artificial Intelligence (AI), losing over NZD16,000 in total.

[**Cook Islanders targeted in \\$16,000 Facebook 'advanced fee' scam | RNZ News**](#)

Federated States of Micronesia



Cybersecurity and Intelligence Bureau (CSIB)

The CSIB resides within the Department of Justice and has the objective of establishing a practical and operational link to relevant national agencies dealing with cyber security, threats, and management.

This report provides an overview of CSIB's activities, achievements, and legislative engagement in FY2025, highlighting nationwide cyber security awareness initiatives and progress towards key legislation.

Awareness-raising

During FY2025¹, the CSIB continued to lead nationwide cyber security awareness programs across the Federated States of Micronesia, including:

- **Yap and Kosrae:** these outreach programs were conducted in the previous year, reaching schools and communities with targeted awareness sessions.
- **Pohnpei:** these awareness sessions are ongoing in local schools, engaging students and adults alike.
- **Chuuk:** the CSIB counterparts are actively delivering similar programs in collaboration with local stakeholders.

All educational materials provided by PaCSO have been highly effective and well received. The content is accessible, engaging, and has contributed significantly to increasing cyber security awareness throughout the communities visited.

¹ The financial year for the Federated States of Micronesia is October 1 to September 30.

Legislative engagement

As of the end of FY2025, several key legislative initiatives remain pending in Congress. These are the:

- Cybersecurity Bill
- Cybercrime Bill
- Personal Data Protection Bill
- Electronic Transactions Bill.

CSIB is confident these bills will be enacted into law. During FY2025, CSIB representatives conducted visits to all 4 states, alongside FSM Senators, to meet with state legislatures and gather feedback on the proposed legislation. While additional time and information were requested by the states, these consultations established a strong foundation for the bills' eventual passage in FY2026.

Achievements

FY2025 was a productive and impactful year for the CSIB. Nationwide, cyber security awareness initiatives successfully reached communities across all 4 states, effectively engaging both students and adults. Outreach efforts strengthened public understanding of cyber security risks and safe practices.

While key legislative measures are still pending, meaningful progress was made in building consensus with Congress and state legislatures, laying the groundwork for their future enactment. Overall, FY2025 reflects significant achievements in both public awareness and policy engagement, positioning the Federated States of Micronesia for continued advancement in cyber security in the coming year.

Fiji



Fiji Computer Emergency Response Team (Fiji CERT), Department of Information Technology and Communication (ITC) Services, and the Cyber Affairs Unit

Fiji's cyber security responsibilities fall under the Ministry of Policing and Communications² and comprises the close partnership and efforts of the Fiji CERT, ITC Services, and the Cyber Affairs Unit.

Fiji CERT is a national resource and was established in June 2025. Fiji CERT has 3 positions, being an incident responder, a communications officer and the Director Fiji CERT. Fiji CERT is actively recruiting staff members.

The Department of ITC Services has a Security Operations Centre (SOC) that, in 2025, consisted of 2 security administrators and the Manager of Compliance and Information Security. ITC Services is currently recruiting positions to enhance its operational capabilities, aiming to support up to 6 distinct roles within the team by the end of 2026

Together, Fiji CERT and ITC Services look after government networks and systems and, along with essential service operators, academia and the private sector, manage nationally significant cyber security incidents and provide advisory support for cyber security incidents.

The Cyber Affairs Unit is responsible for the cyber security policy arm within the ministry, and is tasked with creating national cyber security governance frameworks and controls. It is also responsible for implementing the National Cybersecurity and Resilience Strategy 2026–31, as well as providing oversight of cyber activities and initiatives within Fiji, ensuring alignment across critical sectors and a streamlined national approach.

The unit consists of 3 members, 2 cyber security analysts and the Manager of Cyber Affairs. The unit works closely with Fiji CERT, ITC Services, and other stakeholders to ensure that policy enables swift and practical cyber incident response.

² As at 3 November 2025, the Communications Portfolio moved from the Ministry of Trade, Micro, Small and Medium Enterprises, and Communications to the Ministry of Policing and Communications.

Threat landscape

Since 2025, there have been 3 reporting channels available for cyber security incidents:

- Anyone can directly email the Fiji CERT at its designated email address.
- Ministries report directly to ITC Services' SOC who can escalate to Fiji CERT when needed.
- For cybercrime, including scams, fraud, and threat to life matters, reports are made to the Fiji Police Force.

For online harm, such as cyber harassment or bullying, people can report to the Online Safety Commission (OSC) for support from the Fiji Police Force or help in removing the harmful content.

The 3 key cyber security threats are:

- financial fraud
- ransomware and unauthorised access
- phishing emails.

During the report period, Fiji has responded to:

- **Ransomware incidents:** Any ransomware attack that results in significant data encryption or operational disruption at a national level necessitates Fiji CERT's involvement. We assist in containment, response, recovery, and communication strategies.
- **Data breaches:** Incidents that also require immediate Fiji CERT action are those where unauthorised access leads to the compromise of sensitive or critical information.
- **Denial of service attacks:** Significant service disruption due to denial of service attacks (DoS) that impact critical services or operations will trigger Fiji CERT intervention to mitigate the attack and restore normal operations.
- **Phishing campaigns:** Large-scale phishing incidents that target multiple users or organisations, particularly when they lead to data compromise or credential theft, require Fiji CERT's coordination for assessment and response.
- **Malware infections:** Outbreaks of malware that affect multiple systems or networks, especially those causing significant operational impact, need Fiji CERT's expertise for containment and remediation efforts.
- **Insider threats:** Incidents involving potential insider threats, such as unauthorised data access or sabotage, require Fiji CERT's involvement to investigate and manage the situation effectively.
- **Critical vulnerability exploitation:** Exploitation of critical software vulnerabilities that pose a significant threat to organisational security requires Fiji CERT to assess the risk and assist in implementing mitigation measures.

ITC Services responds to all cyber security incidents that impact government ministries and departments whose networks are hosted by Department of ITC Services. We collaborate with those government entities whose networks are hosted outside the ITC ecosystem.

As Fiji CERT was only established in June 2025, it is not yet positioned to provide definitive insights into trends pertaining to fluctuations in reported cyber security incidents.

Nevertheless, it is noteworthy that Fiji CERT has made considerable progress in its nascent phase by actively receiving and analysing cyber security incident reports from both local organisations and international partners, many of whom have identified potential cyber security threats.

Throughout this phase, numerous organisations within Fiji have encountered various cyberattacks and have exhibited a commendable level of vigilance and responsibility by promptly reporting such incidents to Fiji CERT.

Awareness-raising

Educational workshops and training sessions

We have conducted workshops and training sessions targeting different audiences, including industry, civil society, government agencies, and the public. These sessions focus on best practices for online safety, recognising cyber threats, and responding to incidents.

Public awareness campaigns

Fiji CERT has conducted public awareness campaigns through community events. These campaigns aimed to inform individuals about common cyber threats, such as phishing attacks and ransomware, and provide practical tips for safeguarding personal and organisational data.

The ministry also leveraged and amplified the efforts of other agencies. In 2025, the Online Safety Commission launched the 'Think Before You Click' Campaign, emphasising that, in a digital world where a single click can either uplift or cause harm, users should consciously promote digital kindness and responsible online behaviour. This message was further amplified by the Fiji Police Force who, in collaboration with the Cyber Safety Pasifika program, conducted a nationwide roadshow to raise awareness of cyber safety and safe online practices across schools, community groups and civil society organisations.

Incident response support

By providing guidance on how to respond to cyber security incidents, Fiji CERT helped organisations understand the importance of preparedness and the need for proactive measures.

Celebrating days of awareness

Notable 'days of awareness' were celebrated across Fiji to raise community awareness of cyber threats and cyber hygiene. These days help to amplify community awareness. This included the Safer Internet Day, hosted by the Online Safety Commission, which is a global initiative promoting a safer and more responsible online world. On this day, people were asked to come together to

empower communities, educate young minds, and inspire positive digital habits. In October 2025, we held our second National Anti-Scam Awareness Week, highlighting the Fiji Government's strong commitment to protecting Fijians from the growing threat of online scams and cyber fraud.

Uplifting women and girls in the cyber domain

The Fijian Government expanded partnerships with civil society, including Women in Tech Fiji, which launched in 2025 and began delivering youth-focused and women-focused digital and cyber security initiatives. Then Deputy Prime Minister and Minister for Trade, Cooperatives, MSMEs and Communications, the Hon Manoa Kamikamica, launched the Fijian chapter of the initiative, underscoring the Fijian Government's dedication to closing the gender gap and empowering women to embrace technology.

The Girls in ICT Programme

The Girls in ICT (GICT) is a national capacity-building initiative implemented by the Ministry of Policing and Communications to address persistent gender disparities in ICT education, participation, and career progression. It aligns with the International Telecommunication Union (ITU) global GICT framework and supports national priorities on digital inclusion, skills development, and gender equity within Fiji's emerging digital economy.

In 2025, the programme was delivered across 3 secondary schools – Rampur College, Labasa College, and Rotuma High School – reaching 88 female students from Years 11 to 13. It comprised 4 interactive sessions focused on foundational ICT concepts, practical digital competencies, cyber security and online safety, and also connected ICT and STEM (Science, technology, engineering and mathematics) career pathways. Delivery followed a blended approach combining guided instruction, hands-on activities, group learning, and role-model engagement, supported by experienced ICT industry facilitators.

The ITC Services education outreach

ITC Services conducted phishing simulation exercises and delivered online awareness training through a dedicated platform, at least twice during the year, reinforcing cyber security awareness and strengthening user resilience against social engineering threats. In addition, during 2025, ITC Services organised targeted workshops with government IT officers, which was aimed at enhancing technical capacity, promoting best practices in cyber security, and fostering a more coordinated and proactive approach to protecting government digital infrastructure.

Publications

Fiji CERT produced a range of publications, and advisory bulletins to enhance cyber security awareness and provide guidance to both organisations and the wider community. Our primary offerings included:

- Incident reports: We compiled and disseminated summaries and analyses of significant cyber security incidents impacting local organisations. These reports aimed to share lessons learned and improve collective response strategies across the community.

- **Guideline documents:** Our comprehensive guidelines assisted organisations in implementing effective cyber security measures and responding proficiently to incidents. Topics addressed included incident response protocols, risk management strategies, and secure operational practices.
- **Awareness campaigns:** We developed and promoted resources that supported community awareness campaigns, which educated businesses and individuals about the significance of cyber security and safe online behaviours.
- **Newsletters:** We periodically published newsletters for circulation to stakeholders. ITC Services additionally sent out updated circulars to government ministries and agencies.

Achievements

Launch of Fiji's National Digital Strategy

The National Digital Strategy (NDS) was launched in April 2025. The NDS aims to facilitate the creation of a digitally empowered, resilient nation – inclusive of universal high-speed broadband access, responsible and accelerated technology adoption (such as AI and the Internet of Things [IoT]), and boosting economic growth. The NDS reflects Fiji's commitment to transforming its socio-economic landscape by harnessing the power of digital technologies.

Establishment of the national CERT

We are proud to announce the official establishment of the national CERT capability, Fiji CERT. This foundational step enhances Fiji nation's capability to respond effectively to cyber threats and incidents.

On 5 June 2025, Fiji signed the Second Additional Protocol to the Budapest Convention.

Fiji has become the first in the Pacific region and the 50th globally to sign this protocol. This reaffirms Fiji's commitment to combating complex cybercrime and for more efficient cooperation with service providers in other jurisdictions, emergency cooperation, and joint investigations.

Development of Fiji's National Privacy and Personal Data Protection Policy

The creation of this policy represents a significant milestone in safeguarding the privacy rights of individuals, strengthening the data protection framework, and enhancing public trust in Fiji's digital ecosystem. Fiji's National Privacy and Personal Data Protection Policy has been developed by the Ministry of Policing and Communications to strengthen Fiji's governance framework for privacy and personal data protection in an increasingly digital environment.

UN Convention Against Cybercrime membership

In December 2025, Fiji became a signatory to the United Nations Convention Against Cybercrime, making it the 74th UN Member State. The ministry represented Fiji in actively participating in the negotiations, which took over 3 years.

Increased international cyber diplomacy efforts

It was a busy period, with the UN Open-Ended Working Group (OEWG) negotiations in the US, the Budapest Cybercrime Convention Committee sessions in France, the Global RSA Conference in the US, the Singapore International Cyber Week, the ICT Senior Officials and Ministerial Meeting in Fiji, the Asia–Pacific Telecommunity Policy and Regulatory Forum in Fiji, the Women in Tech® Global Summit in Japan, and the ITU World Telecommunications Development Conference (WTDC) in Azerbaijan.

Case study. Ransomware, deepfakes and BEC in Fiji

In 2025, Fiji faced significant challenges in the realm of cyber security. The rise in various cyber incidents globally showed that heightened awareness and prompt action was more important than ever across multiple sectors. A particularly notable event was a series of ransomware attacks that targeted several organisations, and severely disrupted operations and compromised sensitive data. These incidents exposed vulnerabilities and underscored the urgent need for enhanced cyber security measures within both public and private sectors.

In addition to the ransomware attacks, there was an increase in attempts at unauthorised access, where malicious actors attempted to exploit weaknesses in organisational security protocols. These breaches highlighted the critical importance of establishing robust access controls and implementing continuous system monitoring.

The emergence of deepfake technology has also posed challenges, as organisations reported incidents of manipulated media being used to disseminate false information and harm reputations. This trend raised unique issues related to verification and trust, which prompted organisations to improve awareness and training regarding media authenticity and misinformation.

Furthermore, incidents of BEC have become increasingly prevalent, with cybercriminals using sophisticated tactics to impersonate executives and deceive employees into transferring funds or disclosing sensitive information. In response, organisations have had to intensify efforts to implement stronger email security measures and provide comprehensive employee training programs.

In addressing these challenges, Fiji CERT has been proactive in raising awareness and supplying guidelines to help mitigate the risks associated with these cyber threats. Additionally, Fiji CERT has facilitated training sessions to equip organisations with the necessary knowledge to recognise and effectively respond to emerging threats within the cyber security landscape.

In April 2025, the National Digital Strategy (NDS) was launched. Rooted in the National Development Plan, the strategy outlines a clear path towards fostering a dynamic and inclusive digital ecosystem. Central to this vision is developing state-of-the-art digital infrastructure and robust cyber security measures, ensuring that all citizens have secure, continuous, and reliable access to digital services.



Figure 8: The NDS was launched by then Deputy Prime Minister and Minister for Trade, Cooperatives, MSMEs and Communications, the Hon Manoa Kamikamica.



Figure 9: Signing the Second Additional Protocol to the Budapest Convention, 5 June 2025, Director-General Digital Government Transformation, Cybersecurity and Communications, Tupoutuah Baravilala, in the presence of Director of Legal Advice and Public International Law Directorate of the Council of Europe, Jörg Polakiewicz



Figure 10: National Cyber Week, August 2025

In August 2025, Fiji hosted a national Cyber Week, bringing together key government agencies, industry stakeholders, and regional partners to strengthen cyber security awareness and resilience. The Ministry of Communications participated in the event, contributing to discussions on emerging cyber threats, digital governance, and protecting critical information infrastructure. Through its engagement, the ministry reinforced its commitment to enhancing national cyber security capabilities, promoting best practices, and fostering collaboration across sectors. Cyber Week served as a valuable platform for knowledge-sharing, capacity-building, and aligning Fiji's cyber security strategies with global standards and evolving threat landscapes.



Figure 11: The Global RSA Conference in a session titled, 'The Great Cybersecurity Divide', 30 April 2025, with Director-General Digital Government Transformation, Cybersecurity and Communications, Tupoutuah Baravilala (second to right); together with PNG Permanent Secretary for Communications, Steven Matainaho; Singapore's Cybersecurity Agency Deputy Commissioner, Kuan Seah; and Australian Cybersecurity and Critical Technologies Ambassador, Brendan Dowling (moderator)

Cyber diplomacy efforts



Figure 12: The Singapore International Cyber Week panel discussion on, ‘The UN and the Future International Cyber Cooperation’, October 2025, with Director-General Digital Government Transformation, Cybersecurity and Communications, Tupoutuua Baravilala (centre); with Malaysia’s Minister of Digital, the Hon Gobind Deo Singh; Singapore’s Cybersecurity Agency Commissioner, David Koh; Brazil’s Head of the Cyber Defense and Security Division of the Ministry of Foreign Affairs, Larissa Calza; and the UK’s Foreign, Commonwealth and Development Office Cyber Director, Andrew Whittaker



Figure 13: The APT Policy and Regulatory Forum for the Pacific, hosted through the ministry, August 2025, Fiji

Cyber Hygiene Awareness training

Throughout the year, we successfully organised numerous cyber hygiene events aimed at enhancing cyber security awareness among participants from various sectors. These events attracted a diverse group of attendees, including government officials, business representatives, and members of the public.

Each event focused on key topics such as identifying cyber threats, understanding security best practices, and implementing effective cyber security measures. Participants engaged in interactive discussions, hands-on activities, and expert-led presentations designed to empower the audience with the knowledge and skills necessary to protect themselves and their organisations from cyber risks.

- The cyber hygiene awareness session was held at the Market Day for Women on 3 October. This session aimed to raise awareness about cyber security best practices and online safety, specifically targeting women participants as a way to empower them with essential knowledge for protecting themselves in digital environments.
- On 23 and 27 October 2025, there were 2 cyber awareness training sessions conducted for the Ministry of Trade. These sessions aimed at enhancing the ministry's understanding of cyber security best practices, incident response protocols, and threat awareness, ultimately strengthening its overall security posture.
- A cyber awareness training session was also successfully held for critical infrastructure stakeholders in November. This session aimed to deepen participants' understanding of cyber security best practices and incident prevention strategies, thereby enhancing the resilience of critical infrastructure against cyber threats.
- In December 2025, Fiji CERT conducted a comprehensive cyber hygiene awareness training session at the Fiji Learning Institute for Public Service. This training was designed to enhance the cyber security awareness and hygiene practices of public service employees.

The session covered essential topics, including recognising cyber threats, implementing security best practices, and understanding the importance of maintaining secure digital environments. Participants engaged in interactive discussions and practical exercises that emphasised the critical role of cyber security in their daily operations.



Figure 14: Cyber Hygiene Awareness session held for women at Market Day for Women



Figure 15: Cyber Hygiene Awareness training at Ministry of Trade



Figure 16: Cyber Hygiene Awareness training held for Fiji critical infrastructure



Figure 17: Cyber Hygiene Awareness training held for Fiji Learning Institute for Public Service

In November 2025, the GICT Programme was implemented by the Ministry of Policing and Communications to address persistent gender disparities in ICT education, participation, and career progression. It aligns with the ITU global GICT framework and supports national priorities on digital inclusion, skills development, and gender equity within Fiji's emerging digital economy.

The photo below illustrates girls from Labasa College taking part in the program. Delivery followed a blended approach combining guided instruction, hands-on activities, group learning, and role-model engagement, supported by experienced ICT industry facilitators.



Figure 18: School students engaging in cyber workshop

Kiribati



The Computer Emergency Response Team Kiribati (CERT KI)

CERT KI falls under the Digital Transformation Office, which is part of the Ministry of Information, Communications and Transport. The team is currently made up of 3 people, the Chief Information Security Analyst, the Senior Information Security Analyst and the Information Security Analyst.

Those people or organisations wishing to report cyber incidents can do so via:

Email: cert@mict.gov.ki

Phone: 75125401

Threat landscape

The 3 most common cyber security threats for Kiribati are:

- phishing attacks
- scams
- ransomware.

We often respond to phishing and social engineering incidents, ransomware attacks against the government and independent bodies as well as DoS attacks.

Awareness-raising

We conduct yearly cyber awareness campaigns targeting government officials, high school students, community leaders and the general public.

We post our cyber security events, as well as monthly cyber security tips and advice on our ministry's Facebook page.

Achievements

Our organisation accomplished several achievements this year. In partnership with APNIC, we ran a cyber drill with government ministries and state-owned enterprises. We also reached out to 2 of our remote islands, Tabuaeran and Teraina, to deliver our cyber security awareness campaigns to the workers and general public there. We also successfully ran an ICT boot camp that was focused on programming and cyber security, and we set up a cyber security booth during an interschool competition in order to reach high school students.

However, our major highlight was successfully hosting the PaCSON AGM on Kiritimati Island. This important milestone required strong planning, coordination, and teamwork among our staff and stakeholders. The event ran smoothly and provided a great opportunity for discussions, networking, and strengthening regional partnerships.

This year, we also worked with our legal team in drafting a cyber security bill, which passed its first reading last year during parliament. The bill is designed to strengthen cyber security, protect critical systems and ensure organisations handle cyber risks properly. The bill also sets up a national system to manage cyber security, including a working group and special response teams (such as CERTs) to handle incidents. It also focuses on protecting important systems like government services and infrastructure by requiring organisations to follow security rules, regularly check for risks, report cyber incidents, and fix problems quickly. It also encourages sharing information about threats and includes penalties for those who fail to follow the rules, making sure everyone takes cyber security seriously.

Cyber security law is also being tabled in parliament to establish a comprehensive cyber security legal framework to support the protection of critical infrastructure, setting standards and empowering CERT KI in overseeing cyber security across the country.



Figure 19: ICT boot camp, with high school students, Tarawa



Figure 20: Cyber drill event, with government and state-owned enterprises ICT officers during a tabletop exercise



Figure 21: Domingo giving opening remarks during boot camp



Figure 22: Bongraoi with the CyberUp and PaCSON merchandise at the cyber security booth



Figure 23: Terianna and interschool students at the cyber security booth



Figure 24: School cyber security awareness



Figure 25: Kids at the cyber security booth

Nauru



Department of Information, Communication and Technology, Ministry of Telecommunications

The Government of Nauru has a large investment in computing resources and has encouraged government departments to use these resources effectively to share information and knowledge to support the Government's mission. The computer facilities are a shared system made available to promote atmosphere, 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 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.

Threat landscape

Most of the people of Nauru report cyber incidents directly to the Nauru Police Force through either direct walk-in, phone calls or through Facebook chat. Public service workers report to DICT through either phone calls or emails.

Similar to our Pacific neighbours, Nauru experiences many common cyber security threats, including:

- phishing
- identity theft (copying of Facebook accounts in order to impersonate you)
- account hacking (Facebook, IMO, etc.).

On behalf of the Government of Nauru, DICT responds to threats such as business email compromise, hacked social media accounts and phishing emails.

For the reporting period, there was no increase to cyber incidents experienced in Nauru.

Awareness-raising

Awareness raising is conducted via the radio, translating content from PaCSO^N into local language, travelling around and spreading awareness in person, and using PaCSO^N Cyber Up materials.

Sports are very big in Nauru! Therefore, sporting merchandise is useful, especially for raising awareness with young people. The biggest impact items for promoting cyber awareness are rugby balls and backpack gear that can be useful and help our sports teams to succeed.

In October 2025, DICT was privileged to support Nauru Rugby in a timely boost to the Angam 7s series by delivering a collection of Cyber Up Pacific products. These were received on behalf of Nauru Rugby by Executive Member, Mr Chamrock Agir. Nauru Rugby and DICT were able to advise all players, coaches, volunteers and supporters to:

- protect their information online
- be aware of phishing emails
- report scams and online frauds.



Figure 26: Presentation of PaCSO footballs to Nauru Rugby by DICT member, Brancia Itsimaera

DICT publishes many types of news articles, publications or advisory bulletins for public and government application. These are posted on our Facebook, via email to government departments and on our website.

- PaCSO^N Cyber-Up Awareness
- Department of ICT Facebook page

With support from the Australian Infrastructure Financing Facility for the Pacific, the East Micronesia Cable landed in Nauru on 9 August 2025, following a successful landing in July in Kiribati.

The East Micronesia Cable will bring faster, high quality and more reliable and affordable internet to more than 100,000 people across the three Pacific countries, providing better access to services, information and worldwide markets.

Nauru's cheap, fast and reliable internet comes from the new fiber optic cable near the reef, by the Cable Landing Station (CLS). This is important for our country's future. Figure



Figure 27: Officials inspect the East Micronesia Cable



Figure 28: Images of East Micronesia Cable landing into Nauru

Major achievements

The Department of ICT in collaboration with the International Telecommunication Union (ITU) is conducting workshops as part of digital transformation initiatives, in line with Nauru's national sustainable development strategies.

The two workshops on GovStack and accelerating deployment of digital solutions, and Nauru Cyber Incident Response Team (CIRT) Readiness Assessment, are conducted from 7-11 April 2025 at the Tomano room, Meneñ Hotel.

The workshop covers topics including Govstack's toolkits for designing and implementing the government's interoperable digital infrastructure to improve work processes and a comprehensive assessment of Nauru's cybersecurity.

Participants are representatives from various government departments, regulatory bodies, critical infrastructure providers, law enforcement agencies, emergency support providers, central monetary agencies, ISPs, telecommunications companies, the private sector, academia, and national research bodies.



Figure 29: Participants at the GovStack and CIRT Readiness sessions



Figure 30: Attendees to the ACSC bilateral training

Also in collaboration with the PaCSON and the Australian Cyber Security Centre (ACSC) conducted a week long cyber security training package that focused on incident response. The Incident Response cyber security training ran from March 24th – 28th. The main topics were on open source tools, threat intelligence, incident response tooling, acquisition (disk images) and hands on incident response.

Participants are representatives from various government departments, regulatory bodies, critical infrastructure providers, law enforcement agencies, emergency support providers, central monetary agencies, ISPs, telecommunications companies, the private sector, academia, and national research bodies.

New Zealand



National Cyber Security Centre, New Zealand

The New Zealand National Cyber Security Centre (NCSC NZ) is part of the Government Communications Security Bureau (GCSB). In July 2024, the New Zealand Computer Emergency Response Team (CERT NZ), a part of the Ministry of Business, Innovation and Employment (MBIE), was integrated into the NCSC NZ's organisational structure, making NCSC NZ Aotearoa New Zealand's lead operational cyber security agency.

NCSC NZ has a dedicated Pacific Partnerships Team as part of a program 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 response activities:

- institutional governance (supporting the development of CERT or CERT-like functions)
- workforce development
- awareness-raising
- engagement in regional and international forums.

Threat landscape

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

NCSC NZ handles incident reports through 2 distinct triage processes. Most incident reports are managed through the NCSC NZ's general triage process.

A small number of incidents are triaged for specialist technical support due to the nature of the victim or the seriousness of the incident. These incidents could cause high impact at the national level and are referred to as 'incidents of potential national significance'.

In 2025, the top 3 cyber security threats recorded by NCSC NZ were:

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

The 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. Incidents are categorised by significance from C1 (significant) to C6 (minor).

This may include:

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

For 2025, of the total reports received:

- 14 were categorised as C3, significant incidents
- 101 were categorised as C4, moderate incidents
- 192 were categorised as C5, routine incidents
- 3,122 were categorised as C6, minor incidents.

In the 2025 calendar year, there were 4,731 reported incidents, a decrease of 29% from the number outlined in the previous PaCSO^N report.

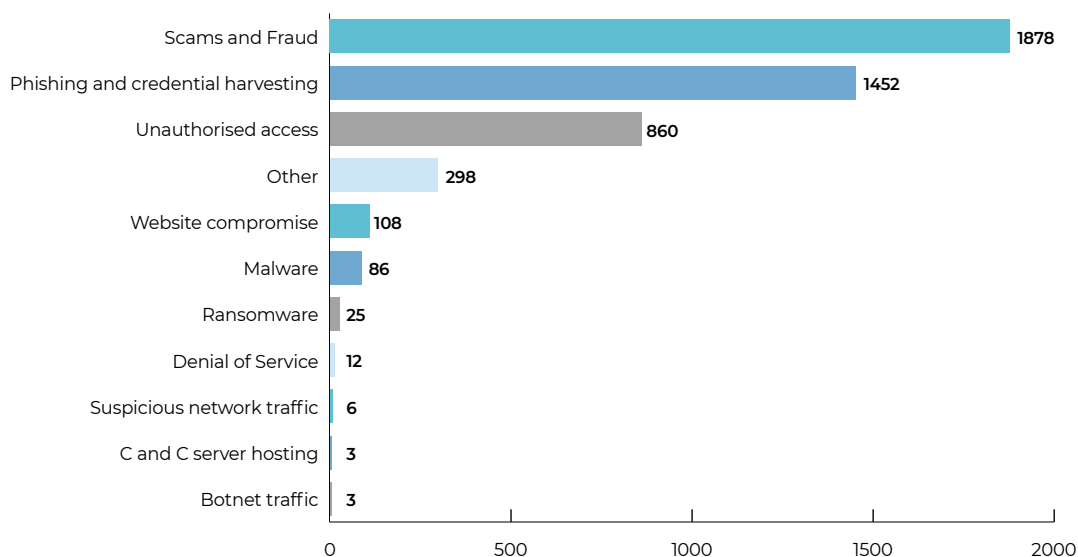


Figure 31: Break-down of reports received

Awareness-raising

Each year, the NCSC NZ runs a public annual awareness campaign during Cyber Security Awareness Month, with Cyber Smart Week running from 6 to 12 October. The campaign for 2025, called 'How Exposed Am I', was designed to show New Zealanders what information scammers might already know about them and to show that we are all vulnerable with our ever-growing digital lives.

It highlighted that over 4.3 million New Zealand account details are exposed to scammers and an estimated NZD1.6 billion is lost every year as a result. The campaign included a website that analyses live data from public global breaches, to provide the user with an exposure score, to indicate how exposed their information is online. Following the exposure score, the site then shares ways the user can protect their information through some basic cyber security actions such as implementing two-factor authentication and long, strong and unique passwords.

<https://www.ownyouronline.govt.nz/how-exposed-am-i/>

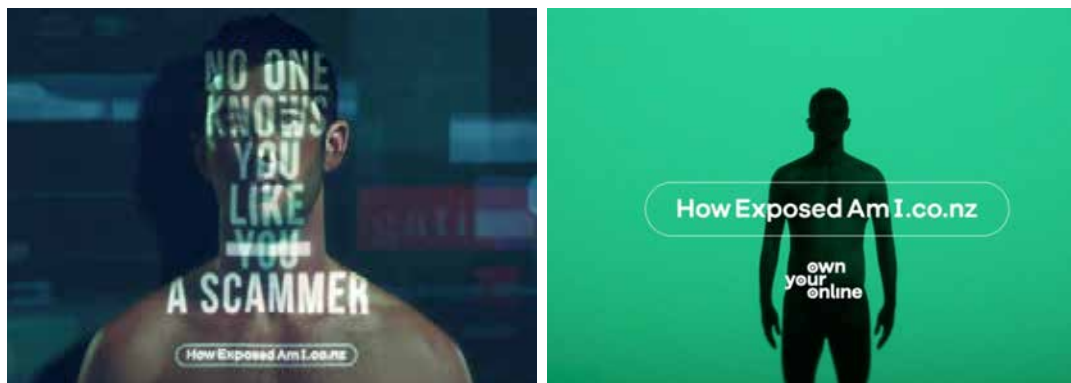


Figure 32: NCSC NZ – 'How Exposed Am I' ad campaign

NCSC NZ continued to publish its quarterly reporting, including the publication of the Cyber Security Insights Report.

In 2025, the NCSC NZ also published research tracking of the cyber security behaviour of individuals and small to medium businesses in New Zealand. Highlights of the research reports were:

- online threats cost New Zealanders an estimated NZD1.6 billion per year
- 94% of New Zealanders believe it's important to protect themselves online
- more than half of New Zealand's small to medium businesses experienced an online threat
- 28% of New Zealand organisations took new cyber security actions in the past 6 months.

In 2025, the NCSC NZ alerted thousands of New Zealanders that their devices had been infected with malware known as ‘Lumma Stealer’, and published guidance on how to look for signs of the malware and how to keep safe after a breach.

NCSC NZ continued to join several international partners in a number of joint publications. These pieces of cyber security advice and guidance ranged from engaging with AI, to cyber security for operational technology and are an effective channel for getting advice out to users.

NCSC NZ also uses their social media channels to draw attention to, and raise awareness of, these publications and general cyber security advice.

Own Your Online social media accounts are tailored for individuals and small to medium businesses, while NCSC NZ accounts target IT professionals and large organisations.



Achievements

As a member of PaCSO^N and co-convenor of the PaCSO^N Capacity Building Working Group (CBWG), alongside CERT Tonga, NCSC NZ supported the development of the **PaCSO^N Capacity Building Action Plan**.

Designed by the Pacific, for the Pacific, the action plan is the key framework for partnering on cyber capacity-building initiatives in the region. It was launched and endorsed by members at the 2025 PaCSO^N AGM.



Case study. Health sector data breach incident

In early 2026, NCSC NZ supported a response to a data breach incident to a third-party contractor in the health sector. The threat actor abused an Application Programming Interface (API), which allowed them to extract sensitive health information from many victims and threatened to post the information online.

The threat actor had a record of targeting health organisations globally, but used common vulnerabilities, suggesting that the New Zealand health sector was not specifically targeted but just happened to be vulnerable.

The response involved multiple government agencies. NCSC NZ supported the victim organisation by providing technical advice on the response actions, reviewing the remediation, and supporting interagency coordination efforts and efforts to minimise the risk of sensitive data being shared publicly. This approach included an emphasis on the New Zealand Government's position to not pay ransoms or negotiate with malicious cyber actors. Ultimately, the data was never published online; the reasons for this are not known to NCSC NZ.



Figure 33: CBWG meeting 2025, Wellington, New Zealand

Figure 34: CBWG meeting, 2025, Wellington, New Zealand



Figure 35: PaCSO AGM, 2025, Kiritimati Island, Kiribati



Figure 36: PaCSO AGM, CBWG Co-convenors CERT Tonga and NCSC NZ launching the Capacity Building Action Plan, Kiritimati Island, Kiribati



Figure 37: Niue–New Zealand engagement



Figure 38: Niue Cyber UP Awareness Roadshow, Chamber of Commerce session

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 for the Republic of Palau.

Threat landscape

The Bureau of Public Safety receives cyber-related reporting through formal reporting frameworks and uses social media, particularly Facebook, to engage with the public.

During the reporting period, among previously reported threats (such as ransomware, malware, phishing attacks, money laundering, identity theft and fraud, and illegal online gambling), the Bureau of Public Safety encountered a notable number of online defamation and libel cases.

Awareness-raising

The Bureau of Public Safety has responsibility for, and conducts various community engagements in, awareness-raising efforts. Much of this engagement in 2025 was through social media, particularly Facebook. The Bureau of Public Safety uses the Ministry of Justice's Facebook page to distribute information and updates and to interact directly with members of the public.

A highlight was launching Palau's Cyber Awareness and Education Campaign in November 2025, which aimed at increasing cyber awareness and safety among Palau's children and included lessons on:

- online safety basics
- cyberbullying awareness
- reporting tools
- digital citizenship.

Achievements

The Bureau of Public Safety looks forward to undertaking further awareness-raising and capacity-building activities in 2026.

Case study. Passing the Cybersecurity Act

A major achievement, supported by the Bureau of Public Safety, was the Palau Senate unanimously passing the Cybersecurity Act, in October 2025. This is the nation's first comprehensive single piece of legislation relating to cyber security. The Senate cited growing digital dependence, rising cyber threats, protection of privacy and digital rights, international alignment, and economic trust and resilience as the key reasons behind passing the legislation. As at the end of the reporting period, the legislation was with the House of Delegates for consideration.

Papua New Guinea



Department of Information and Communications Technology (DICT)

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

The department operates under the Ministry of Information and Communications Technology. Our structure is designed to drive the digital transformation of Papua New Guinea. DICT is led by the Secretary, who is supported by deputy secretaries overseeing various wings, such as the Digital Delivery and the Policy and Emerging Technologies wings.

The mission of DICT is to harness the potential of ICT to help Papua New Guinea become a smart networked and knowledgeable society. This will bring the PNG Government closer to the people through effective governance, improved service delivery, and socio-economic 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 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.

We focus on:

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

We are committed to working as one team, across all 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:

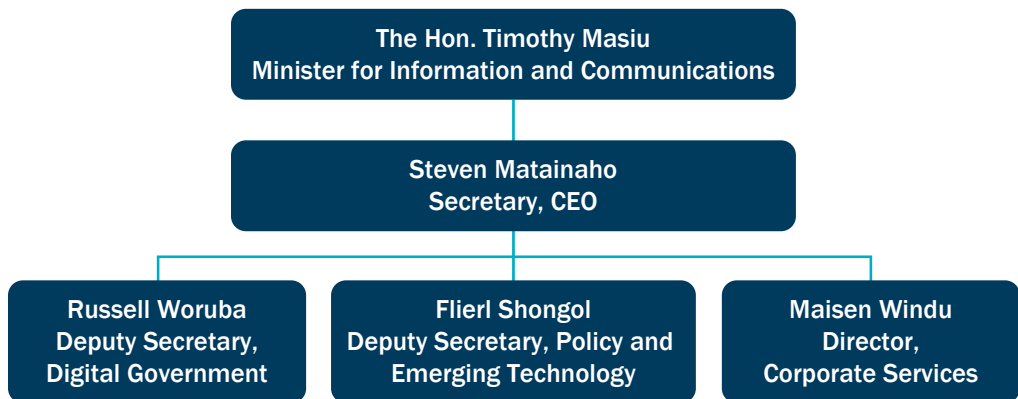


Figure 39: DICT organisational structure

Threat landscape

Individuals and organisations in Papua New Guinea can report incidents through 2 primary channels:

- Technical reporting: Through the PNG National Cyber Security Centre (NCSC PNG) or PngCERT. Reports can be submitted via the official websites www.ncsc.gov.pg or www.pngcert.org.pg.
- Criminal reporting: Cybercrimes, such as online fraud or harassment, should be reported to the Cyber Crime Unit of the Royal Papua New Guinea Constabulary, which works closely with DICT.

Based on recent trends in the region, the most common threats include:

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

Regarding malware incidents, NCSC PNG uses its own Security Information and Event Management (SIEM) to monitor endpoints and firewalls, enabling it to respond to detected threats at any time.

For phishing and social engineering attacks, DICT uses all its social media platforms to provide guidance on containment and prevention, as well as conducting public awareness campaigns.

In addition to technical monitoring and response, DICT actively identifies and responds to online harm such as misinformation, disinformation, impersonation, and scam-related content circulating on social media platforms. Through the eSafety and Social Media Monitoring Desk and the PNG Cyber Safety initiative, suspicious or harmful content is monitored, profiled, and reported to relevant platforms for takedown, while public advisories are issued to prevent further spread and victimisation.

During the reporting period, several incidents were reported. Incidents are not always reported directly or immediately. Some incidents are not reported at all for various reasons that may align with individual organisations' policies.

During the recent reporting period, we have observed an increase in the total number of reported incidents. This increase is attributed to the country's rapid digital expansion and therefore the increased visibility of our reporting channels, which has encouraged more citizens and businesses to come forward.

Awareness raising

DICT provides awareness-raising via its social media pages, mainly Facebook and LinkedIn. These are platforms that are very accessible and are often updated daily!

DICT also supports the PNG Government, and spreads awareness through official communication channels. DICT provides printed materials and graphics online to the community, and raises awareness through local talk back radio shows.

We engage in several initiatives to promote cyber safety:

- **Cyber Security Awareness Month:** Every October, we lead national campaigns to educate the public on digital hygiene.
- **Digital Transformation Summit:** We host annual summits (like DTS25) to discuss data safety and emerging technologies with stakeholders.
- **Community outreach:** We use pamphlets and digital standards guides to teach online safety and responsible social media use.

In addition to existing awareness efforts, DICT operates the PNG Cyber Safety platform, which delivers targeted and simplified cyber awareness content to the public. This includes awareness campaigns on phishing, smishing, misinformation, cyberbullying, and emerging threats such as AI-generated scams.

Content is developed in simple, easy-to-understand language and distributed across Facebook, LinkedIn, and community groups to maximise outreach. The initiative also involves re-sharing awareness materials across multiple online platforms, including Facebook and WhatsApp groups, to reach wider audiences at the grassroots level.

DICT also develops creative content such as infographics, short videos, and thematic campaigns (like Cyber Tuesday Awareness) to continuously engage users and promote safe online behaviour.

On our website, www.ict.gov.pg, DICT regularly supports awareness-raising initiatives, promoting cyber security awareness materials for communities and government users.

The DICT Facebook account is used on a regular basis to support information-sharing and awareness-raising initiatives. Here, DICT can post near real-time updates on what we are working hard to achieve and deliver on behalf of the nation.

In addition to website and social media updates, DICT produces regular cyber safety awareness articles, advisories, and visual content under the PNG Cyber Safety initiative. These include:

- cyber awareness articles (for example phishing, smishing, viral hoaxes, data protection)
- infographics and public advisory graphics
- social media alerts on ongoing scams and misinformation trends
- community-targeted awareness content re-shared across Facebook and WhatsApp groups.

These materials are designed for public consumption and are published regularly to ensure timely awareness of emerging threats.

Case study. Infrastructure Investment Summit – PNG Investment Week 2025

In December 2025, the PNG ICT Delegation met with representatives from Microsoft, in Sydney, Australia, ahead of the Infrastructure Investment Summit – PNG Investment Week.



Here, Papua New Guinea's digital transformation agenda took centre stage at the summit. Leading the delegation was Acting Minister for ICT, the Hon Peter Tsiamalili Jr, and DICT Secretary, Steven Matainaho, who met with Microsoft to explore emerging cyber security challenges, and the role of cloud and data solutions in advancing digital government services.

On Day 4 of the Investment Week, session 2 of the summit was themed 'Stronger Together: Digital Inclusion & Regional Connectivity'. Here, Minister Tsiamalili Jr presented on Papua New Guinea's ICT potential and highlighted the launch of Sevis PNG, which is a foundational digital public infrastructure (DPI) ecosystem designed to drive secure identity, digital payments, and data exchange across sectors.

The minister also covered Papua New Guinea's strategic position as:

- one of the largest digital markets in the Pacific (10+ million people)
- a nation with expanding mobile and FinTech adoption
- a government committed to digital reform
- a rising hub for Pacific digital cooperation
- a prime destination for ICT investment through Investment Week 2025.

The Prime Minister, the Hon James Marape, made an address explaining that the four-day program would focus on regulation, climate, investment, and infrastructure, and also commended Anthony Smaré and the PNG Chamber of Resources and Energy for attracting more than 2,000 participants.

The Australian Prime Minister, the Hon Anthony Albanese, pointed to infrastructure development, defence cooperation, education programs, and growing private sector interest as key areas of progress. He said Australia's support would help Papua New Guinea reach its economic potential and ensure Pacific nations can 'author their own destiny'.

PNG aims to become a digitally inclusive, secure, and innovation-driven economy – inviting global partners to join its transformation journey.



Case study. PNG Cyber Safety initiative

In addition to national and international engagements, DICT strengthened its digital awareness footprint through the PNG Cyber Safety initiative. This included consistent production and distribution of cyber safety content, increased engagement across social media platforms, and successful reporting and takedown of harmful online content that included scam pages, impersonation accounts, and misleading information.

The initiative also contributed to improving public reporting behaviour by encouraging users to identify and report suspicious online activities.

Case study. National SIM card registration

Into the future, DICT is supporting changes to SIM card registration. In 2025, we took the first steps to changing SIM card registration rules for mobile users by aligning current policy with the new National Digital ID Policy 2025.

Acting Minister for ICT, the Hon Peter Tsiamalili Jr, said the National ICT Authority (NICTA) would begin consultations on a revised regulation following the launch of SevisPass and the SevisWallet App at the Digital Transformation Summit 2025.

Key changes ahead include:

- **Adults (18+):** all SIMs must be linked to a SevisPass digital ID through the SevisWallet App
- **Teenagers (13–17):** can register SIMs under a SevisPass-Minor, connected to a parent or guardian's account
- **Children (0–12):** SIMs must be registered as dependent accounts under a parent or guardian's SevisPass
- **Grace period:** from 1 January to 30 June 2026, all existing SIM holders must link their numbers to SevisPas; unlinked SIMs will be deactivated after this date
- **Annual checks:** Every SIM will undergo digital ID re-verification once a year
- **Data protection:** Telcos will no longer store raw biometrics; instead, secure SevisPass tokens will be used.

Why are we doing this? The new regulation aims to:

- clean up PNG's SIM ecosystem
- reduce fraud, scams, and crime
- meet anti-money laundering and counterterrorism obligations
- make it easier for citizens to access government services, financial services, and more online services with a trusted PNG-owned digital ID system.

Acting Minister Tsiamalili Jr said the changes will strengthen trust in mobile services while protecting privacy and giving young people a safe way to connect online.

You can learn more about the process of how Papua New Guinea is implementing SIM card registration via a digital ID here: [SIM Card Registration to Link With Digital ID | DICT I PNG](#)

In addition to policy developments, DICT expanded its cyber awareness and online safety efforts through active monitoring and reporting of harmful online content. A notable activity included identifying and reporting explicit and harmful content online, which resulted in successful takedown actions by platform providers. This demonstrates Papua New Guinea's growing capability, not only in policy and infrastructure, but also in practical cyber safety enforcement and community-level protection through digital platforms.

The National CERT of Papua New Guinea (PNGCert) and the National Information and Communications Technology Authority (NICTA)

PNGCert operates within NICTA, the national ICT regulator, which is under the Ministry of ICT. NICTA, and therefore PNGCert, is tasked with collaborating with government ministries and agencies, universities, internet services providers, banks, and mobile network operators.

The PNGCert works to promote awareness, provide advisory assistance and coordinate responses to cyber security incidents in Papua New Guinea. Its constituency covers all users of the internet ecosystem, including individuals, service providers, enterprises, and government agencies. 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/report-incident/>

Threat landscape

Similar to many in the Pacific region, we face the common threats of account hacking, BEC, phishing emails and financial fraud.

For the reporting period, we observed the following threats:

- ransomware
- BEC
- digital and online abuse material.

NICTA is constantly working with the PNG Government and our colleagues in DICT to improve and enhance national incident response capabilities. During the reporting period, we responded to the common cyber security threats affecting our constituents in Papua New Guinea.

There was an increase in the monetary scamming, social media false news, and targeted attacks on various organisations in the reporting period.

You can learn more about the threat environment and the types of threats affecting different parts of our society here: <https://www.pngcert.org.pg/common-threats/>.

Awareness-raising

NICTA engaged in the following awareness-raising activities during the reporting period:

- Safer Internet Day: an awareness-raising initiative to encourage cyber safety and practice safer behaviours when using the internet
- cyber awareness campaigns: through the NICTA website and NICTA Facebook account, we post regularly as it's the most accessible way to engage our constituents
- awareness-raising materials: provided by PaCSO, these are used as part of our community engagement activities.

We also support in-person awareness-raising initiatives, and engage a lot with school groups to promote cyber security, such as the NextGEN ICT School Exposition and ICT School Competition!

As part of Papua New Guinea's 50th Anniversary celebrations, NICTA invited primary and secondary schools in the National Capital District and Central Province to participate in the NexGen ICT School Exposition, and invited all primary and secondary schools nationwide to participate in the ICT School Competition!

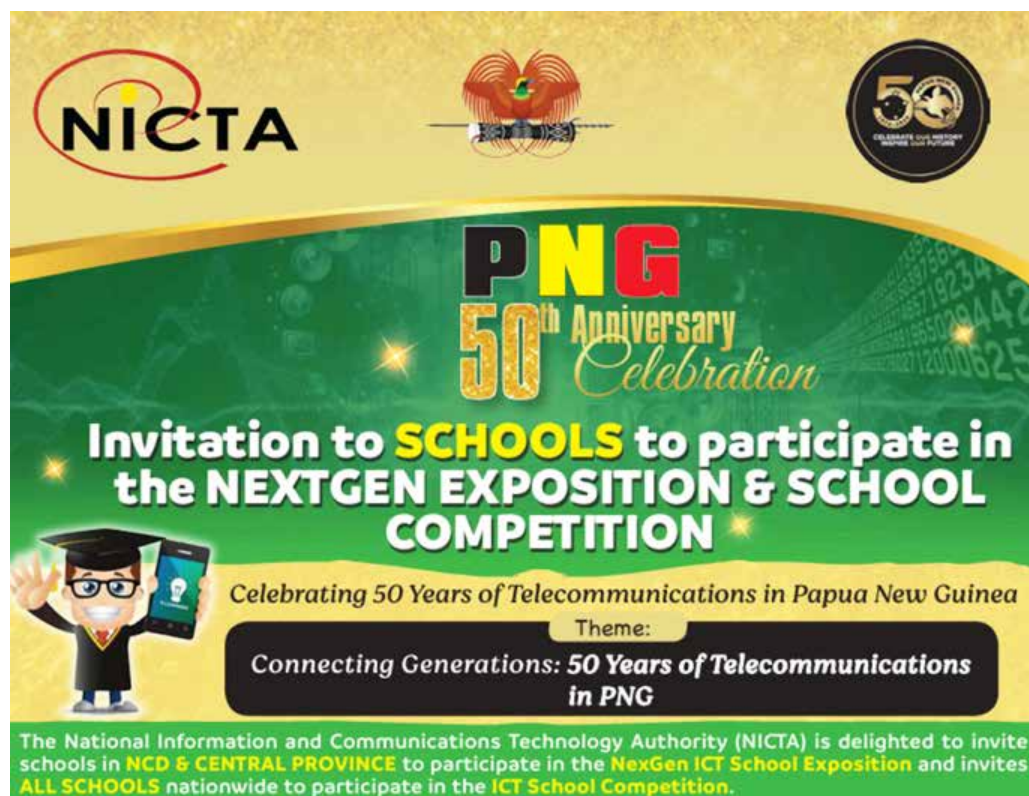


Figure 40: The ICT School Competition advert - the competition was open to all Year 3 to 8 students in primary schools and Year 9 to 12 in secondary schools throughout the country.

Major achievement: Publishing the National ICT Indicators Report 2025

In December 2025, Acting CEO of NICTA, Polume Lume, presented the National ICT Indicators Report 2025, the second edition of Papua New Guinea's national ICT indicators publication.

This report provides ICT industry with a performance overview as well as key developments from 2020 to 2024, and reaffirms NICTA's commitment to maintaining an evidence-based approach to ICT regulation and sector oversight.

Since the publication of the inaugural edition in 2022, Papua New Guinea's ICT industry has continued to evolve. Major structural changes include the amalgamation of Telikom PNG Limited and Bmobile Limited, the transfer of Telikom PNG Limited's wholesale assets to PNG DataCo Limited, and the entry of new operators such as Vodafone PNG (Digitec Communications Limited) and Telstra Limited. These developments have reshaped the sector's competitive dynamics and, together with the operational impacts of the COVID-19 pandemic, highlight the increasing need for accurate, reliable and timely industry data to guide policy, regulation, and long-term planning.

Despite challenges in data availability and reporting consistency, this current edition of the report presents key indicators covering investment, infrastructure expansion, network coverage, affordability, and service uptake. Over the five-year period, total sector investment remained strong at PGK1.64 billion, driven in part by significant capital expenditure following Vodafone PNG's entry in 2022.

Infrastructure growth was substantial during the same year, with the construction of 539 new mobile towers contributing to wider network reach and employment growth across the sector.

However, the findings also highlight areas requiring continued attention. Although infrastructure expanded, mobile population coverage declined from 86% in 2022 to 77% in 2024, signalling persistent gaps in digital accessibility. Affordability remains a challenge for many Papua New Guineans, with mobile broadband prices still above the affordable price target, based on an affordability study conducted by NICTA in 2024 and 2025.

To address gaps in operator reporting, NICTA employed statistical estimation and forecasting methods to ensure that national trends are presented as accurately as possible. Strengthening compliance with reporting obligations remains a priority, and NICTA will continue working with licensees to improve data quality and the overall integrity of national ICT statistics.

I would like to sincerely thank the telecommunications operators, wholesale service providers, internet service providers, broadcasters, narrowcasters and all ICT stakeholders who contributed directly and indirectly in the support of the publication of this report. I also commend NICTA for its commitment to producing this report under challenging circumstances.

As we look ahead, NICTA remains focused on enhancing regulatory frameworks, improving data collection processes, and supporting the development of a more connected, inclusive, and affordable digital future for Papua New Guinea.

Case study. Facebook misinformation about NICTA

In 2025, NICTA found itself in the spotlight of a misinformation campaign, and was supported to release a statement that confirmed its role in mediating and reporting Facebook posts in the country.

This was a case where there was a lot of online misinformation claiming that NICTA ‘pulled down’ many pages, such as Big Lee’s Facebook page. In response, NICTA clarified that it is not responsible for, and does not, pull down Facebook pages. NICTA, in its role as the national ICT regulator, only regulates and issues licences for broadcasting and communication in accordance with our governance and legal authority.

In a public statement, NICTA confirmed for their stakeholders that Facebook pages can only be taken down by Facebook, following an extensive review and moderation process conducted by the owner of Facebook, Meta, and where a report is found to be true and valid. Anyone can report an issue to Meta when they believe that it is not in compliance with Facebook Community Standards.



Separately, the Internal Revenue Commission and Central Bank of PNG both had a cyber incident; the organisations resolved the issues within their capacity with assistance from KPMG.

NICTA conducted specialised cyber security training in international law for government and critical infrastructure stakeholders in Port Moresby in February 2026. The program focused on legal readiness, cyber incident management, and digital forensic training, and was provided often in partnership with international aids.

The training was provided by Cyber Law International and co-funded by NICTA and DFAT.

Papua New Guinea has also officially joined a growing international coalition to combat cybercrime, becoming one of 65 nations to sign the United Nations Convention Against Cybercrime. The signing ceremony took place on 25 October at the National Convention Centre in Hanoi, Vietnam.



Figure 41: Representing Papua New Guinea, the Secretary for DICT, Steven Matainaho, was joined by Chief Legal Officer of NICTA, Oala Moi, who played a key role in the 2024 treaty negotiations.

Samoa



Samoa Computer Emergency Response Team (SamCERT)

SamCERT is a unit of the Digital Transformation & Innovation Division within the Ministry of Communications and Information Technology, for the Government of Samoa. Established in 2019, SamCERT is Samoa's national cyber security agency, with its primary focus being on monitoring and delivering a safe and resilient cyberspace for all Samoan citizens.

SamCERT's 3 key pillars of work are cyber security, cyber safety and cyber inclusion. Its services are available to all citizens of Samoa, tourists, businesses, and government agencies. The SamCERT team currently includes the roles Principal Cyber Emergency Incident Handling Officer, Principal Cyber Emergency Awareness & Engagement Officer and the Senior SamCERT Officer.

Individuals and organisations in Samoa can report cyber security incidents and access guidance on how to protect themselves against cyberattacks through the following channels:

Online incident report form: samcert.gov.ws/report-incident

Email: samcert@mcit.gov.ws

SamCERT encourages all citizens, businesses, and government agencies to report suspicious activity promptly to ensure a timely and effective response.

Threat landscape

Similar to many of our Pacific neighbours, Samoa's commonly experienced cyber security threats include:

- malware and ransomware attempts
- phishing emails targeting individuals and organisations
- spam email campaigns.

In addition, SamCERT has observed a growing sophistication in threats targeting the Pacific, including activity by state-sponsored threat actors such as APT40, as detailed in SamCERT's February 2025 advisory.

SamCERT responds to a broad range of cyber security incidents affecting individuals, businesses, and government agencies across Samoa. The types of incidents SamCERT handles include:

- malware and ransomware infections on government and private sector networks
- phishing campaigns targeting Samoan citizens and government departments
- BEC and social engineering attacks
- exploiting critical software vulnerabilities in widely used platforms (such as FortiOS, FortiProxy)
- suspicious or malicious network activity identified through monitoring of government infrastructure
- disinformation and social media misuse, including monitoring activity during national events such as the Samoa general elections
- requests for technical assistance and cyber incident guidance from public sector agencies.

SamCERT's response activities include triaging and analysing reported incidents, issuing advisories, coordinating with international partners (including PaCSO members), and targeting technical support to affected organisations.

In 2025, a notable example of SamCERT's response work was the publication of an advisory on APT40 – a sophisticated state-sponsored cyber group conducting malicious operations against Pacific government networks and critical infrastructures. This advisory drew on SamCERT's own investigations and intelligence shared by partner countries. You can read the full advisory:

https://www.samcert.gov.ws/sites/default/files/documents/2025-02/APT40%20-%20SamCERT%20Cyber%20Threat%20Advisory_FINAL_0.pdf

For the reporting period, there was an increase of cyber incidents responded to by SamCERT.

Awareness-raising

SamCERT undertook a wide range of awareness-raising and capacity-building activities throughout 2025, targeting government staff, the private sector, and the broader public.

Threat Hunting Training – February 2025

SamCERT facilitated an intensive five-day Threat Hunting Training activity for government IT staff. The training provided participants with hands-on skills in identifying and responding to advanced threats on government networks. The closing ceremony was attended by Australian High Commissioner, Will Robinson, reflecting the strong bilateral partnership supporting Samoa's cyber security capability.



Figure 42: Group photos, threat hunting training

Cyber security tabletop exercise – May 2025

SamCERT conducted a series of cyber security tabletop exercises throughout May 2025 for about 15 government agencies. These exercises were designed to test the cyber preparedness and incident response procedures of participants in a simulated environment, building cross-government resilience and coordination capacity.



Figure 43: Group photo, cyber security tabletop exercises

National Cybersecurity Strategy 2025/26–2030/31, Stakeholder Validation Workshop June 2025

The Ministry of Communications and Information Technology (MCIT), through SamCERT, hosted the National Cybersecurity Strategy 2025/26 – 2030/31 Stakeholder Validation Workshop. This was a significant milestone in Samoa's national cyber security planning, bringing together government agencies, private sector representatives, and development partners to validate the strategic direction of the next 5 years.



Figure 44: Group photo, National Cybersecurity Strategy Stakeholder Validation Workshop

Talavou Cyber – May and July 2025

SamCERT launched 'Talavou Cyber', a targeted cyber security education program for young Samoans. The pilot session was held in May 2025 with students from 2 secondary schools, incorporating a cyber awareness presentation and a mini capture-the-flag (CTF) activity. Building on this success, the program was extended to tertiary-level institutions in July 2025, with a larger session in July 2025.



Figure 45: Group photo, Cyber Pilot, Talavou



Figure 46: Group photo, Cyber Launch, Tavalou

Cyber induction at MCIT – October 2025

SamCERT hosted its internal cyber induction sessions for MCIT staff as part of the Cyber Awareness Month. The pilot session introduced the staff to PaCSON's Cyber Upskill Program (CUP), building practical skills for staying safe online, and engaged them in a CTF activity to reinforce their learning. This pilot was the foundation for a planned full rollout of the CUP across the entire ministry.



Figure 47: Group photo, Cyber Induction at MCIT, October 2025

Media engagement and collaboration with the Ministry of Police

Throughout 2025, SamCERT engaged local media outlets to amplify cyber security awareness messaging to the wider public. SamCERT also collaborated with the Samoa Police to monitor social media activity during the general elections, ensuring the integrity of the digital information environment during the national event.

Regional resources

SamCERT continues to draw on and distribute regionally developed cyber security awareness materials, including the PaCSON CUP and Cyber Up Pacific materials.

SamCERT produces many types of news articles, publications or advisory bulletins for public and government application. These are posted on our Facebook page, via email to government departments, and on our website.

Example of SamCERT Cyber Threat Advisory, published in 2025, regarding FortiOS & FortiProxy.***Authentication bypass in Node.js websocket module vulnerability:***

Fortinet has identified a critical vulnerability in FortiOS and FortiProxy and has observed active exploitation of this vulnerability. The vulnerability may allow an unauthenticated remote attacker to gain 'super-admin' privileges to the firewall device. This is typically used as an initial access vector for threat actors to gain access to target environments. Devices running FortiOS 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 may be affected.

More information on the vulnerability can be found in the National Vulnerability Database. The Fortinet vulnerability notification published by the vendor describes possible indicators of compromise and IPs associated the threat actor, which may assist in identifying suspicious activity on potentially affected Fortinet devices.

SamCERT advises that organisations and government departments implement the following controls to determine if you are [affected by] and to detect for instances of, exploitation of FortiOS and FortiProxy devices and to limit its effectiveness:

- *determine potential impact*
- *enhancing detection*
- *mitigating controls.*

You can read the full advisory at www.samcert.gov.ws

Achievements

Samoa participates in the Forum of Incident Response & Security Teams (FIRST). In November 2025, SamCERT was accepted into the 2026 FIRST Suguru Yamaguchi Fellowship Program, connecting Samoa directly to a global trust network of over 800 incident response teams. This participation connects SamCERT to a global cyber incident response network via a prestigious four-year Fellowship.

This highly competitive Fellowship transitions SamCERT from a national operator to a key member in the international cyber security community. The program provides SamCERT with real-time global threat intelligence, specialised mentorship, and a pathway to full membership in FIRST.

Key program highlights include:

- **incident response collaboration and partnership:** Foster strong relationships and trust with other fellowship teams, regional and international partners to enhance information-sharing and lay the groundwork for future collaboration.
- **annual FIRST conference support:** Participate in hands-on training and mentoring and building SamCERT technical capacity.
- **FIRST membership support:** Receive assistance in becoming a full member of the FIRST community.

Neighbouring Pacific Island Countries that have graduated from the Fellowship Program include Tonga's Computer Emergency Response Team–CERT Tonga and CERT Vanuatu–CERT VU.

Cyber threats do not respect borders, and this program ensures that when SamCERT and Samoa face a threat, we are not fighting alone in ensuring a cyber secure and resilient Samoa and Pacific.

Case study. SamCERT APT40 Advisory – February 2025

In February 2025, SamCERT published a landmark advisory on APT40. This advisory was prompted by the discussions, at the PaCSO^N 2024 AGM, about the ongoing challenges Pacific nations have been grappling with for years regarding cyberattacks from state-backed and criminal groups. The purpose of producing this document for public release was to advise our Pacific community of the threat and to remain alert.

This advisory outlined the activity of a sophisticated cyber group and the threat it posed to networks hosted in the Blue Continent. The advisory drew on both SamCERT's investigations and insights shared by other partner countries that had reported extensively on this threat actor.

APT40 is a state-sponsored cyber group that uses advanced capabilities to conduct malicious cyber operations against government and key critical infrastructure systems.

This group has previously targeted the US and Australia, and has most recently been observed conducting operations directed at the sensitive networks administered by Pacific nations.

- You can read the full SamCERT advisory at www.samcert.gov.ws
- You can read the full ACSC advisory at www.cyber.gov.au
- You can read the NCSC alert at www.ncsc.govt.nz/alerts/prc-mss-tradecraft-in-action/

Case study. Samoa Cyber Week 2025 – October 2025

Samoa Cyber Week 2025, themed 'Protecting our Future, Empowering our People', was held from 26 to 31 October 2024. Organised by SamCERT, under MCIT, the event brought together government, development partners, the private sector, communities, and youth in a comprehensive national capacity-building initiative.

Cyber Week 2025 was structure across 4 complementary tracks:

- Community & Business Awareness Track (2 days)
- Technical Cyber Detect and Defend Practicum (4 days)
- Government Preparedness Track (2 days)
- GovStack Digital Government Consultation (2 days).

This week-long event represented Samoa's most comprehensive national cyber security event to date, uniting strategic policy dialogue, hands-on technical training, government incident preparedness, and digital government transformation under a single national platform. The event has established a strong foundation for a whole-of-government approach to cyber resilience in Samoa.



Figure 48: Official photo from Samoa Cyber Week 2025

Solomon Islands



Solomon Islands Government Information and Communication Technology Services (SIG ICT Services)

SIG ICT Services is under the Ministry of Finance Corporates Services and 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, which includes technical, management and administration positions, and 10 junior professional staff. 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.

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

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

Threat landscape

The 4 common cyber security threats in the Solomon's include:

- phishing attack
- malware
- brute force attack
- AI-driven attack.

Similar to the rest of the Pacific, the Solomon Islands experience a wide range of cyber threats from local and international actors.

SIG ICTS Services is equipped to respond to a variety of cyber security incidents affecting government ministries and agencies. Our growing team is always improving its tradecraft and working with stakeholders to increase awareness of how everyone can work to make themselves cyber secure. The type of incidents and the SIG ICT Services responses to them include:

- **Phishing and social engineering attacks:** Investigating and mitigating email-based attacks where users are tricked into revealing sensitive information or clicking malicious links.
- **Malware infections:** Detecting and responding to infections by viruses or malicious software on government systems and networks.
- **Unauthorised access and account compromise:** Identifying and containing incidents where user accounts or systems are accessed without permission, often due to weak passwords or credential theft.
- **Insider threats:** Investigating security breaches caused by employees or contractors, with legitimate access, who misuse their privileges.
- **Endpoint security alerts:** Handling alerts from security tools such as antivirus, firewalls, or endpoint detection platforms (for example, CrowdStrike) to take immediate remediation actions.
- **Nation-state threats:** Close monitoring of nation-state actors, alerted to by their known intrusion and attack tactics, character and behaviour. Endpoint Detection and Response (EDR) tools can identify nation-state actors and monitor them closely.
- **AI-driven attack:** We have seen a lot of AI-driven attacks, which have been described by Crowdstrike as a new class of threat, where adversaries use artificial intelligence to enhance malware, phishing, and intrusion campaigns.

For the reporting period, cyber incidents in Solomon Islands were sustained compared to the number experienced in the last period.

Awareness-raising

Our organisation is dedicated to enhancing cyber security awareness through ongoing campaigns for staff and communities. We have established awareness training in collaboration with the Institute 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. We also sponsor the Women in IT Solomon Islands – GICT Day, and the CyberQuest.

We will be conducting cyber awareness education sessions in 20 schools in Honiara and 18 Starlink pilot sites in the Western Province.

Awareness is an ongoing activity that we are proud to support.

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.

SIG ICT Services is a regular promoter of the PaCSO_N Cyber Smart Pacific Campaign, which is always met with much appreciation and interest by our stakeholders.

Achievements

Throughout 2025, SIG ICT Services was pleased to conduct a series of practical exercises on incident and communication response, broaden the awareness campaign, improve cyber security resilience and support a mass Windows 10 software upgrade.

Case study. 2024 Pacific Islands Forum Leaders Meeting

In 2025, following a request from the Solomon Islands Government and support from Australia's regional Cyber RAPID Assistance for Pacific Incidents and Disasters (RAPID) program, SIC ICT Services provided cyber security support for the 54th Pacific Islands Forum (PIF) Leaders Meeting. This was achieved alongside the efforts of our Solomon Islands colleagues and brothers and sisters from other Pacific CERTS.

The support activity included cyber specialists from Papua New Guinea, Vanuatu, and Samoa, operating under the PaCSO_N, as well as Australian government officials and cyber security experts from the private firm CyberCX.

This collaborative effort underscores the importance of Pacific partnerships in delivering effective cyber security solutions. In preparation for the meeting, Cyber RAPID established dedicated secure networks at event venues to ensure safe internet connectivity for delegates. A SIEM system was also deployed to monitor network activity and respond to potential cyber threats.

Cyber RAPID and SIG ICT Services worked together closely, along with SICERT, to monitor systems and provide incident response support for the duration of the whole event.

Australian High Commissioner to Solomon Islands, His Excellency Rod Hilton said, 'as Solomon Islands' primary security partner, Australia is committed to supporting the Solomon Islands Government's operations to ensure the 54th Pacific Islands Forum Leaders Meeting is safe and secure – both offline and online [and] ... Australia's Cyber RAPID deployment, along with the deployment of cyber expertise from Pacific Islands countries, demonstrates that cyber security is best delivered from within the Pacific region'.

Beyond the immediate support for the Pacific Islands Forum Leaders Meeting, the deployment also took advantage of the gathered specialists to deliver training and capacity-building for SIG ICT Services and the SICERT staff. This component focused on strengthening the Solomon Islands' sovereign cyber security capabilities in ways that will ensure long-term resilience and preparedness experience for future major events.



Figure 49: Participants from the 2025 PILFM SOC

Solomon Islands Computer Emergency Response Team (SICERT)

The Ministry of Communication and Aviation (MCA) is comprised of 2 key divisions: the Communications Division, and the Aviation Division. SICERT is a unit under the Communications Division. SICERT is responsible for providing services related to cyber security to the Solomon Islands Government, statutory bodies, law enforcement agencies, businesses and the people.

The team currently consists of 6 officers: the Deputy Director Cybersecurity, the Chief Cybersecurity Officer, and 4 cyber security officers. The Deputy Director provides strategic oversight, while the Chief Cybersecurity Officer manages operational coordination. The 4 cyber security officers support incident response, monitoring, reporting, stakeholder engagement, and awareness activities. We are currently a small team and are in the process of recruitment planning and restructuring of SICERT to strengthen our capacity and improve our operations.

Given the always developing cyber security environment, our officers perform cross-functional roles to support current operations and strengthen SICERT's capacity as it continues to develop.

Individuals and organisations in the Solomon Islands can report cyber incidents directly to SICERT through official communication channels. Reports can be submitted via email, phone contact, or formal written correspondence to the MCA. SICERT is working towards establishing an online presence through a website, which will serve as a cyber incident reporting channel.

Threat landscape

- phishing
- online scams
- social engineering attacks.

Currently, the team is not yet actively engaged in formal incident response operations. The organisation is working towards developing this capability.

SICERT has not conducted any incident responses during the reporting period.

Awareness-raising

SICERT has been focusing efforts on actively promoting cyber security and highlighting the importance of safe and responsible digital technology use across the Solomon Islands through various outreach activities.

- **Awareness sessions in the rural communities:** We have expanded our cyber security awareness programs to rural communities, including sites where new telecommunications towers have been established and internet access is being introduced for the first time. These sessions aim to educate communities on both the benefits of being online and the potential risks, ensuring they are informed about safe and responsible internet use.

- **Radio broadcasts:** Cyber security tips and advice are aired nationwide to reach a wide audience. These broadcasts focus on raising awareness of common cyber threats such as online scams, phishing, fake social media accounts, and misinformation, and also provide practical guidance on safe online behaviour, including protecting personal information, using strong passwords, and being cautious when engaging with unknown links or messages. The aim is to ensure that even communities without regular internet access can receive timely and accessible cyber security awareness information.
- **Printed awareness materials:** We develop and distribute posters, online safety-tip calendars, and pamphlets to ministries, schools, and communities to support ongoing cyber security education and awareness.

Through these efforts, SICERT educates the public, builds safer online practices, and strengthens the overall cyber security culture in the Solomon Islands.

SICERT produces various materials to inform the public and organisations about cyber security threats and best practices, including:

- **Social media updates (Facebook):** We share cyber security awareness content, including best practices, online safety tips, and cyber awareness posts through our official Facebook page: <https://www.facebook.com/solomonislandscert>.
- **Awareness materials:** We produce printed awareness materials such as posters, online safety tips incorporated into calendars, and pamphlets to support cyber security education and outreach activities.

Achievements

Our organisation has achieved several of its key goals, including:

- providing cyber security awareness
- successfully installing a server environment that is now used to support internal systems and enhance operational capability
- working in collaboration with CyberCX to develop cyber security frameworks and standard operating procedures.

Case study. Cyber security support at the Pacific Islands Forum Leaders Meeting

No major cyber events were been reported this year; however, during the Pacific Islands Forum (PIF) Leaders Meeting, from 8 to 12 September, our team worked alongside SIG ICT Services, CyberCX, Vanuatu CERT (CERTVU), and representatives from Papua New Guinea and Kiribati to provide cyber security support, address any potential incidents, and gain valuable insights from their expertise.

Case study. Launching the SICERT Project

The Solomon Islands Government, through MCA, and in partnership with the governments of Australia, the UK, and New Zealand, launched the SICERT Project as a collaborative effort to strengthen our country's cyber security resilience and combat emerging cyber threats.



Figure 50: Launching the SICERT Project, SICERT officer, Madlyn Watatofea, and Deputy Director Cybersecurity, Allen Danitofea, at Ngella, Central Island Province



Figure 51: Madlyn Watatofea and Allen Danitofea at Siota Provincial school, Central Island province



Figure 52: SICERT officer, Andrew Aratara, at Nukufero village, Central Island Province

Tokelau



Office for the Council of the Ongoing Government of Tokelau (OCOg)

OCOg is the executive body in Tokelau. It was established in November 2003 and leads the non self-governing territory of New Zealand. Its leadership and capital rotates yearly between its 3 coral atolls, Atafu, Nukunonu and Fakaofu.

The team is small but provides a wide range of support and guidance to the services and functions of OCOg.

OCOg is responsible for the National IT Unit, which oversees the country's core IT infrastructure and ongoing technology developments, while also working closely with the local IT units across the atolls.

Cyber incidents are reported directly to the National IT Unit, which is responsible for mitigating, isolating, and resolving the issue. The National IT Unit is also responsible for providing updates and reports to the Head of OCOg (National GM), who will then report to the council.

Threat landscape

During the reporting period, Tokelau has experienced:

- ransomware events
- credential harvesting
- malware attacks.

New Zealand statute law does not apply to Tokelau unless expressly extended to Tokelau, and no New Zealand legislation is extended to Tokelau without its consent. This means that, when responding to cyber incidents, Tokelau does it on a case-by-case basis with NCSC NZ.

OCOg and the National IT Unit are responsible for dealing with any type of cyber security incident. This includes supporting our local IT teams in the villages, departments and our local ISP (TeleTok).

During this period, there was only one major cyber incident recorded. The incident involved a ransomware attack targeting the main server room at the Tokelau Apia Office. Fortunately, the

National IT Unit responded quickly by identifying and isolating the issue before it could spread further across other servers and the wider network infrastructure.

During the reporting period, Tokelau has maintained the number of incidents experienced. As our ability to manage cyber events matures, we can better deter and respond to cyberattacks.

There have been major upgrades to the IT infrastructure at our Apia office, resulting in a significant reduction in potential threats and reported incidents. These improvements have strengthened the overall security and reliability of the network environment.

The next phase of the project is to implement similar upgrades and infrastructure improvements across the atolls within the coming months, with the aim of enhancing cyber security and system performance throughout Tokelau.

Awareness-raising

Merchandise and promotional products are a very impactful way to raise awareness. The team regularly uses PaCSO materials to engage our constituents and most vulnerable digital operators across all atolls.

The use of social media is also a very effective tool for awareness-raising. OCOG regularly shares updates and notices on our official Facebook account.

We are currently planning an NCSC NZ-funded roadshow to Tokelau, focused on raising awareness about cyber threats and the importance of cyber security. The initiative aims to educate communities on safe digital practices and strengthen overall cyber resilience.

The roadshow is intended to involve the wider community, including the Council of Elders, NGOs, schools, churches, and other community groups, to ensure broad engagement and awareness across all sectors of society.

The team provides awareness-raising via its social media pages, mainly Facebook. These are platforms that are very accessible and are often updated weekly! We also email our government officers with urgent notices when required.

- www.facebook.com/GovernmentofTokelau
- [Government of Tokelau - https://www.tokelau.org.nz/](https://www.tokelau.org.nz/)

Achievements

With assistance from the NCSC NZ, the OCOG is exploring the possibility of establishing an upskilling program for government officials and developing a formal cyber security response function. We are also:

- creating virtualisations of the server network
- in the final stages of completing the rebuild and revamp of the government's website.
- implementing our centralised data management system.

Casestudy: Locky Ransomware

During the reporting period, Tokelau experienced a ransomware attack. The team observed weird icons associated with 'Locky' on the desktop, after browsing the servers.

Locky is a type of malware that locks access to your files and demands a ransom to unlock: 'here's how your team can prevent a Locky ransomware attack'.

This attack was an important learning opportunity for us. As a small team, we had limited resources to support the response and limited internal process for managing a cyberattack. From this, we decided to change our network structure to be a virtual network, with the rebuilding process ongoing.



Tonga



Tonga Computer Emergency Response Team (CERT Tonga)

CERT Tonga serves as the Kingdom of Tonga's National CERT. It acts as the central point of contact for national cyber security matters, including incident response, digital forensics, awareness programs, professional training, and the dissemination of security bulletins and advisories.

The department operates under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications, and Climate Change (MEIDECC).

Organisational Structure and Divisions

To better align with international standards and national needs, CERT Tonga recently restructured from 2 divisions (Engagement and Technical) into 3 specialised divisions:

- Governance, Risk Management, and Compliance (GRC)
- Communication, Awareness, and Engagement (CAE)
- Digital Forensics and Incident Response (FIR) Workforce and Development

The department's current workforce is a blend of permanent staff and contracted specialists.

- Permanent staff: Currently includes the Director, Senior Engagement Officer, Assistant Engagement Officer, and Information Security Analyst.
- Cyber security Workforce Development Program (CWDP): Funded by CERT NZ since November 2021, this program supplements the team with an IT System Operator (apprentice) and a Security Forensic Analyst. The CWDP was concluded in August 2025.

- Future growth: For FY2025–26, a proposal has been submitted to establish several new leadership and technical roles, including:
 - Deputy Director Communication, Awareness and Engagement (CAE)
 - Deputy Director Digital Forensics and Incident Response (DFIR)
 - Chief Information Security Officer (CISO)
 - Senior Information Security Analyst
 - Digital Forensic Analyst
 - IT System Operator.

Constituents

CERT Tonga provides critical cyber security services and support to a broad range of stakeholders across the Kingdom, including:

- government ministries, departments, and agencies
- private sector businesses
- public enterprises
- NGOs.

Stakeholders and the general public across the Kingdom of Tonga may report cyber security incidents through several accessible channels. CERT Tonga maintains a multiplatform intake system to ensure timely assistance and comprehensive coverage:

- Digital reporting: Secure reporting is available via the official CERT Tonga website and dedicated email correspondence.
- Direct communication: For immediate inquiries, the public can reach our team via telephone or through our official Facebook page.
- In-person consultations: For sensitive or complex matters, face-to-face reporting is available at our office during standard business hours.

Threat landscape

The common cyber security threats faced by Tonga include:

- ransomware attack (INC Ransom)
- phishing email and fraud email
- malware (info stealer).

CERT Tonga responded to the following types of incidents during the reporting period, and collaborated with stakeholders to achieve outcomes:

- ransomware attacks, to a limited extent, mainly coordinating stakeholders and third parties
- phishing emails (scam emails), collaborating with stakeholders and third parties
- fraud emails, coordination and collaboration with stakeholders and third parties
- CERT Tonga has often been requested by the Cybercrime Working Group to support the Attorney General.

There is still an increasing number of incidents with new variations of phishing scams and fraud. However, there is also an increase in brute force attacks on credentials to obtain access using Secure Shell (SSH), Remote Desktop Protocol (RDP) and Telnet.

There are also ongoing scams of free online education and courses translated into Tongan, as well as web defacement incidents, which mainly affect the government websites. A number of malicious IP addresses were also reported from our Telecom sector. These were addressed by reaching out to the organisations who owned these IP addresses.

Awareness-raising

Targeted awareness programs

In 2025, CERT Tonga conducted a series of strategic awareness initiatives for key stakeholders, including government ministries, departments, and Tonga Women in ICT (TWICT).

These sessions delivered a comprehensive briefing on the agency's operational mandate and an in-depth analysis of the 2025 cyber threat landscape, successfully strengthening national digital resilience through targeted stakeholder engagement.

Public engagement: 'Empowering a Resilient Digital Tonga'

CERT Tonga leveraged the National ICT Expo to advance the 'Empowering a Resilient Digital Tonga' initiative, providing a platform for direct public consultation and cyber security advocacy.

Technical capacity-building and training

Awareness is only half the battle; the other half is technical readiness. CERT Tonga invests heavily in enhancing the skills of ICT personnel across the Kingdom:

- CERT Tonga successfully completed a specialised technical workshop facilitated by APNIC at the national CERT office. The session provided practical, hands-on experience in deploying security monitoring tools and refining investigation workflows. This initiative marks a significant step in enhancing the team's operational readiness to detect and mitigate sophisticated cyber threats.
- To move from a 'reactive' to a 'proactive' stance, CERT Tonga collaborates with the RAPID Team from Australia:
 - Practical workshops: This involves 'threat hunting' exercises joined by CERT Tonga Team and the staff from Digital Transformation Department.
 - Incident response: Training ensures that, if a major attack occurs, participants have the hands on experience to work alongside international experts to contain the threat and restore services quickly.

Advisories and security bulletins can be seen through CERT Tonga's website:

<https://cert.gov.to>



Achievements

In 2025, CERT Tonga significantly advanced the Kingdom's digital resilience through international collaboration, specialised capacity-building, and intensive national outreach. Key achievements include:

- **International strategic alignment:** The signing of a landmark cyber security MoU with Australia established a framework for threat intelligence sharing and coordinated incident response, serving as a pillar of the 2025 Australia – Tonga Development Partnership Plan.
- **Advanced institutional capability:** Internal technical expertise was substantially elevated by the return of a senior staff member from Australia, following the completion of a Master of Cybersecurity Analysis. This specialised skill set enhances the department's daily operation.
- **National resilience and outreach:** The department successfully delivered 10 comprehensive awareness sessions across the Kingdom. These targeted initiatives improved the security posture of Government Ministries and NGOs, ensuring that critical infrastructure and civil society remain protected against evolving digital threats.

In 2025, Tonga reached 2 significant milestones in its cyber security landscape: a major defensive response to a national crisis and the enactment of landmark legislation.

Case study, The National Health Information System ransomware attack

In June 2025, Tonga's Ministry of Health (MoH) was targeted by a major ransomware attack that paralysed the National Health Information System (NHIS).

The incident was discovered on June 15, 2025: the attack encrypted vital patient records, prescriptions, and medical histories across the country's 4 hospitals.

Hackers encrypted the NHIS Oracle database API (the VAMED application not the actual data files) and sent a ransom note saying that they were well aware of cases where recovery companies tell MoH that the ransom price is TOP5 million, but in fact the recovery company is secretly negotiating with the hackers for TOP1 million. The note went on to say that, if MoH approached them directly without intermediaries, MoH would pay several times less. The Tongan Government refused to pay or negotiate with the perpetrators.

However, Tonga (MoH) requested help from the Australian Government's program for emergency cyber disaster relief provided by the Cyber RAPID Team (Deloitte). From there, a Cyber RAPID team was deployed to assist CERT Tonga and the MoH. By July 18, 2025, the system was reported as fully restored using backups and enhanced security protocols, though the event underscored the urgent need for digital resilience.

Case Study. The Cybersecurity Act 2025

Following the health sector crisis, the Kingdom formally strengthened its legal framework with the Cybersecurity Act 2025, which received Royal Assent on 28 August, 2025.

Training sessions

Hands-on session exploring tools for security monitoring, incident response, and investigation with APNIC.



Figure 53: CERT Team in their office during the training session, 23 July 2025.



Figure 54: Threat Hunting Practical Training, CERT Tonga and the Digital Transformation Department led by Australia's Cyber RAPID Team



Figure 55: Threat Hunting with Australia's RAPID Team at the Ministry of MEIDECC

Cyber security awareness to the following stakeholders

Throughout 2025, CERT Tonga executed a series of targeted awareness initiatives involving key stakeholders, including various Government Ministries, departments, and our strategic partner, TWICT. These sessions were designed to provide a comprehensive overview of CERT Tonga's operational mandate and an in-depth analysis of the 2025 cyber threat landscape. By fostering these partnerships, CERT Tonga continues to strengthen the nation's collective defence against evolving digital risks.



Figure 56: Community, Free Wesleyan Church of (Halafo'ou) Pahu



Figure 57: WICT ICT Expo, 2 May 2025



Figure 58: Non-government organisations, government ministries and departments



Figure 59: TWICT staff



Figure 60: Images from awareness raising events



Figure 61: Department of Communications operates under the Ministry of MEIDECC

International collaboration

CERT Tonga became a co-convenor with NCSC NZ for the Capacity Building Working Group (CBWG) and the first formal meeting took place in June 2025, Wellington, New Zealand. However, a key part of PaCSO is the CBWG. Over the years, we have seen the implementation of various initiatives and the capacity growth of members who have contributed to their respective national efforts. To help shape future efforts in the Pacific, and noting the increase of partners wanting to engage on capacity-building, members have agreed to the establishment of the CBWG Three-Year Action Plan to signal the areas of need at a Pacific regional level.

The 5 pillars will channel our focus to help build capacity in areas that matter most to our PaCSO members and chart a way forward that will be tangible and measurable.



Figure 62: PaCSO Capacity Building Working Group official visit photo - June 2025

Training

In September 2025, CERT Tonga, with representatives from TWICT and the Digital Transformation Department, joined the Cybersecurity Training & Exercise for Pacific Islands facilitated by Japan's Ministry of Internal Affairs and Communications and the Japan International Cooperation Agency in Fiji.



Figure 63: Images from regional workshop – December 2025, Vanuatu

In December 2025, Senior Internet Security Specialist, Adli Wahid, and Dr Etuate Cocker led a regional cyber security workshop in Port Vila, Vanuatu. Collaborating with ITU and APNIC, the program, which included a CERT Tonga staff member, built capacity for 10 Pacific nations. The session focused on strengthening digital pathways and fostering regional cooperation.



Figure 64: Images from KISA training - August 2025, Tonga

In August 2025, 2 participants from CERT Tonga attended the APISC training course in the Republic of Korea hosted by the Korea Internet and Security Agency (KISA).

In September 2025, CERT Tonga also participated in the APT Training Course on AI and Cybersecurity in Shanghai, China.



Figure 65: Images from APT Training – September 2025, Shanghai



Drills and exercises

From 6 to 8 May 2025, CERT Tonga also attended the GISEC Global CyberDrill 2025 in Dubai, UAE. Organised by the ITU and hosted by the UAE's Cyber Security Council, this drill aims to enhance international cyber resilience and strengthen cyber security capacity through regional cooperation. It involved over 130 national cyber security authorities and global CERTs, CIRTs, and CSIRTs, fostering cross border collaboration and response strategies against evolving cyber threats, cyber security tactics and procedures.

The 2025 ITU Regional CyberDrill for Asia and the Pacific Region took place from 2 to 5 September, 2025, in Ulaanbaatar, Mongolia. This event aims to unite the cyber security community across the region and foster international cooperation. It will feature 4 thematic sessions: Reflect, Share, Learn, and Practice, focusing on building cyber resilience and safeguarding critical information infrastructure. The event will include high-level regional conferences, hands-on training sessions, and simulated cyber incident response exercises.



Figure 66: CERT Tonga attended GISEC Global CyberDrill 2025, Dubai, UAE



Figure 67: CERT Tonga and a few others from the Pacific attended the Asia-Pacific CyberDrill, September 2025, Ulaanbaatar, Mongolia

Seminars and presentations



Figure 68: FIRST Conference, June 2025, CERT Tonga and participants from PaCSON community, Copenhagen



Figure 69: FIRST Conference, June 2025, CERT Tonga and participants from PaCSON community, Copenhagen



Figure 70: CERT Tonga also attended the Cybersecurity Workshop for ASEAN Member States and Pacific Island Forum Member States, December 2025



Figure 71: The RSA Conference International Cyber Security Forum, 28 May to 1 June, San Francisco, US



Figure 72: Telecommunication study tour to Australia's Regulators and Commission Authorities, 5 to 9 May 2025, Melbourne and Canberra, Australia



Figure 73: Global Forum on Cyber Expertise Annual Working Group Meeting and Global Conference on Cyber Capacity Building, 13 to 15 May 2025, Geneva, Switzerland



Figure 74: The first Pacific Cyber Week, with second Pacific Cyber Capacity Building and Cooperation Conference, 11 to 14 August 2025, Nadi, Fiji



Figure 75: Internet Corporations for Assigned Names and Number 84 2025 AGM, 25 to 30 October 2025, Dublin, Republic of Ireland



Figure 76: Asia Pacific Internet Governance Academy 2025, 18 to 22 August 2025, Busan, Republic of Korea

Other International activities

Under the engagement between CERT Tonga and the Council of Europe, here are the following activities that CERT Tonga attended in 2025.



Figure 77: The TCY 32, Octopus Conference and the Glacy-e Steering Committee



Figure 78: The Underground Economy Conference 2025, co-hosted by the Cybercrime Programme Office of the Council of Europe (C-PROC) in cooperation with Team Cymru, 1 to 4 September 2025, Headquarters of the Council of Europe, Strasbourg, France.



Figure 79: CERT Tonga is currently a member of the PaCSO community, which includes 17 Pacific countries that have joined this community. In October 2025, the PaCSO AGM was held on Christmas Island, Kiribati



Figure 80: In November 2025, CERT Tonga also attended the APCERT AGM and Conference that was held in, Sydney, Australia

Tuvalu



Department of Information and Communication Technology (DICT)

DICT, within the Ministry of Transport, Energy, Communications and Innovation, has 9 staff and from the 9, 2 cyber security staff.

For any assistance, customers can write us an email or come see us at our office.

Threat landscape

The most common cyber security threats to Tuvalu are:

- scams
- phishing
- ransomware.

During the reporting period, the DICT team experienced a sustained rhythm of incidents. For 2025, there was one significant incident the team needed to respond to.

Awareness-raising

Through public awareness efforts, the DICT Team engages local community groups, schools and at-risk users to educate them on cyber security awareness using the PaCSO promotional products and campaigns.

DICT does not produce alerts or advisories for the public, but does develop them to use within government and then circulates them using email.

Achievements

The team regularly conducted Outer Islander awareness-raising initiatives during the reporting period. These are an important tool to ensure that all peoples across Tuvalu are receiving cyber security advice and can engage with the team to best protect themselves online.

Phishing the Tuvalu

The only cyber event that has occurred this year, and was responded to, was the phishing email that has been circulating around government staff using a government email account, which has been compromised.



Figure 81: Tuvalu ICT staff



Figure 82: School Awareness for Niulakita Island, Tuvalu



Figure 83: School Awareness for Vaitupu Island, Tuvalu



Figure 84: School Awareness for Motufoua Secondary School, Tuvalu



Figure 85: School Awareness for Nukufetau Island, Tuvalu

Vanuatu



CERT Vanuatu (CERTVU)

CERTVU is Vanuatu's national CERT, established under the Department of Communication and Digital Transformation (DCDT), within the Ministry for the Prime Minister, Vanuatu Government. CERTVU currently has 4 dedicated staff members, 3 of whom are employed full-time and 1 on a contract basis.

CERTVU is the national CERT for Vanuatu and serves the entire country, including government institutions, private sector organisations, NGOs, civil society, and visitors who live in or visit Vanuatu.

Report incidents to CERTVU via:

- CERTVU's online incident report portal at our website: <https://cert.gov.vu/index.php/services/incident-resolution>
- our phone contact
- our social media platform
- our office. CERTVU is operating on an open-door policy, meaning people do not necessarily need to make an appointment to come to the office. People can come in at any time during working hours.

Threat landscape

- phishing
- malware
- ransomware.

CERTVU responds to reported cyber security incidents and any other form of related issues or abuse. We also provide ongoing support to the Vanuatu Police on cybercrime and cyber-related crimes investigations.

Awareness-raising

CERTVU delivers its cyber security awareness campaigns by various methods. These methods include:

- national radio talk show, on cyber security and selected ICT topics
- national events: delivering awareness through our participation in national events throughout the country
- cyber security awareness videos: we develop cyber security awareness videos and upload to our websites and social media platforms
- Cyber Smart Pacific – CyberUP Campaign
- one-on-one community awareness program: provides specific cyber awareness to rural communities
- Schools' Cyber Awareness Campaign: provides cyber security awareness to primary and secondary schools
- business house awareness
- public and private awareness, and intelligence sharing
- flyers, brochures, and guides on cyber security:
- bulletins – <https://cert.gov.vu/index.php/information/security-bulletin>
- advisories – <https://cert.gov.vu/index.php/advisories>
- news and press releases – <https://cert.gov.vu/index.php/news-latest>.

Achievements

Some of our major achievements this year include:

- Senior Secondary School Cybersecurity Boot Camp in Luganville, Santo
- Cyber Smart awareness program
- Cybersecurity Radio Talk Show program
- Train the Trainers Initiative
- Famili i Redi program.

Case Study, Cyber security boot camp on Santo Island, Luganville

The primary objective of this boot camp is to develop future cyber security experts across multiple focus areas. We believe that involving students as early as high school will help shape and guide them towards careers in cyber security.

In May 2025, CERTVU marked a significant milestone by expanding its cyber security boot camp to the northern province of Sanma, Santo Island, Luganville. Partnering with APNIC and collaborating with 9 senior secondary schools and the University of the Pacific sub-centre, we delivered the second Vanuatu Senior Secondary School Cyber Security Boot Camp to more than 50 students over 2 intensive days. Sessions covered cyber security fundamentals, threat identification, best practices, and responsible ICT use, culminating in a hands-on CTF challenge and a career panel featuring ICT and telecommunications professionals who shared their educational journeys.

The boot camp's primary objective is to cultivate future cyber security experts by engaging high school students early and guiding them towards rewarding careers in this critical field.



Figure 86: Cyber security boot camp, May 2025



Figure 87: Some participants receive certificate of participation after completing the boot camp



Figure 88: Luganville Senior Secondary School cyber security boot camp

Train the Trainers initiative



Figure 89: Train the Trainers Initiative, Emua Community

Youth partnership



Figure 90: We are partnering with the National Youth Council of Vanuatu for a day, delivering a cyber security presentation at the Youth Seminar.



Figure 91: CERTVU supporting location sports days

Digital Week Cyber Challenge game



Figure 92: The CERTVU team put out a cyber challenge game for the public during Digital Week celebrations



Figure 93: CERTVU delivers a one-hour session on ICT and cyber security on Radio Vanuatu every Friday

Schools cyber security awareness



Figure 94: Cyber Awareness Raising sessions with local school groups

Famili i Redi



Figure 95: Our team, during our Famili i Redi program, along with our local partners (World Vision Vanuatu, Ministry of Justice, Digicel Pacific, and Vodafone Vanuatu)



Figure 96: Local community cyber security awareness and capacity-building session



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 many teams, including cyber threat intelligence (CTI) teams, a response team (CERT-FR), regulation and certification teams, regulatory teams, and an expertise team. ANSSI's mission is to defend national information systems, as well as to advise and support the French Government, administrations and French critical infrastructure and companies.



ANSSI is an agency of approximately 700 employees and depends on General Secretariat for Defence and National Security (SGDSN), which is within the Prime Minister's Department.

Threat landscape

- attacks conducted for profit, sabotage and/or destabilisation
- ransomware attacks (128)
- data breach / data leaks (196).

Achievements

The AI Action Summit

The summit was held in Paris from 6 to 11 March, 2025, and gathered representatives from 100 countries. For more information go to: <https://www.elysee.fr/en/emmanuel-macron/artificial-intelligence-action-summit>. During the summit, a document relating to AI risk analysis was signed by 19 international partners and 5 national partners and has since been published: https://messervices.cyber.gouv.fr/documents-guides/high_level_risks_analysis_ai_paris_summit.pdf.

REMPAR25

On 18 September, 2025, ANSSI organised REMP25 with the support of associations, national and regional partners. This was a nationwide cyber crisis exercise held in 8 different time zones, and gathered more than 5,000 participants and 1,000 entities.

In French Polynesia and New Caledonia, 42 public and private entities active in various fields (such as telecommunication, transport, tourism, energy, and health care) participated in this exercise. The simulation aimed at testing organisations' ability to respond to a systemic cyberattack, and focused on the needs related to anticipation, preparedness, and training for crisis management and business continuity systems.

For more: <https://cyber.gouv.fr/securisation/gestion-de-crise/entrainement-crise/rempar/rempar25/>

Awareness-raising

- <https://cyber.gouv.fr/nous-connaître/publications/>
- activity reports
- guides and recommendations
- scientific publications
- risk analysis (by sectors and on technologies).
- <https://www.cert.ssi.gouv.fr/>
- security advisories
- cyber threats reports.



Figure 97: ANSSI's HQ, Hotel National des Invalides, Paris

Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security (CCCS), also referred to as the Cyber Centre, is part of the Communications Security Establishment (CSE), Canada's national cryptologic agency, and reports directly to the Minister of National Defence.



The Head of CCCS is supported by various directorates focused on operations, partnerships, and technical expertise. As part of the broader CSE (which employs over 3,800 people), CCCS draws on a highly specialised workforce, combining expertise in software engineering, mathematics, and cyber threat intelligence.

The CCCS uses its technical expertise to safeguard the information and systems that Canadians rely on. We:

- defend Government of Canada networks
- advise and assist other levels of government and the operators of Canada's critical infrastructure, such as banks, telecommunications companies and other companies that are essential for the functioning of our society and economy
- offer simple and effective tips that all Canadians can use to help keep themselves safer online.

Threat landscape

According to the National Cyber Threat Assessment 2025–2026, the top threats facing Canada are:

- **state-sponsored cyber threats:** the cyber programs of the People's Republic of China (PRC), Russia, and Iran remain the greatest strategic cyber threats to Canada
- **cybercrime:** financially motivated and opportunistic cybercrime continues to be the cyber threat activity that is most likely to affect Canadians and Canadian organisations. Ransomware, fraud, scams, and phishing remain persistent threats
- **trends shaping Canada's cyber threat landscape:** CCCS uses its expertise to help monitor, detect, and investigate threats against Canada's information systems and networks. We have identified 5 trends that are shaping Canada's cyber threat environment:
 - **Trend 1:** AI technologies are amplifying cyber space threats
 - **Trend 2:** Cyber threat actor tradecraft is evolving to evade detection
 - **Trend 3:** Geopolitically inspired non-state actors are creating unpredictability
 - **Trend 4:** Vendor concentration is increasing cyber vulnerability
 - **Trend 5:** Dual-use commercial services are in the digital crossfire.

Achievements

- CCCS responded to 2,561 cyber security incidents affecting federal institutions and critical infrastructure partners during FY2024–25, underscoring sustained, high-tempo national operations.
- CCCS formally established the Canadian Cyber Defence Collective (CCDC) in February 2025, following its announcement in Canada’s new National Cyber Security Strategy (NCSS). The CCDC was created as a national public–private partnership mechanism to advance cyber resilience through direct collaboration with industry, critical infrastructure operators, academia, and other stakeholders.
- CCCS co-sealed 26 cyber threat intelligence products with international partners during FY2025–26.
- CCCS published the National Cyber Threat Assessment 2025–2026.
- CCCS released its Ransomware Threat Outlook 2025–2027.
- CCCS released the new tool, CLUE. This is a centralised framework that can be integrated into other applications to provide users with enrichments and insights to help them in the discovery, investigation, triaging and reporting of cyber security incidents.

Awareness-raising

CCCS releases publicly accessible news, publications or advisory bulletins at:

- <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 America's cyber defence agency and 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; federal, state, local, territorial, and tribal governments; the private sector; and the American people.



CISA's primary constituencies include:

- federal and state, local, territorial, and tribal governments
- critical infrastructure sectors
- the private sector
- education institutions
- NGOs
- the general public
- international partners.

Threat landscape

- ransomware
- phishing
- malware.

Achievements

- In August, CISA launched the Software Acquisition Guide: Supplier Response Web Tool. This is a no cost, interactive resource that helps government and industry decision-makers embed cyber security best practices into their procurement activities.
- In September, CISA collaborated with the National Security Agency and 19 international partners to launch a Software Bill of Materials for Cybersecurity Guide. This enables organisations to identify components, assess risks, and take informed action to protect critical systems.
- In December, CISA launched the Cybersecurity Performance Goals 2.0. This gives critical infrastructure owners and operators clear, practical steps to reduce risk.

Awareness-raising

CISA regularly releases advisory bulletins to update entities about significant cyber security vulnerabilities, incidents, and mitigations. Regular publications include the Known Exploited Vulnerabilities Catalogue, phishing-resistant MFA fact sheets, and Security-by-Design and Secure-by-Default advice. CISA also publishes MITRE ATT&CK guidance and cyber assessment fact sheets as seen below.

- <https://www.cisa.gov/news-events/alerts/2026/04/16/cisa-adds-one-known-exploited-vulnerability-catalog>
- CISA Issues Updated RESURGE Malware Analysis Highlighting a Stealthy but Active Threat
<https://www.cisa.gov/news-events/news/cisa-issues-updated-resurge-malware-analysis-highlighting-stealthy-active-threat>
- CISA Adds One Known Exploited Vulnerability to Catalog
<https://www.cisa.gov/news-events/alerts/2026/04/16/cisa-adds-one-known-exploited-vulnerability-catalog>

Federal Bureau of Investigation

The US Federal Bureau of Investigation (FBI) has 56 field offices with a cyber task force at each. The FBI has the cyber action team that acts as an incident response team, with the ability to deploy globally if a cyber incident meets certain thresholds. The FBI has cyber experts in many US embassies, including Canberra, Australia, that act as liaisons to host countries.



The FBI is willing to conduct cyber investigative training in the Pacific.

The FBI's foremost obligation is to protect the people of the US and uphold the Constitution. This includes safeguarding public safety, civil liberties, and national security, and investigating federal crimes in the public interest.

In the modern threat environment, this responsibility explicitly includes cybercrime and cyber security, recognising that:

- digital systems are critical to public safety and national security, including financial markets, health care, elections, energy, and communications
- cybercrime directly harms individuals, businesses, and institutions through fraud, ransomware, identity theft, intellectual-property theft, and data breaches
- cyber threats from nation-states and criminal groups can undermine democratic institutions, economic stability, and trust in government.

Threat landscape

- BEC
- data breach
- ransomware

Achievements

In 2025, the FBI released Internet Crime Complaint Center reporting covering ransomware and cyber-enabled fraud losses.

Key outcomes highlighted in 2025 briefings included:

- hundreds of millions of US dollars in ransom demands disrupted or prevented
- increased use of FBI-facilitated decryption tools and early warning alerts
- lower successful payment rates among organisations that engaged the FBI early.

Awareness-raising

Throughout the year, the FBI also continued high-visibility efforts to expose and warn about foreign cyber actors pre-positioning in US critical infrastructure, notify affected entities directly (sometimes privately, sometimes publicly), and coordinate removals of compromised devices and access points.

Please see Internet Crime Complaint Center (IC3) - <https://www.ic3.gov/Home/IndustryAlerts>

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 over 830 teams from corporations, government bodies, universities, civil society, and other institutions, representing 115 countries around the world.



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 meeting events for security experts
- hands-on workshops
- annual incident response conferences
- good practices and community built standards
- special interest groups
- community and capacity-building.

FIRST has been a PaCSON partner since 2023 and enjoys a strong, shared community with PaCSON and mutual engagement across our events and activities.

Achievements

FIRST has collaborated with PaCSON and the Pacific community through various channels. Some select examples from 2025 have included:

- In June 2025, FIRST worked with the PaCSON Secretariat to welcome a strong delegation of Pacific participants and PaCSON partners to the 2025 FIRST Annual Conference (FIRSTCON25) in Copenhagen, Denmark.
- FIRST was pleased to continue collaboration with CERTVU as part of the Suguru Yamaguchi Fellowship Program. In 2025, FIRST also received SamCERT's application to join the program and is excited to welcome Samoa as part of the 2026 cohort. CERT Tonga graduated from the program in 2024.
- FIRST continues to engage in international forums alongside Pacific partners, including collaboration at the UN OEWG sessions during the Pacific Cyber Week, and through the Global Forum on Cyber Expertise (GFCE). As part of the May 2025 GC3B, held in Geneva, Switzerland, FIRST worked with Pacific partners on a joint Working Group B workshop, on an incident response surge capacity with SamCERT, FIRST and the Swiss National Cyber Security Centre (NCSC CH), and also on a panel discussion on cyber capacity building that included NCSC PNG.
- In the last year, FIRST hosted and supported 15 events including the FIRST Cyber Threat Intelligence Conference, CVE–FIRST VulnCon 2025, the September APNIC–FIRST Technical Colloquium at APNIC 60, and the FIRSTCON25 held in Denmark.

Awareness-raising

FIRST community trainers have supported training workshops and capacity-building initiatives involving PaCSON members and Pacific partners, including at the September 2025 ITU Regional Cyber Drill for Asia and the Pacific Region, as part of the Women in International Security and Cyberspace (WiC) Fellowship workshops ahead of the February and July 2025 UN OEWG sessions.

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 2026.

In June 2025, FIRST launched the FIRST CORE sponsorship initiative to expand the impact of the FIRST community and capacity-building activities, including with the Pacific:

<https://www.first.org/global/core/>

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



Friends Updates



Cyber Safety Pasifika

Cyber Safety Pasifika (CSP) has supported Pacific police in the global fight against cybercrime since 2011. CSP is the Pacific Islands Chiefs of Police (PICP) cybercrime training partner of choice and a signatory to the Declaration of Partnership signed in 2023 by the 22 Chiefs.



CSP delivers face-to-face cybercrime training, bringing Pacific police from multiple Pacific nations together to share knowledge, resources, experience and build relationships and networks.

The CSP programs are complementary, helping Pacific police reduce the effects of cybercrime on their communities and develop the capability to effectively investigate a wide range of cyber threats.

Achievements

CSP delivered the following training in 2025–26:

- Cook Islands in February 2025: Cybercrime Investigation Foundation (CIF) and Cyber Awareness Prevention & Education (CAPE). Participants from the following countries attended: American Samoa, Cook Islands, French Polynesia, Kiribati, Niue, Samoa, Tonga and Tuvalu.
 - In keeping with our philosophy of ‘by the Pacific, for the Pacific’, the CAPE course was presented by Sergeant Allen from Kiribati and Senior Constable Tatakura from the Cook Islands.
- Suva, Fiji, May 2025: CIF and CAPE was attended by participants from the following countries: Nauru, Solomon Islands, Vanuatu and members from the outer islands of Fiji – Nausori, Tavua, and Labasa. The CAPE course was presented by Officer Sitafine from American Samoa, Acting Supervisor Langi from Tonga and Tivalu from Samoa.
- At the request of the AFP – Timor-Leste Police Development Program, CSP provided a bilingual delivery of the CIF and CAPE programs to Timor-Leste police and the Pacific jurisdictions: the Northern Mariana Islands, the Federated States of Micronesia, the Marshall Islands, Kiribati and Timor-Leste. The CAPE course was presented by Sergeant Matapo from Cook Islands and Tivalu from Samoa.
- CSP is scheduled to deliver a CIF–CAPE program in the Solomon Islands in April 2026 and a CAPE workshop and program in Samoa in May 2026.
- Please refer to the Cyber Safety Pasifika website: <https://www.cybersafetypasifika.org>

Global Forum on Cyber Expertise – Pacific Hub

The primary constituency of the Global Forum on Cyber Expertise (GFCE) are the national governments, cyber-security authorities, CERTS, and ministries responsible for ICT, security, and/or digital transformation of Pacific countries and territories.



The broader beneficiaries of GFCE's work consists of the broader, multi-stakeholder cyber ecosystem that participates in and/or benefits from cyber capacity-building in the Pacific that includes, for example, regional organisations, private sector cyber security entities, and academia.

Achievements

GC3B and GFCE AGM, Geneva, May 2025

The Pacific Hub team attended the Global Conference on Cyber Capacity Building (GC3B) and the GFCE Annual General Meeting, engaging with key global stakeholders and donors to advance Pacific cyber security capacity-building priorities on the international stage. The Hub Director facilitated the panel on 'Regional Governance – Opportunities and Challenges in the Pacific' and supported DFAT and the GC3B Secretariat with organising travel logistics for 10 Pacific participants who featured across various panels throughout the event.



Figure 98: Mitchell Dunn (DFAT), Pua Hunter (GFCE), Pateli Vailea (Tonga), Esau Tupou (Tonga), Athena Matalavea (Samoa), Jobenz Manoa (Samoa)

GeekWeek, Ottawa, Canada

In June 2025, the Pacific Hub supported Canada with logistical arrangements for a nominated fellow from Fiji to participate in the Canadian Centre for Cyber Security's GeekWeek, a highly technical cyber threat intelligence sharing and analysis event. The participation strengthened relationships with the Canadian cyber security community and provided insights into emerging global cyber threats relevant to the Pacific region.

Pacific Cyber Week and P4C Conference, Nadi, Fiji

The Hub played a central role in supporting DFAT and the US Department of State in organising the flagship 'Pacific Cyber Capacity Building Coordination Conference (P4C)' that ran from 11 to 14 August, 2025, with sessions covering discussions on ransomware, operational security, AI, cybercrime, cyber diplomacy and more. The GFCE Pacific Hub Regional Meeting was held during the event where it featured the sessions on '*Strengthening Coordinated Approaches to Cyber Incident Management*' and '*Critical Infrastructure Protection Across the Pacific*'.



Figure 99: Suetena Loia (Samoa), Allan Cabanlong (GFCE), Cherie Lagakali (GFCE), Pua Hunter (GFCE), Alastair MacGibbon (Cyber CX)

Summer School on Internet Governance and International Law, University of Lodz, Poland

The GFCE Pacific Hub coordinated the participation of Pacific delegates from Tuvalu, the Federated States of Micronesia, Palau, and Fiji to the Summer School from 23 to 26 September, 2025. The overarching objective was to explore the intersection of satellite connectivity, disaster resilience, cyber security and digital policy with a particular emphasis on ‘Pacific realities and priorities’.



Figure 100: Melnguis Mesubed, Tenanoia Simona (Tuvalu), Berna Akcali Gur, Pua Hunter (GFCE), Joanna Kulesza, Minoru Stephen (FSM), Swaran Ravindra

Singapore International Cyber Week, Singapore

During the week, held from 20 to 23 October, 2025, the Pacific Hub Director served as a panellist on the Southeast Asia regional panel, ensuring that Pacific small island state perspectives were meaningfully represented alongside larger economies.



Figure 101: Keith Detros (Tech for Good Institute), Ghislain De Salins (World Bank), Masao Shino (Japan), Pua Hunter (GFCE), Filipe Beato (World Economic Forum)

‘Strengthening Pacific Cyber Resilience’, online webinar

The Pacific Hub organised and delivered a webinar on 12 November, 2025, featuring Co-Founder and Director of CI-ISAC Australia, Scott Flower, introducing the concept of cyber threat intelligence fusion and the national shared services and ISAC model to Pacific stakeholders across government, NGOs, civil society, and the private sector. The webinar focused on shifting from reactive to preventative cyber security approaches, particularly for small and medium enterprises and CERTs.

Awareness-raising

GFCE publishes the Global Cyber Expertise Magazine, a multi-stakeholder publication centred on cyber capability. It published the 13th issue in May 2025. GFCE also contributes to news articles and announcements on cyber security initiatives.

Pacific Fusion Centre

The Pacific Fusion Centre (PFC) delivers training and strategic analysis against priorities identified by Pacific Islands Forum (PIF) Leaders in the 2018 Boe Declaration on Regional Security. Our beneficiaries are PIF members as well as the following regional organisations identified in our Charter:



- Pacific Islands Forum Secretariat
- Secretariat of the Pacific Regional Environment Programme
- The Pacific Community
- Pacific Islands Forum Fisheries Agency
- Pacific Immigration Development Community
- Pacific Islands Chiefs of Police (including the Pacific Transnational Crime Network)
- Oceania Customs Organisation
- Pacific Islands Law Officers Network
- Asia Pacific Group on Money Laundering
- Pacific Cyber Security Operational Network
- Pacific Tourism Organisation
- Pacific Aviation Safety Office.

Achievements

The PFC offers practical training to Pacific security officials and produces strategic assessments that assist Pacific decision-makers respond to regional security challenges. What we deliver includes:

- Hosting secondees from across forum member states and providing training, mentoring, and regional engagement opportunities that enhance analytic and thematic skillsets. In 2026, the PFC welcomed its first cohort of secondees to the Pacific Analyst Program, as well as an intake of senior analysts dedicated to PFC productivity.
- Providing a range of domain awareness resources to build situational awareness across the Pacific, including media monitoring and Maritime Domain Awareness portal, Maritime Intelligence Risk Suite (MIRS). In 2026, PFC has also drawn in dedicated Maritime Domain Awareness analysts providing coordination and situational awareness across the Pacific.
- Engaging with Pacific Islands and regional organisations to develop shared and aligned efforts on Boe Declaration security priorities to avoid duplication of effort.
- Fostering a culture of regional information-sharing, in line with the Principles of Regional Information Sharing agreed at the Regional Security Information Sharing Workshop (Honiara, April 2018).

Awareness-raising

- Conducting research across a variety of open-source and authorised unclassified materials to produce a suite of strategic assessments that support Pacific security decision-making, as well as bespoke strategic assessments on request by PIF members. In 2026, PFC published major assessments such as the 2026 Pacific Security Outlook Report.
- Centre assessments are available to PFC beneficiaries only, and are available via the PFC online portal. The Pacific Security Outlook Report contains assessments on cyber security and is the only publicly available assessment from the PFC. It is available on the public-facing section of the PFC online portal and the PIF Secretariat website.



Working Group Updates



Awareness Raising Working Group

The **Awareness Raising Working Group (ARWG)** is responsible for raising awareness on behalf of the PaCSO^N community. The purpose of the working group is to advocate the PaCSO^N Vision and Mission on behalf of the community. Since the establishment of PaCSO^N in 2017, the ARWG serves the primary objective of acting on behalf of the PaCSO^N community and taking the lead on the following key initiatives:

- to increase cyber security awareness in all PaCSO^N member nations
- to increase regional collaboration among Pacific Island Countries for security information-sharing
- to increase awareness and collaboration with international partners to combat cross-border or transnational cybercrime activities
- to work effectively with the PaCSO^N Secretariat, PaCSO^N Capacity Building Working Group, and the PaCSO^N Communication Working Group on PaCSO^N operations.

2025 activities

For the reporting period, the ARWG proudly continued to support the various awareness-raising initiatives of PaCSO^N, its members and the wider Pacific cyber community. In the PaCSO^N AGM 2025, the working group decided to change the campaign period from 1 year to 2 years. This will allow one year for the creation, design and launch of a new campaign, proceeding to an extra year to allow for effective promotion and socialisation of the campaign materials.

The Cyber Up Pacific resources will continue to be used as complementary and supplementary awareness packs. A Signal group chat for ARWG was created after the AGM to increase engagement, information sharing and collaboration



Capacity Building Working Group

The goal of the **Capacity Building Working Group (CBWG)** is to identify practical steps that PaCSO^N members can take to strengthen their cyber security capability and capacity, as well as to identify ways in which other PaCSO^N members may contribute support.

A key objective of this group is to ensure that PaCSO^N members have the necessary mechanisms, contacts, and plans in place so that, in the event of a serious cyber security incident, each member can effectively cooperate and collaborate. This includes empowering members to share cyber security threat information, tools, techniques and ideas.

2025 activities

In 2025, a key part of PaCSO^N was the CBWG. Over the years, we have seen the implementation of various initiatives and the growth in members' capacity, which has contributed to their respective national efforts.

To help shape future efforts in the Pacific, in light of the increasing number of partners seeking to engage in capacity-building, members agreed to establish the Capacity Building Working Group Three-Year Action Plan. This plan signals priority areas of need at the Pacific regional level.

CBWG convenors presented the action plan to PaCSO^N members at the PaCSO^N AGM in Kiribati, highlighting the 5 pillars that will guide efforts to build capacity in the areas that matter most to our members and chart a tangible and measurable path forward.

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

Capacity Building Working Group membership:

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



Figure 102: CBWG Members Meeting in Wellington, New Zealand, hosted by NCSC NZ 9–13 June 2025

Communications Working Group

The aim of the **Communications Working Group (CWG)** is to improve information-sharing and the communication tools used by the PaCSO community. During the life of the CWG, its members work towards achieving a collection of tools and processes that enable better communication and information sharing within the PaCSO community.

Leading the CWG through their roles as co-convenors are the PaCSO Secretariat and Solomon Islands SIG ICT Services. The co-convenors work together and are responsible for improving communication outlets and information-sharing processes.

2025 activities

In 2025, the CWG was proud to publish the PaCSO Annual Report 2024 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 it to be a valuable resource for the community. The 2024 report was PaCSO's largest to date – covering 128 pages of updates, case studies and photos of cyber security as it happens across our Pacific!

In addition to publishing the report, the CWG is also pleased to have published 2 news articles over the course of 2025.

The articles focused on the PaCSO delegation that attended the 2025 Annual FIRST Conference in Copenhagen, Denmark, and the 2025 PaCSO AGM, hosted on Kiritimati Island, Kiribati. These articles serve the purpose of publicising the important work that PaCSO does, along with promoting awareness of key initiatives delivered by our members and partners.

The CWG continues to maintain and sustain the PaCSO website, pacson.org. In 2025, the website continued to be a central source of cyber security news and information. The website provides the PaCSO 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 pacson.org through organic searches.

Sharing merchandise and promotional materials to PaCSO members was a highlight for the working group in 2025. Being able to support the awareness-raising and capacity-building initiatives of members by providing them with physical materials is one way that safe cyber messages can be spread further. CWG is thrilled to see how these materials were used and shared through the updates provided by members for this report.



The PaCSO CUP continued to be a valued feature of the program's awareness-raising and capacity-building repertoire in 2025. This material continued to be a powerful tool designed to enhance the existing PaCSO priorities of information-sharing, awareness-raising and capacity-building. Supporting members to use the CUP materials to enrich their existing national awareness-raising efforts, the CUP seeks to enable users with an understanding of how to protect themselves, their family, their workplaces and communities by being secure online.

The PaCSO Signal group chat continued to be a mainstay for real-time communication among all community members. The chat encourages the PaCSO community to share with alerts and advisories, as well as to seek answers to questions, advice or anything else that can be shared or asked of a like-minded community. This more informal means of interaction has promoted increased cooperation and communication within PaCSO. In 2025, the chat experienced 41 advisories being shared and 7 general news links. These real-time interactions can assist to improve awareness and promote near instant insights into the wins, challenges and crises that Pacific cyber infrastructure is experiencing.

An exciting addition to the CWG in 2025 was the introduction of the PaCSO Community Newsletter.

Published to the PaCSO Community on a quarterly basis, 2 newsletters were published in 2025 (Q2 and Q4). This newsletter hopes to be a new and engaging way for the PaCSO community to receive and digest the latest updates, news, and content. The newsletter will include various opportunities for engagement, capacity-building and networking across the Pacific region and further through the global cyber and incident response community. In drafting, everyone within the PaCSO community is encouraged to provide input and suggestions on content.



To enhance the newsletter, and draw a reader's attention to specific sections or highlight a point of importance, the CWG took the PaCSO turtle logo and brought it to life using the power of AI. Meet **Pacifico!** This little turtle is a character you will now associate with the newsletter and is another way the CWG hopes readers will identify and increase engagement with PaCSO.



The CWG continues engaging with the Awareness Raising Working Group and the Capacity Building Working Group in their efforts to uplift PaCSO^N members throughout 2025, and looks forward to continuing collaboration into 2026. Outcomes for CWG in 2026 will include:

- reinvigorating the PaCSO^N Remote Session Series
- continuing to publish newsletter items that promote the innovative approaches of the community to enhance nations' cyber security and digital prosperity across the Pacific
- increasing the amount of news articles published on pacson.org to promote the incredible ways that the community achieves its collective mission of working together to develop cyber security incident response capabilities.

The CWG welcomes the opportunity to engage with the newly formed PaCSO^N Women in Cyber Security Working Group, and offers the communication tools currently available as a means to amplify its messages, and further promote the important role that women and individuals from diverse backgrounds have in shaping the cyber security landscape of the Pacific.

Partners Working Group

The **PaCSO^N Partners Working Group (PPWG)** was established with the aim of providing PaCSO^N partners with opportunities to support and collaborate with the PaCSO^N working groups. The PPWG is driven by the aspiration to provide a whole-of-community benefit to PaCSO^N, working with all PaCSO^N members to increase knowledge, capacity, and resilience in matters of cyber security.

2025 activities

Throughout 2025 and beyond, the PPWG will continue to support the PaCSO^N community to deliver against the mission of working together across the Pacific to develop 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 PaCSO^N partners to help realise these goals is highly valued, and is an effective mechanism for success.

Efforts by CCCS to support PaCSO^N's attendance at GeekWeek, hosted in Ottawa from 28 May to 6 June, 2025, was an exciting evolution in the partnership. GeekWeek brought together over 300 participants from 105 organisations across 16 countries. The theme, 'Demystify Cyber Security', focused on practical collaboration to tackle emerging threats. Participants worked on 37 projects, including:

- cyber threat hunting and analytics
- operational technology security for energy systems
- malware detection and decoding

- cloud security monitoring and scaling
- open-source cyber tools development.

These projects offered exposure to turnkey solutions, community toolkits, and open-source platforms that can be adapted without heavy resource investment. GeekWeek's collaborative model of blending experts in diverse teams helps participants learn advanced techniques while building trusted networks for future incident response.

This engagement marked a milestone of Canadian capacity-building support with PaCSON.

From 22 to 27 June, 2025, PaCSON and FIRST collaborated to support attendance by Pacific delegates at the FIRSTCON25 in Copenhagen, Denmark. The conference was conducted over 6 days and included networking opportunities, presentations and various workshops. Throughout the event, PaCSON representatives engaged in a variety of workshops, presentations, and lightning talks. This included presentations from Ukraine, Switzerland, Spain, Japan, Australia, New Zealand, the US and the UK. Topics included digital forensics, incident response, case studies, AI and many more.

Throughout 2025 and beyond, the PPWG will continue to support the PaCSON community to deliver the mission of working together across the Pacific to develop 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.

Pacific Women in Cybersecurity Working Group

The **Women in Cybersecurity Working Group (PWICWG)** is responsible for nurturing and developing PaCSO^N women and allies through training and development, supporting current and incoming women within the PaCSO^N community, and linking the PaCSO^N community with Pacific and industry cyber women.



2025 activities

In 2025, the PWICWG was officially launched, at the PaCSO^N AGM, in memory of the late Georgina Kiele, who was a strong advocate for women in cyber.

2026 is the first year of this working group and the members have discussed exciting opportunities the PWICWG can make use of in support of existing programs and the other PaCSO^N working groups. Consideration is also being given to ways the PWICWG can drive new initiatives to support the PaCSO^N community and broader Pacific.



Figure 103: The PWiC is currently represented by Fiji, New Zealand, Papua New Guinea, Samoa, Tonga and Australia.



Progress Reporting



PaCSO Priorities

Reflections and future plans

PaCSO continues to progress action items aligned to the 2024–25 priorities, as follows.

1. Solidify PaCSO’s position within the regional architecture through formalising its status as a regional body

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

Status	Ongoing
Actions	- PaCSO has established a position within the PIF Thematic Action Group on Peace and Security. In this role, PaCSO informs the broader regional architecture of current and long-term cyber security trends. - Efforts to advocate on behalf of the PaCSO community continued at the Pacific Cyber Capacity Building and Coordination Conference (P4C) 2025.

2. Increase engagement opportunities internally and externally

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

Status	Ongoing
Actions	- CWG convenors introduced the quarterly PaCSO Newsletter as another means to communicate with the community. - CCCS facilitated fellowship support for PaCSO delegates to attend the GeekWeek events in Ottawa, Canada. - PaCSO facilitated fellowship support for PaCSO delegates to attend the FIRSTCON25 in Copenhagen, Denmark. - The CBWG launched the PaCSO Capacity Building Action Plan. This is the key guiding framework for developing and delivering cyber capacity-building initiatives in the region.

3. Encourage information-sharing and confidence to seek assistance

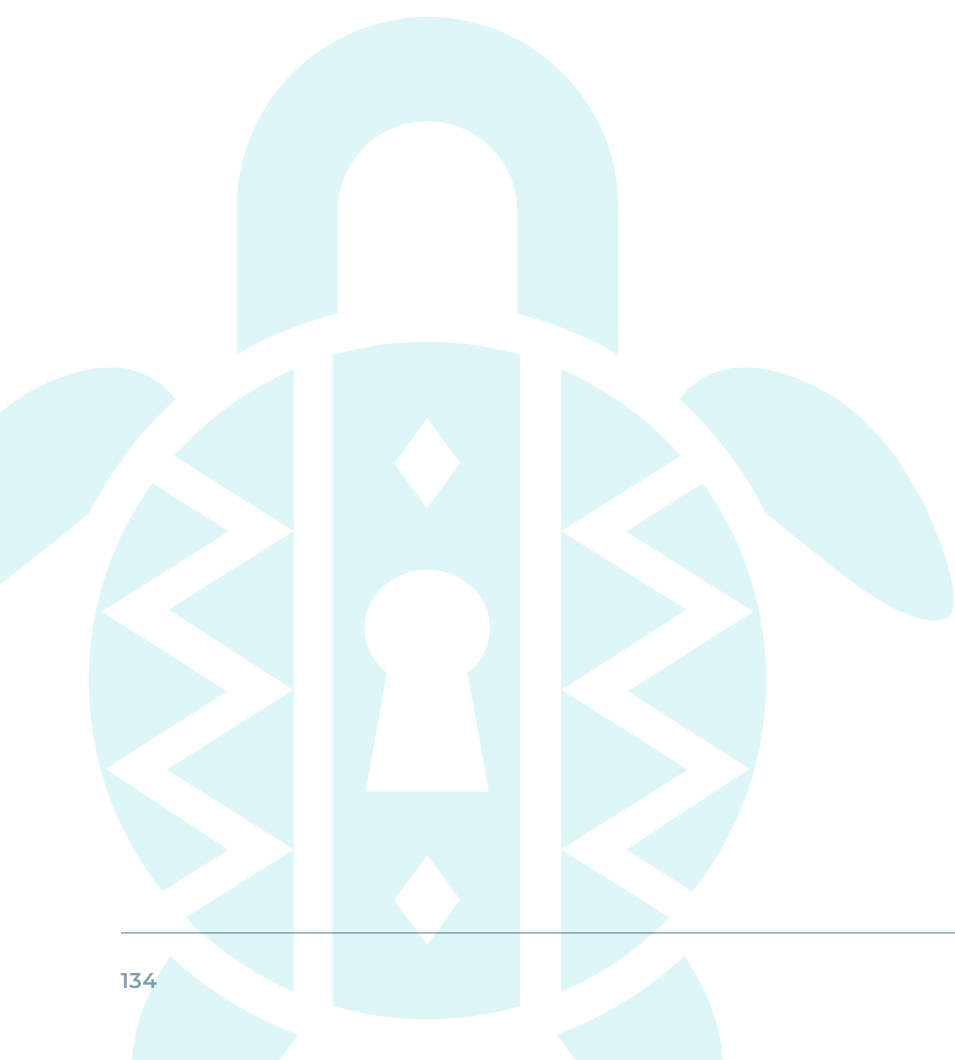
Further establish PaCSO^N as a safe and open environment to share information, enabling members to learn from one another and share key insights to increase the region's capabilities and cooperation.

Status	Ongoing
Actions	▪ The Secretariat and community shared alerts and advisories to the Signal group chat to allow members to safely 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. ▪ The AGM TLP:RED session continued to be refined to ensure its relevance and usefulness to participants.

4. Implement a comprehensive PaCSO^N monitoring and evaluation framework

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

Status	Ongoing
Actions	▪ Efforts are underway to understand the priorities and work programs of all elements of the PaCSO^N program, including working groups, partner engagement, and fellowship opportunities.





2025 Financial Statement



As outlined in the 2024–25 priorities, PaCSO^N members and the PaCSO^N Executive Committee wish to make public the financial commitments made by members, partners, friends, the Secretariat and other relevant stakeholders. The intention behind this is to increase the transparency of the network, and enable members to understand the commitments made by those who are invested in the network. Below is a list of stakeholders and their financial contributions to PaCSO^N for the period 2024–25. Please note, some stakeholders were unable to publish their financial commitments due to internal organisational constraints.

All figures are in Australian dollars.

PaCSO^N Secretariat

1,051.90	Annual account subscriptions – communications and feedback services
14,586.00	PaCSO ^N website management – annual service charge for content updates, enhancements and security updates to pacson.org
182,258.48	PaCSO ^N 2025 AGM – delivered and facilitated 2025 AGM, Kiribati
94,914.00	FIRST Conference 2025 Fellowship – supported 3 PaCSO ^N members to attend FIRST Conference, Denmark
179.97	Merchandise shipping costs – shipment of PaCSO ^N merchandise

292,990.35 Total

Australian Cyber Security Centre

48,821.14	Training–Nauru and Kiribati (March 2025)–by ACSC Incident Response team
73,150.00	Training–Federated States of Micronesia (May 2025)–by ACSC Incident Response team

121,971.14 Total

Canadian Centre for Cyber Security

20,400.00	Geekweek fellowship–travel and participation costs for a PaCSO ^N member to attend
-----------	--

20,400.00 Total

Government of Kiribati

2,885.80	Grand Opening Lunch–minister-hosted, 2025 AGM, Kiribati
5,700.00	Official Dinner–as host, 2025 AGM, Kiribati
7,797.20	Saturday Cultural Program–funded cultural experience program, 2025 AGM, Kiribati
3,508.00	Dinner at Tabontekeeke–provided networking, 2025 AGM, Kiribati
6,600.00	Farewell dinner–provided farewell before departure, 2025 AGM, Kiribati
20,136.00	Operational cost for AGM–daily and transport costs for advance team to Kiritimati Island

46,627.00 Total

481,988.49 Grand total



Acknowledgements



Acknowledgements

PaCSO^N acknowledges the valuable contributions made by all of our collaborators and partners. The PaCSO^N community is very grateful for the advice, contributions and support of all the government organisations, NGOs, private enterprises and academic bodies who work with our network.

This report and the activities of PaCSO^N are made possible thanks to the support and advice of many individuals and organisations. The Executive Committee, on behalf of the PaCSO^N community, would like to thank everyone who contributed to PaCSO^N in 2025, with special thanks to the following.

Canadian Centre for Cyber Security (CCCS)

The Canadian Centre for Cyber Security (the Cyber Centre) is part of the Communications Security Establishment Canada. It is the single unified source of expert advice, guidance, services and support on cyber security for Canadians.



To learn more, please visit: <https://www.cyber.gc.ca/en>

Government of Kiribati

The Government of Kiribati works as a team to look directly at the needs of the people.

To learn more, please visit: <https://www.president.gov.ki/>



ASIA PACIFIC COMPUTER EMERGENCY RESPONSE TEAM (APCERT)

APCERT cooperates with CERTs and CSIRTs to ensure internet security in the Asia-Pacific region, 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/>

PACIFIC ISLANDS LAW OFFICERS NETWORK (PILON)

The 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 to review progress across all work streams, share best practice and plan future initiatives.



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

GLOBAL CENTRE FOR CYBER EXPERTISE (GFCE), 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/>

CYBER SAFETY PASIFIKA (CSP)

CSP is a program led by the Australian Federal Police 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: <https://www.cybersafetypasifika.org/>

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE (DFAT)

Between 2016 and 2024, under the Cyber and Critical Tech Cooperation Program (CCTCP), DFAT funded 156 cyber cooperation and capacity building initiatives worth \$71.9 million in 24 ODA-eligible countries throughout the region to uplift cyber resilience in the region.

DFAT has refocused CCTCP into the Southeast Asia and Pacific Cyber Program (SEA-PAC Cyber) in order to provide more targeted, impactful and sustainable capacity-building initiatives for enduring cyber resilience in Southeast Asia and the Pacific, and so ensure regional governments are better positioned to prevent and respond to cyber incidents.

Under SEA-PAC Cyber, DFAT continues to support partner countries to build and enhance their cyber-capacity, including:

- partnering with the US in Palau to provide support following cyber incidents in early 2024. Australian support includes a vulnerability assessment on key parts of Palau's Government network and provision of a private sector expert as a Cyber Security Adviser
- delivering cyber security exercises in countries across the Pacific and Southeast Asia, to improve incident response resilience and the knowledge and capability of participating governments
- strengthening cyber capability in Laos, through partnering with its government, to enhance cyber incidence response, uplift cyber awareness and training of its workforces, and build cyber security resilience
- supporting women from across the Indo Pacific to attend meetings of the UN OEWG.

PaCSO^N acknowledges the support and funding provided by the DFAT SEA-PAC Cyber.

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



Abbreviations

ACSC	Australian Cyber Security Centre
AGM	Annual General Meeting
AI	Artificial Intelligence
ANSSI	Agence nationale de la sécurité des systèmes d'information
APCERT	Asia Pacific Computer Emergency Response Team
API	Application Programming Interface
APT	Asia Pacific Telecommunity
ARWG	Awareness Raising Working Group
ASD	Australian Signals Directorate
ASX	Australian Stock Exchange
BEC	Business Email Compromise
CBWG	Capacity Building Working Group
CCCS	Canadian Centre for Cyber Security
CERT	Computer Emergency Response Team
CERT NZ	Computer Emergency Response Team New Zealand
CERT KI	Computer Emergency Response Team Kiribati
CI	Critical Infrastructure
CISA	Cyber security and Infrastructure Security Agency
CSAT	Cyber Security Awareness Team
CSP	Cyber Safety Pasifika
CSIRT	Computer Security Incident Response Team
CTI	Cyber threat intelligence
CTIS	Cyber Threat Intelligence Sharing platform
DFAT	Department of Foreign Affairs and Trade
DoS / DDoS	Denial of Service / Distributed Denial of Service
EC	Executive Committee
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
FY	Financial Year
GCSB	Government Communications Security Bureau
GFCE	Global Forum on Cyber Expertise
GICT	Girls in ICT Programme
ICT	Information and Communication Technology
IOC	Indicator of compromise
IoT	Internet of Things

ITU	International Telecommunication Union
MBIE	Ministry of Business, Innovation and Employment
MICT	Ministry of Information, Communications and Transport
MIRS	Maritime Intelligence Risk Suite
MoPC	Ministry of Policing and Communications
MSMEs	Micro, Small and Medium Enterprises
NCSC	National Cyber Security Centre
NDS	National Digital Strategy
OSC	Online Safety Commission
PaCSON	Pacific Cyber Security Operational Network
PFC	Pacific Fusion Centre
PNG	Papua New Guinea
PPWG	Partners Working Group
RBF	Reserve Bank of Fiji
RDP	Remote Desktop Protocol
SSH	Secure Shell
SOC	Security Operations Centre
TLP	Traffic Light Protocol
UN	United Nations
WG	Working Group

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