



PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

ANNUAL REPORT 2022





TLP:CLEAR = Disclosure is not limited.

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

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

CONTACT DETAILS AND FEEDBACK

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

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

PACSON 2022 ANNUAL REPORT



Contents

| | |
|--|-----------|
| From the Chair | 1 |
| Program Overview | 5 |
| PaCSO^N 2022 Annual General Meeting | 9 |
| Member Updates | 13 |
| Australia | 14 |
| Cook Islands | 19 |
| Fiji | 21 |
| Kiribati | 23 |
| Nauru | 25 |
| New Zealand | 27 |
| Papua New Guinea | 37 |
| Samoa | 42 |
| Solomon Islands | 44 |
| Tokelau | 48 |
| Tonga | 50 |
| Tuvalu | 54 |
| Vanuatu | 56 |
| Partner Updates | 59 |
| Cybersecurity and Infrastructure Security Agency | 60 |
| Federal Bureau of Investigation (FBI) | 67 |
| Reserve Bank of Fiji | 68 |
| Working Group Updates | 69 |
| Awareness Raising Working Group | 70 |
| Capacity Building Working Group | 73 |
| Communications Working Group | 75 |
| Partners Working Group | 77 |
| Future Plans 2023 | 79 |
| Acknowledgments | 81 |

From the Chair



Welcome to the 2022 Pacific Cyber Security Operational Network (PaCSO^N) Annual Report. I am thrilled to warmly extend the thanks and appreciation from our PaCSO^N Community to our Stakeholders and Partners for their continued support and encouragement. While 2022 continued to sow uncertainty and strife throughout the global community, CERT Tonga has been privileged to hold the Executive Committee Chair of PaCSO^N. It is as the Chair that I am proud to present this report to you, containing considerations on our collective efforts as PaCSO^N during 2022.

PaCSO is a regional network of cyber security incident response professionals collaborating on best-practice information-sharing and developing incident response capability. Since its establishment in 2017, PaCSO has continued to grow and prosper partnerships numbers and also in the work that we undertake. Our PaCSO Community encourages development, shares cyber security information, enhances technical skills and knowledge, builds relationships with other cyber-related programs and progresses work through our 4 Working Groups: Awareness Raising, Capacity Building, Communications, and the PaCSO Partners. Together, we are contributing to strengthening the cyber security posture for our Pacific region.

My predecessor noted that cyber security is a complex recipe, with collaboration and cooperation as 2 key ingredients. Without these, tangible results for our Pacific community cannot be won. Relationships built on collaboration and cooperation continue to be crucial for achieving success; we are stronger together than we can ever be apart. The significance of our collective professional development and ability to respond to cyber events has positioned PaCSO as the focal point of cyber security coordination in our region. I feel incredibly blessed to have led our magnificent PaCSO Community. Cyber security is a growing matter of national significance for the Pacific nations, and as I reiterate the statements made by our 2020 and 2021 Chairs, I too am glad to witness such excellent cooperation among our blue continent community.

During 2022, our community continued to provide a vital resource for our region. The return of in-person engagements in the wake of COVID-19 restrictions did not diminish the reliance our communities have developed on the online environment that has become synonymous with the new century. New digital habits developed by our communities over the course of the pandemic have shown us that the PaCSO mission has become more important than ever.

In the last year alone, cyber threats against the Pacific region have increased dramatically in size, speed and sophistication. The current threat landscape across the Pacific is one of uncertainty and reaction. It is an environment where cyber criminals currently hold the initiative, and use it to dictate terms to sovereign nations. PaCSO is key to changing this dynamic, and together we can address the growing number of cyber threats affecting our region. By enabling cyber security officials to learn from each other and exchange ideas, we can regain our agency in the online domain, not have it dictated to us by insidious elements. Collaborating on cyber security is vital, as is ensuring the robust nature of our most valuable partnerships. By working together, we are ensuring that the cyber security capabilities and professional competencies that currently exist, continue to grow to protect our increasing reliance on cyber and digital mechanisms.

An open, free and safe cyber space is a goal shared by likeminded nations throughout the world, and the continued strength and resilience of the PaCSO Community reinforces the Pacific's commitment to that cause. From the simple act of sharing information on a recent incident, promoting our community awareness-raising initiatives to better prepare our citizens, to supporting capacity building activities to strengthen our defences, no action undertaken by our members is without value or positive impact.

The year 2022 welcomed the return of the in-person PaCSO Annual General Meeting (AGM) for the first time since the COVID Pandemic. This was an excellent opportunity for our community to reconnect in the physical world, and renew our friendships after conversing only through digital means for so long. I would once again like to take the opportunity to thank the people of Fiji for their hospitality in hosting the AGM, and for welcoming us all into their country. This event allowed members to present on some of the major cyber security challenges that had affected their nations over the past 12 months, sharing information, knowledge, and lessons learned from these events with the community. We also saw presentations from our PaCSO Partners, the Cybersecurity Infrastructure & Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the Reserve Bank of Fiji, as well as invited guests from the Asia Pacific Network Information Centre (APNIC), Meta, and the Global Forum on Cyber Expertise (GFCE).

I also wish to share my appreciation for our valued Stakeholders, who also contribute to the continued success of PaCSO. I would especially like to pass along my appreciation to the PaCSO Secretariat and the Department of Foreign Affairs and Trade's (DFAT's) Cyber and Critical Tech Cooperation Program who committed its support to PaCSO.

I believe that the last year has been another year of success and challenge for PaCSO. I wish to reflect on our achievements and give thanks to those in and around our PaCSO Community. As my time as the Chair of the PaCSO Executive Council draws to a close, I wish the very best of luck and dedicate my ongoing support to Vanuatu, the 2023 Chair for the Executive Committee. Finally, I wish our Community all the best for the remainder of 2023, and very much anticipate witnessing your future triumphs.

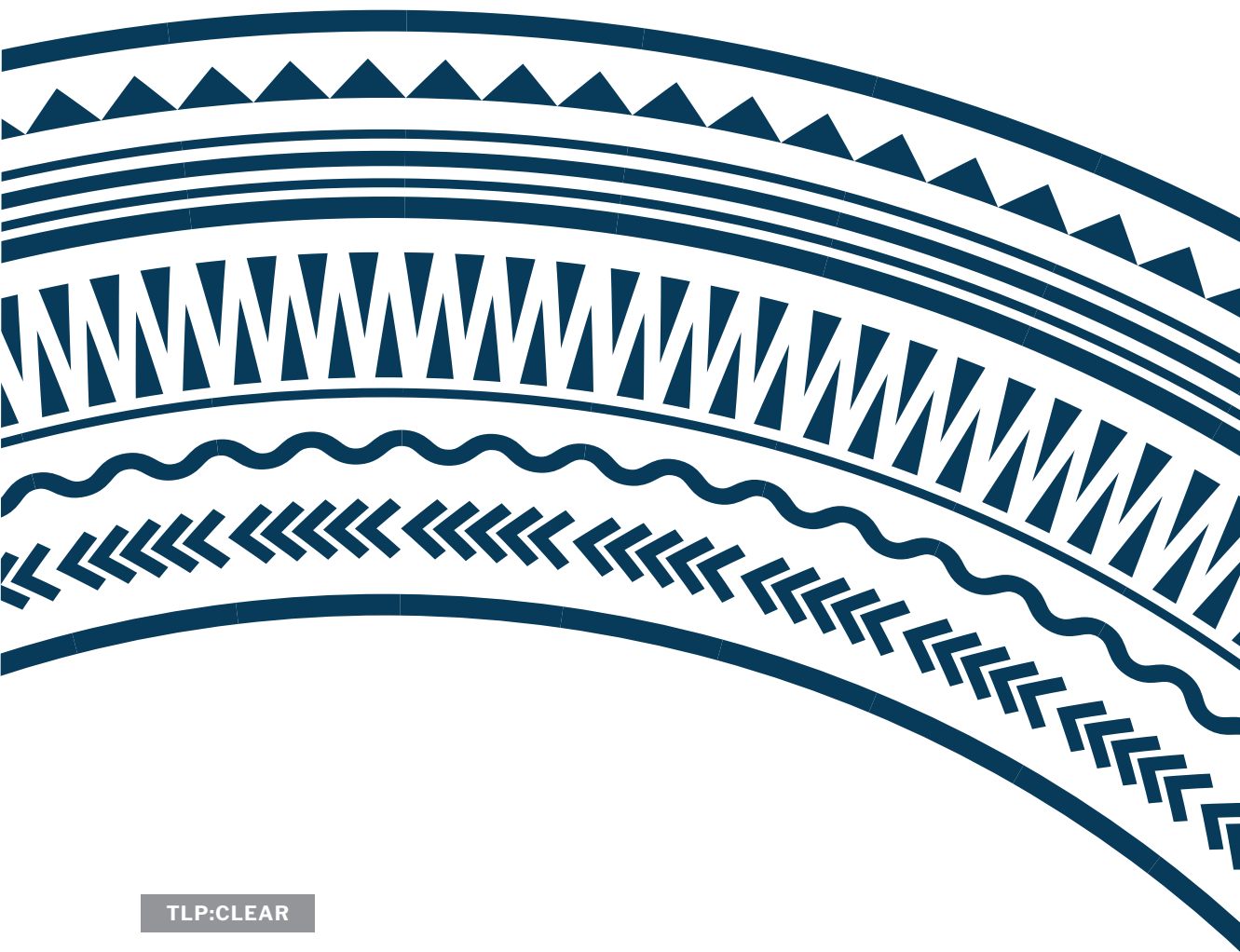


Ms Pelenita Milika Atoa
2022 PaCSO Chair – CERT Tonga

February 2023



Program Overview



Program overview

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

PaCSO is an operational cyber security network of regional working-level cyber security experts in the Pacific. PaCSO 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.

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

In support of PaCSO, partners – including other government organisations, not-for-profit organisations and academia – are able to join the network. The partner organisations to PaCSO include the Reserve Bank of Fiji (RBF), and the US's CISA and the FBI.

PaCSO is not a Computer Emergency Response Team (CERT) or 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 PaCSO is guided by the Executive Committee (EC), that provides leadership on behalf of the whole PaCSO Community. The EC is empowered to make decisions on behalf of PaCSO and is responsible for the management and direction of PaCSO. All PaCSO members are eligible to nominate for any of the EC positions.

The structure of the PaCSO^N EC included:

| | 2022 | 2023 |
|----------------|--------------|--------------|
| Chair | Tonga | Vanuatu |
| Deputy Chair | Cook Islands | Kiribati |
| Incoming Chair | Vanuatu | Cook Islands |

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

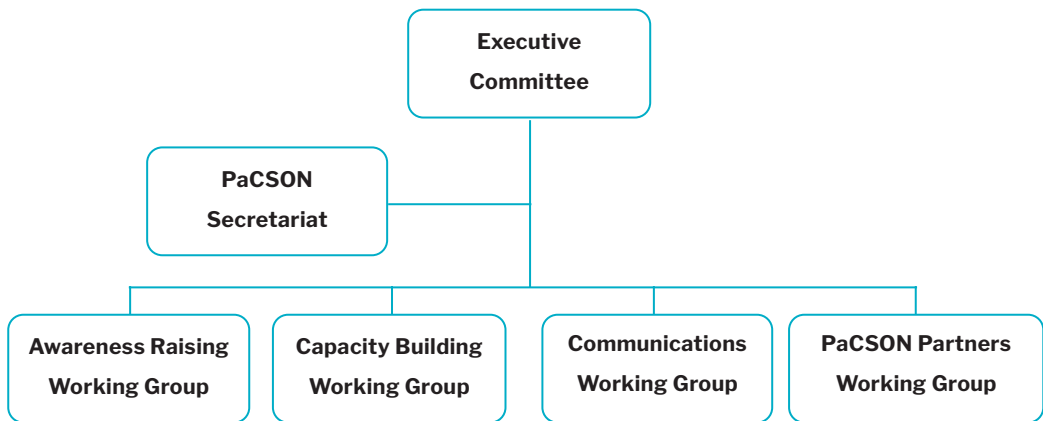


Figure 1. PaCSO^N Governance Structure.

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.



PaCSO^N 2022 Annual General Meeting



PaCSO^N 2022 Annual General Meeting

Every 12 months, the PaCSO^N Community comes together to celebrate and recognise its collective efforts, and plan for the coming year's activities. For the first time since 2019, the PaCSO^N Annual General Meeting (AGM) was held in person. Being able to come together after being separated for so long was an important opportunity to strengthen the PaCSO^N relationships and rekindle the trust and respect that underpins the success and impact of the network.



Figure 2. PaCSO^N 2022 Annual General Meeting attendees.

The event was hosted from 18 to 22 September 2022 in Suva, Fiji, and was well attended by the PaCSO^N Community with the inclusion of invited guests supporting the event as part of the opening ceremony.

During the week-long program, some of the events included:

- Participating in the Cyber Security Information Exchange. This was a chance to share lessons learned by individual nations with their neighbours in an effort to strengthen the wider Pacific cyber landscape and increase PaCSO^N's collective understanding of the issues facing the region.
- Workshops from PaCSO^N Partners and Members. These covered a range of topics within the cyber security domain that presenters specialise in, and that have a direct impact on the Pacific region.

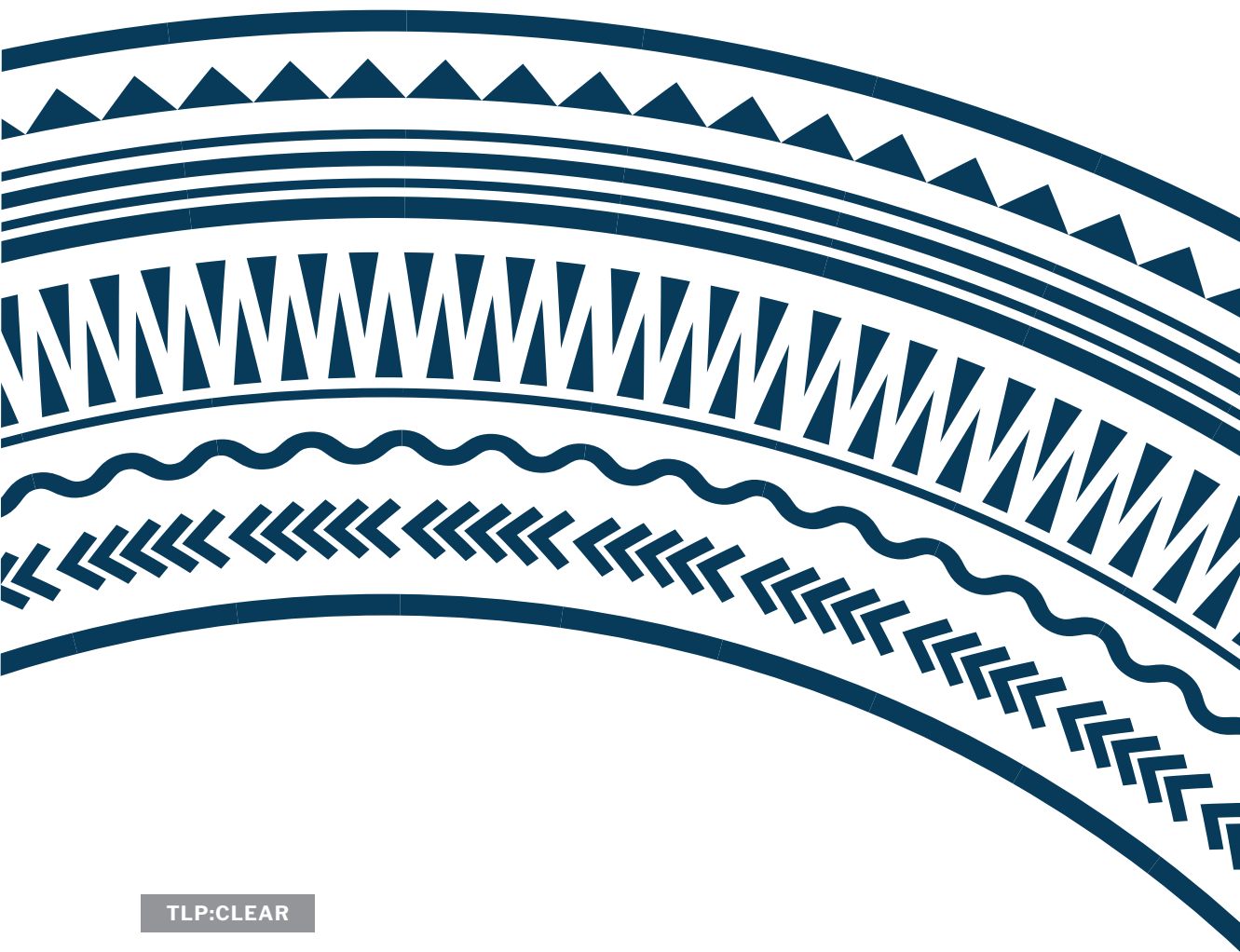
- Capacity-building activities. These support new skills development for PaCSO^N Members and included an exercise that focused on the importance of communicating clearly, regularly and concisely during a cyber security incident.
- Endorsing the new cyber e-learning program, the Cyber Upskill Program (PaCSO^N CUP). The PaCSO^N CUP is a module-based program that includes videos and learning packages aimed at all levels of the community, government and small businesses with the aim of supporting key tools and information to assist in increasing cyber literacy and creating a more cyber-resilient Pacific.

A notable achievement was celebrating the launch of the 2022 Cyber Smart Pacific Campaign. This included welcoming 4 new characters designed to support PaCSO^N's cyber awareness-raising efforts by providing memorable ways to link the close and enduring relationship the Pacific shares with its ocean environment. PaCSO^N looks forward to continuing to hold in-person events into the future, and to engage in further face-to-face engagement in 2023. The PaCSO^N 2023 AGM will be hosted in Port Villa by CERT Vanuatu.





Member Updates





AUSTRALIA



Australian Cyber Security Centre

The Australian Cyber Security Centre (ACSC) is based within the Australian Signals Directorate (ASD).

We provide advice and information about how to protect individuals, families and businesses online.

The ACSC's cyber security mission is supported by ASD's wider organisation. We lead the Australian Government's efforts to improve cyber security. Our role is to help make Australia the most secure place to connect online. The ACSC reports to the Minister for Cyber Security.

ASD is a statutory agency within the Defence portfolio which reports to the Minister for Defence. At the end of the 2021–22 financial year, ASD employed approximately 2,500 full-time equivalent staff.

The ACSC brings together cyber security capabilities from across Australian government agencies to improve the cyber resilience of Australian society.

The primary constituency for the ACSC includes:

- government agencies
- large organisations and critical infrastructure
- small and medium business
- individuals and families.

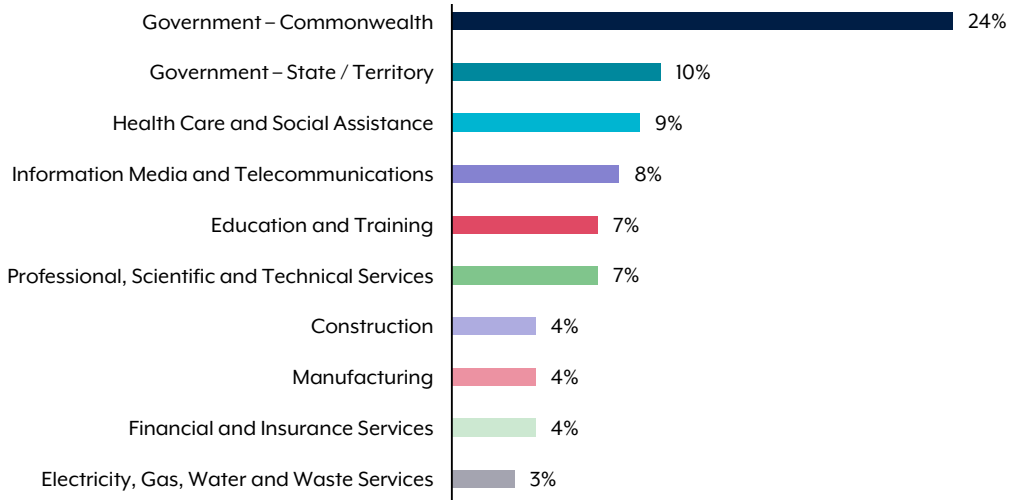


Figure 3. Cyber security incidents to which the ACSC responded in the 2021–22 financial year, top 10 industry sectors.

Threat landscape

Australians can report a cyber security incident or cybercrime via our ReportCyber website (www.cyber.gov.au), or by contacting the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).

The ACSC uses reported incidents to enhance national situational awareness of the cyber security environment in Australia, identify emerging trends, and support timely and tailored advice and assistance to Australian organisations.

The scale and sophistication of cyber threats to Australia and the Indo-Pacific is increasing. Australia cannot, and does not, act in isolation in addressing cyber threats. International partnerships create opportunities for information sharing, operational collaboration and support, and cooperation to build technical capacity.



Figure 4. Screenshot from the ACSC Annual Threat Report - What the ACSC Saw.

The top 5 most frequently reported cybercrimes in the 2021–22 financial year were:

- online fraud
- online shopping scams
- online banking scams
- investment scams
- business email compromise.

We monitor cyber threats across the globe 24 hours a day, 7 days a week, so we can alert Australians early on what to do. We provide advice and information on how to protect them and their businesses online. When there is a cyber security incident, we provide clear and timely advice to individuals, businesses and critical infrastructure operators. We work with our businesses, government and academic partners, and experts in Australia and overseas to investigate and develop solutions to cyber security threats.

In the 2021–22 financial year, the ACSC received over 76,000 cybercrime reports via ReportCyber, an increase of nearly 13 per cent from the previous financial year. This equates to one report every 7 minutes. Over the 2021–22 reporting period, medium-sized businesses experienced the highest average financial losses, averaging AU D \$88,407. The ACSC encourages the reporting of all cybercrime and cyber security incidents, via our ReportCyber website (www.cyber.gov.au).

The ACSC uses reported incidents to enhance national situational awareness of the cyber security environment in Australia, identify emerging trends, and supplying timely and tailored advice and assistance to Australian organisations.

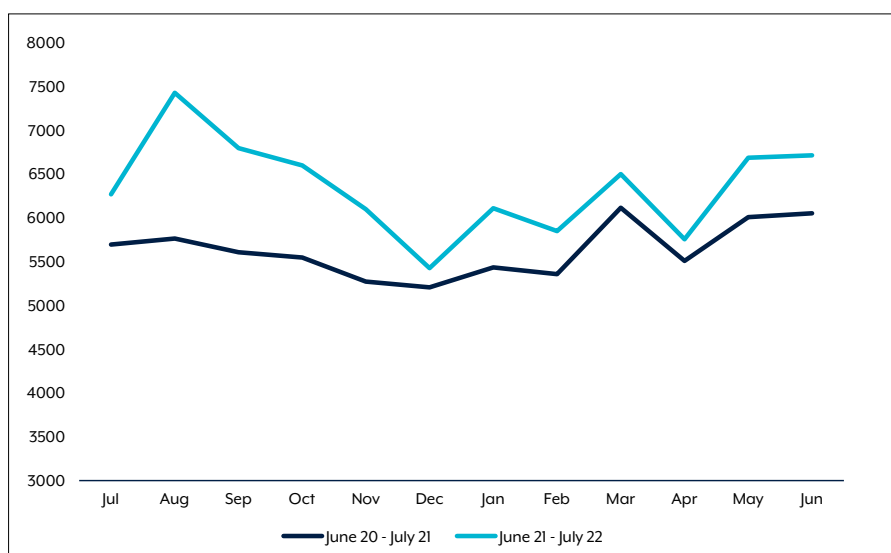


Figure 5. Cybercrime reports by month for financial year 2021–22 compared with financial year 2020–21.

Awareness raising

In 2022, the Act Now, Stay Secure Campaign ran from January to June 2022. The campaign sought to raise awareness of relevant cyber security threats, provide cyber security advice and educate users on simple cyber security practices. It also encouraged ACSC audiences to visit cyber.gov.au, as the trusted voice of authority for cyber security advice and support for individuals, businesses and organisations. The next phase of advertising for the Act Now Stay Secure Campaign is to be launched in 2023.

ACSC online learning resources are designed to provide users with practical, actionable approaches to prepare for, prevent, and respond to cyber incidents. They are tailored to each audience and in a format accessible to a diverse Australian community.

The ACSC produces several types of news, publications and advisories. These are all available on the ACSC website through the ‘view all content’ function.

In the 2022 calendar year, the ACSC released:

- 1 ACSC Annual Cyber Threat Report
- 24 news items
- 28 new publications and guidance
- 10 advisories
- 25 alerts.



Figure 6. Screenshots of products available on cyber.gov.au.

2022 CASE STUDY - RANSOMWARE INCIDENT

In April 2022, a New South Wales local council was impacted by a ransomware incident. The initial access occurred at least 2 weeks before the incident, with the malicious actor likely timing the incident to occur over the Easter long weekend.

The incident impacted a wide range of business operations for the council, including council minutes, employee financial data, and systems responsible for monitoring water quality. The incident also had a huge impact on council technology staff, who worked 40–80 hours overtime each week during the initial response.

Upon discovery, manual processes were immediately implemented to manage water-quality testing and level monitoring, and temporary servers were established within 24 hours to restore remote monitoring. The council engaged a commercial incident response provider, and its managed service providers (MSP) deployed additional capabilities. The ACSC provided advice to the council and warned ACSC Partners in the water sector to be alert to possible ransomware targeting.

The incident demonstrates the interplay between the ransomware, the operational technology, and the physical environment. The initial access through a legacy entry point impacted multiple systems, including operational technology systems. This meant council workers had to manually test water quality and levels following overnight rain. A swift response by the council, its MSP and the ACSC ensured there was no compromise of water or sewage services. The council's MSP continues to monitor the dark web for data leaks.

This case study demonstrates the importance of decommissioning legacy systems and/or erecting firewalls between them and operational technology systems.



COOK ISLANDS



Information, and Communications Technology (ICT) Division, Office of the Prime Minister (OPM)

Our organisation consists of 5 technical staff under the Director of ICT reporting directly to the Chief of Staff in the Office of the Prime Minister.

Threat landscape

Cyber incidents in the Cook Islands can be directed to the police, the Financial Intelligence Unit or to the ICT Division of the OPM.

For the Cook Islands, common types of cyber threats include:

- phishing
- email spam
- viruses
- malware.

Our division responds to cyber incidents by:

- filtering and informing users to block and delete spam emails
- quarantining viruses and malware and, if necessary, deleting and cleaning affected devices
- informing users to block and delete phishing attempts.

The ICT Division responds by deleting approximately 1,000 spams per month, cleaning at least 5 infected devices per month, and sends at least one email per month to all users informing them about phishing emails and what to do.

Awareness raising

For the Cook Islands, the ICT Division raises cyber safety awareness through a tablet training partnership with the Climate Change Office and a non-government organisation (NGO) focusing on our community in the Outer Islands including their schools. In the workshops, we promote the getsafeonline.org.ck website and our contacts in the event that if they think they are a victim of cybercrime, they know who to contact.





Ministry of Communications

There are 3 departments under the Ministry of Communications.

These departments are the:

- Department of Communications
- Digital Government Transformation Office
- Department of Information, Technology and Computing Services.

The Minister for Trade, Co-operatives, Small and Medium Enterprises, and Communications is the Hon Manoa Seru Kamikamica, with Mr Shaheen Ali as the Permanent Secretary, and Ms Tupou'tuah Baravilala as the Director-General for Digital Government Transformation, Cybersecurity and Communications.

Our primary constituencies are the Government and nation of Fiji.

Threat landscape

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

- Fiji Police Force
For more information refer website – <https://www.police.gov.fj/>
- Fiji Independent Commission Against Corruption (FICAC)
For more information refer to website – <https://ficac.org.fj/>
- Fiji Financial Intelligence Unit (FIU)
For more information refer to website – <https://www.fijifiu.gov.fj/>
- Online Safety Commission (OSC)
For more information refer to website – <https://onlinesafetycommission.com/>

The top 5 cyber security threats that faced Fijians in 2022 were:

- website defacement
- phishing
- malware and ransomware
- financial fraud or financial crimes, including pyramid schemes
- business email compromise.

The Ministry of Communications responds to cyber incidents that affect government networks and infrastructure. All events are thoroughly investigated and resolved.

Over the course of 2022, our ministry continued to experience and respond to several cases of misinformation, disinformation, fake news and malinformation, including related to COVID-19.

The *Cybercrime Act 2021* was passed by the Parliament of Fiji in 2021, which aligned Fiji to the Budapest Convention, and work is currently being undertaken to ascend Fiji to the Budapest Convention.

Work is also being undertaken to establish Fiji's CERT, as well as a review of the 2016 National Cybersecurity Strategy.

Awareness raising

Within the civil service, and also for the public, when launching national initiatives, cyber security is a core component in our communications and PR strategy.

Security advisories and awareness notices on critical vulnerabilities are also disseminated to government ministries and agencies on a regular basis to help improve awareness and promote safe cyber practices.



KIRIBATI



Ministry of Information, Communications and Transport (MICT)

The Digital Transformation Office (DTO) of the Ministry of Information, Communications and Transport (MICT) comprises 6 units, one of which is the National CERT which has three permanent staff being the Government Chief Information Security Officer, the Senior Information Security Analyst, and an Information Security Analyst.

The National CERT is housed within the DTO and is run by the Government National ICT Director who also oversees the other 5 units of the DTO. The DTO was established as part of a restructuring of all government ICT personnel who are now under the DTO. The Government Chief Information Security Officer will lead the National CERT and report to the National ICT Director. The National ICT Director reports to the Secretary of the MICT and the Honourable Minister of the MICT.

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

Threat landscape

Cyber incidents in Kiribati are most often reported to the ministry or National CERT via direct telephone calls, through law enforcement notification, and emails direct from victims.

The top 5 most common cyber security threats that face our population are:

- social media phishing attacks
- financial scamming online
- disinformation
- use of unlicensed cracked, malware, and ransomware infected software
- unpatched systems (vulnerable systems usage).

We do not have the formal capability to respond to cyber incidents; however, we provide responses to a limited extent where the cyber incidents are severe and on government networks, critical infrastructure and against service providers. The National CERT will greatly assist our ability to respond and provide advice on cyber incidents.

During the reporting period, the ministry continued to provide considerable support to the COVID-19 response for the Kiribati Government.

Awareness raising

The DTO and National CERT regularly provide cyber security and cyber safety awareness training. It is provided to schools via the ministry's Cybersecurity Awareness School Campaign, and to communities regarding cyber safety tips and best practices on staying secure on the internet. This effort is conducted annually.

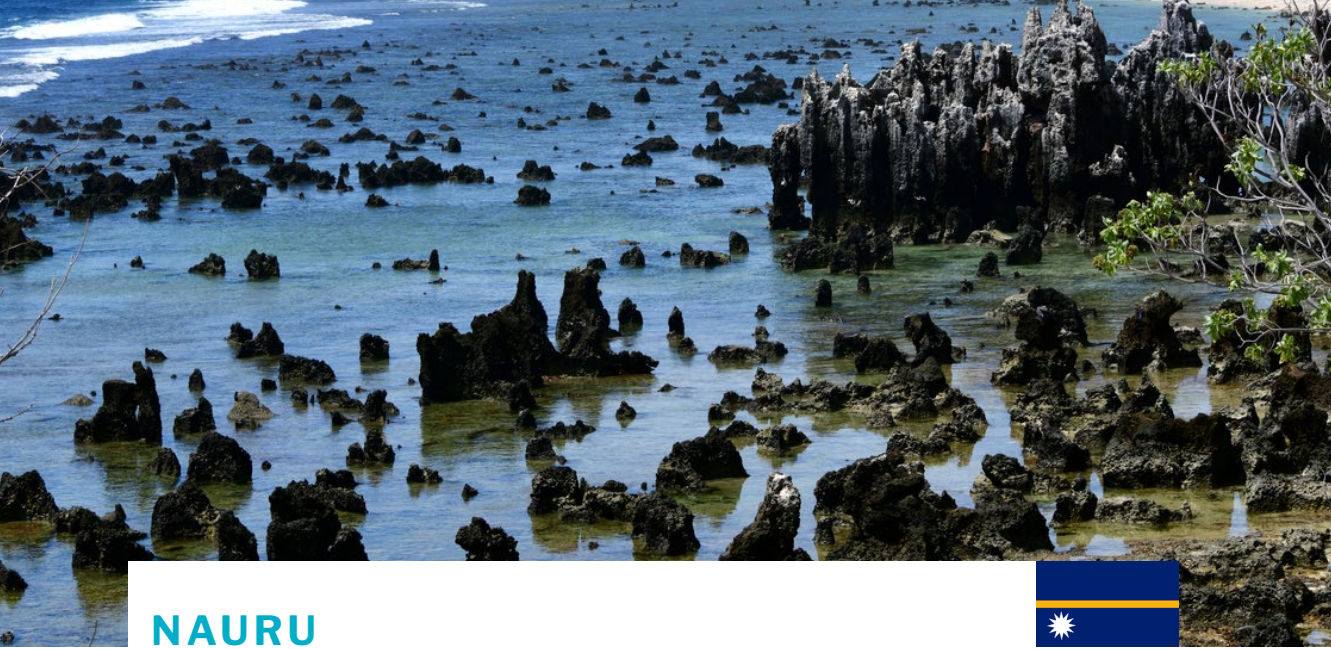
The MICT also hosts an annual MICT Day, where the DTO provides a focused awareness program on current and persisting cyber security issues.

Get Safe Online ambassadors are active in the Kiribati community and they aim to improve cyber awareness online. We have also published the PaCSON Cyber Smart Pacific Campaign on our website to assist in educating our citizens on ways to strengthen their personal cyber security.

The MICT provides advisories to government ICT professionals on cyber security issues. We also published national cyber security guidelines for government agencies. Email is our primary means of notification.

2022 CASE STUDY - 2FA

In 2022, the Kiribati Government began to roll out two-factor authentication (2FA) to specific government departments as part of a campaign to reduce security risk exposure in the face of increasingly sophisticated cyber attacks from a range of threat actors. This effort has greatly improved the government departments' abilities to reduce security risks.



NAURU



The Department of Information, Communication and Technology, Ministry of Telecommunications

The department currently has 22 staff members, plus 3 more if we include the head of the department, the minister and the deputy minister.

Threat landscape

Most of the citizens of Nauru report their cyber concerns directly to the Nauru Police Force through direct walk-ins, phone calls, or Facebook chat. Public service workers report to us (ICT) through either phone calls or emails.

Our most commonly reported cyber threats include:

- phishing
- identity theft (copying of Facebook accounts in order to impersonate a victim)
- hacked accounts (Facebook, IMO, etc.)
- scam emails getting through to government emails.

Awareness raising

ICT used the PaCSO Cyber Up Pacific information and materials to raise awareness to public servants during a Public Service Day Program held in November 2022. We are in the process of planning an awareness campaign that will start off with each department of the government and then slowly branching out into schools and communities using the PaCSO Cyber Up Pacific Program.

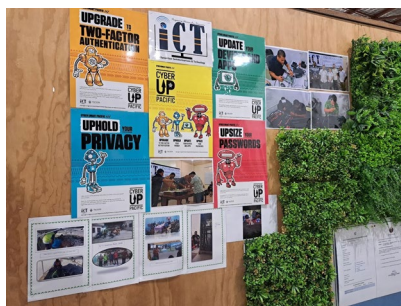


Figure 7. Awareness raising materials during the Public Service Day program.



NEW ZEALAND



CERT New Zealand

CERT NZ is a branded business unit within the Ministry of Business, Employment and Innovation. It has 35 staff, including operations, communications and engagement, governance, and analytical reporting. CERT NZ also has a contact centre to receive incident reports.

CERT NZ works to support businesses, organisations and individuals who are affected, or may be affected, by cyber security incidents. CERT NZ provides trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand.

Anyone can report a cyber security incident to CERT NZ, from members of the public, businesses, and government agencies to IT professionals and security personnel. We also receive incident notifications from our international incident response counterparts when they identify affected New Zealand organisations in their investigations.

CERT NZ also has a dedicated Pacific Partnership Team that works closely with Pacific incident response counterparts and the wider regional cyber community. The Pacific Programme delivers 2 primary activities which are business-as-usual (BAU) collaboration and standalone responsive programming.

BAU activities include:

- information and good practice sharing and development
- community development and engagement
- formal and informal mentorship activities
- direct incident response support
- community outreach

- contribution to PaCSON, including convenorship of the PaCSON Capacity Building Working Group
- support, advice, and contributions to New Zealand, regional, and global cyber capacity building.

Responses since January 2022 have included:

- the PaCSON Remote Session Series, with 9 sessions for 235 participants in 2022
- spearheading the development and delivery of the Cyber Smart Pacific Annual Regional Awareness Raising Campaign
- establishing the Pacific Data and Insights Project, with the Shadowserver Foundation, to provide localised data to each PaCSON Member
- support for the relaunch of Cyber Smart Samoa, led by SamCERT and MCIT
- in-country bilateral meetings and training with Vanuatu, Samoa and the Cook Islands
- sharing CERT NZ reporting templates
- collaboration with CERT Tonga on a Cybersecurity Workforce Development Program. See <http://www.cert.govt.nz> for more information.

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

The online tool can be accessed here:

- <https://www.cert.govt.nz/individuals/report-an-issue/> (for individuals and businesses)
- <https://www.cert.govt.nz/it-specialists/report-an-incident/> (for IT specialists)
- Full contact details are available here: <https://www.cert.govt.nz/about/contact-us/>

CERT NZ also has a Coordinated Vulnerability Disclosure Policy and Process. More information can be found here: <https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/>

Threat landscape

The top 5 incident categories in 2022 were:

- phishing and credential harvesting: 4315, up 16% on 2021
- scams and fraud: 2296, up 15% on 2021
- unauthorised access: 931, up 23% on 2021
- malware: 225, down 88% on 2021
- other: 217, down 21% on 2021.

Malware significantly decreased in 2022 due to large numbers of FluBot being reported and addressed in 2021.

Over the course of 2022, CERT NZ observed new techniques and tactics across many common scams including phishing, phone scams, online shopping scams and romance and investment scams. The increase in the success of these scams contributed to increased financial losses, with losses reaching the highest amount ever reported to CERT NZ in a single quarter: a staggering NZD \$8.9 million in Q3.

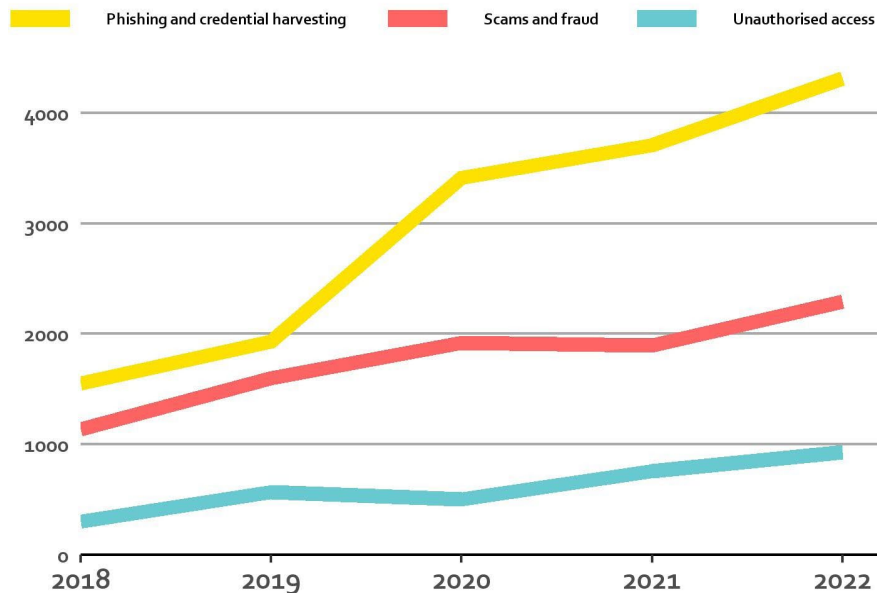


Figure 8. Over the course of 2022, Phishing is the most used tactic for cyber criminals, with scams and unauthorised access also on the rise.

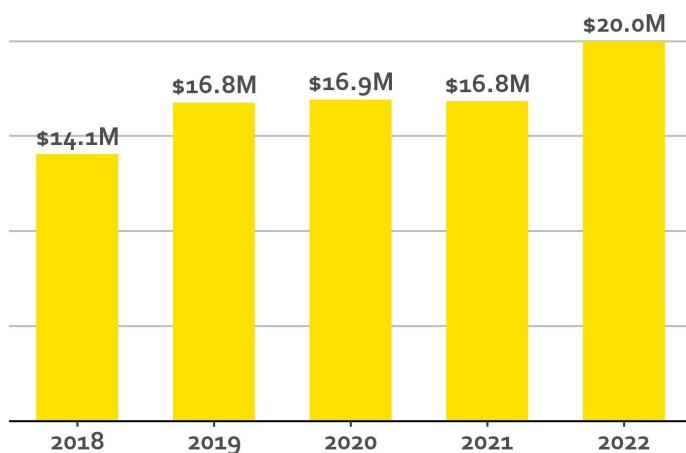


Figure 9. Of the reports received by CERT NZ in 2022, 22 per cent included a direct financial loss, with a combined total of NZD \$20 million.

CERT NZ responds to cyber security threats and issues in New Zealand. CERT NZ's core mission is supporting businesses, IT specialists and members of the general public with any form of cyber security incident.

This may include:

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

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

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

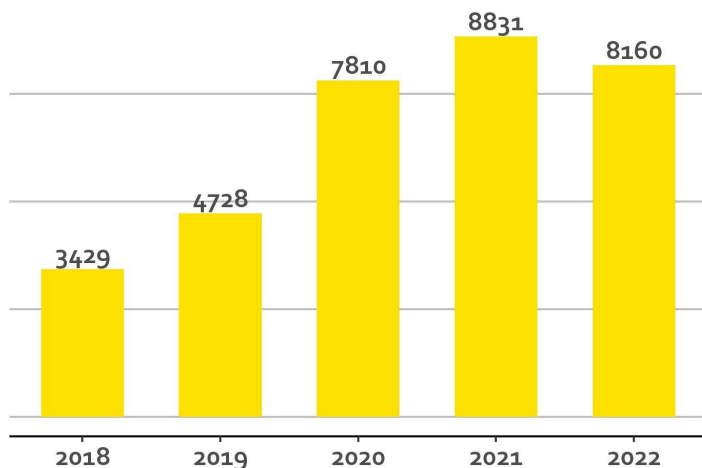


Figure 10. In 2022, a total of 8160 incidents were reported to CERT NZ, an 8 per cent decrease from 2021.

Awareness raising

As part of October International Cyber Awareness Month, CERT NZ supported the development and complete rebrand of the collaborative Cyber Smart Pacific Initiative. It is the third year CERT NZ has been a part of the initiative, through the PaCSON Awareness Raising Working Group.

In 2022 the Working Group, led by CERT VU, proposed and voted on themes, taglines, and materials, resulting in a revitalised regional campaign that included the launch of several local and regional websites and awareness efforts, and included numerous localised and translated banners.

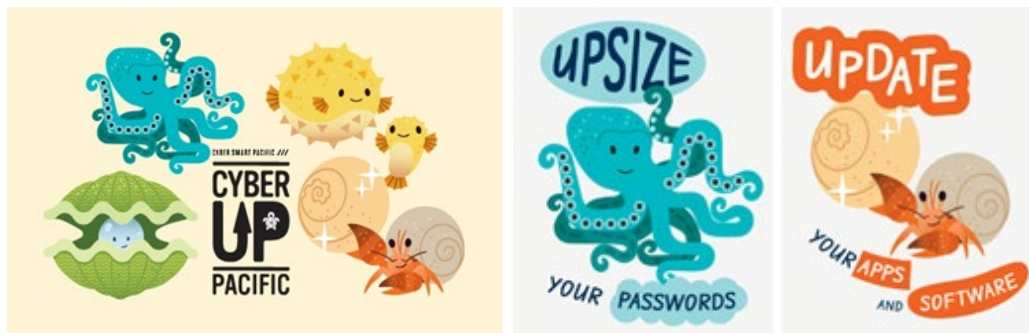


Figure 11. Domestically, CERT NZ ran its 6th Annual Cyber Smart Week, also taking place in October. Banners from the 6th Annual Cyber Smart Week.

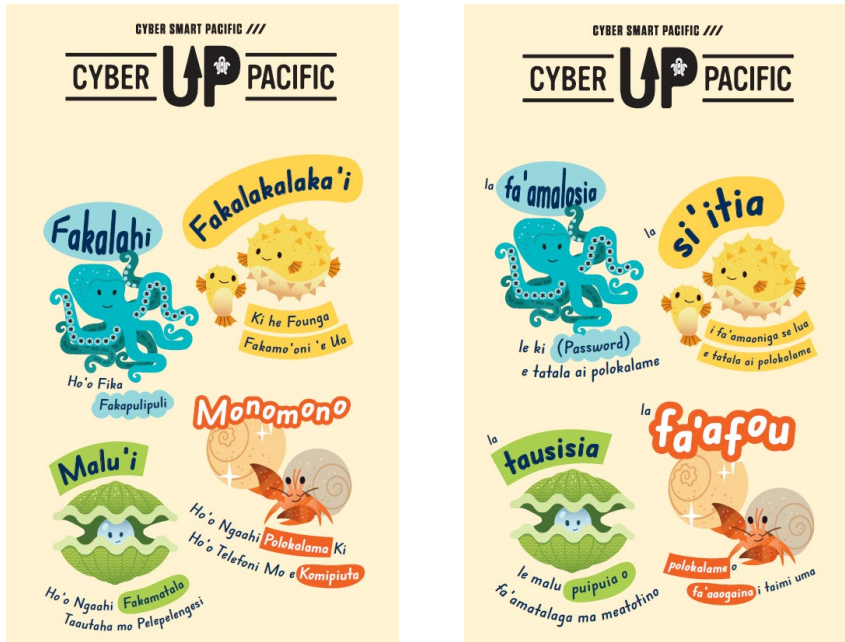


Figure 12. Cyber Smart Pacific translated banners (Tonga and Samoa).

CERT NZ engaged with partners from across the government and private sectors to share the 4 simple steps all New Zealanders can take to be more secure online. During the campaign, CERT NZ worked with 515 partner organisations to help amplify the reach and impact of the campaign.

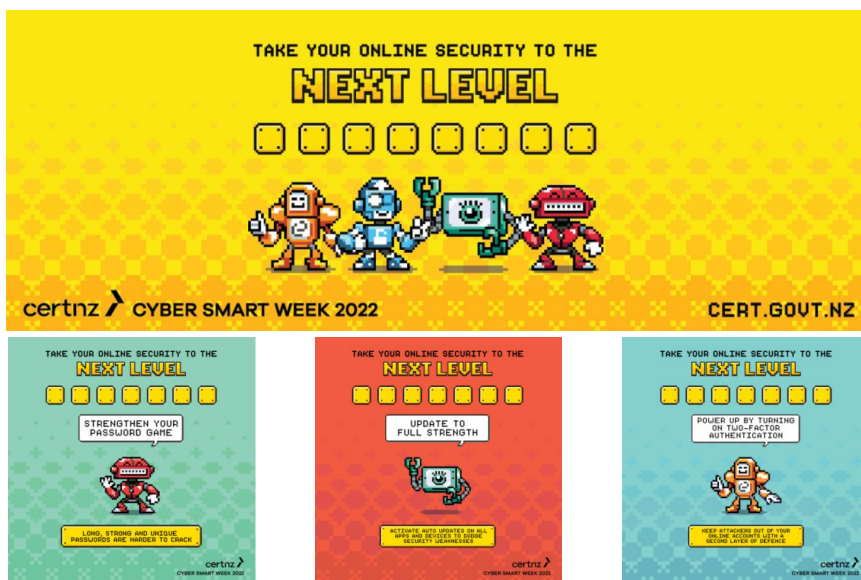


Figure 13. A wide range of resources – from graphics to editorial content – were available for partners to use and share.



Figure 14. CERT NZ also ran 2 mini-campaigns in 2022.

1. 'Two-steps, Too Easy' was a mini-campaign which encouraged small-to-medium businesses to implement 2FA.
2. 'Big Password Energy' was a mini-campaign targeting New Zealanders to get better at creating passwords by using passphrases which can be stronger and easier to remember.



Figure 15. CERT NZ Cyber Security Insights Reports covers published quarterly.

CERT NZ regularly publishes advisories and guides and makes these available on the CERT NZ website. In addition, CERT NZ's quarterly reports continued in 2022. These have been renamed as Cyber Security Insights with the publication of 2 reports each quarter.

- Quarterly Insights: Highlights document, focusing on selected cyber security incidents and issues.
- Quarterly Insights: Data landscape document, providing a standardised set of results and graphs for the quarter.

In 2022, CERT NZ updated its Critical Controls for the year, maintaining the controls from 2021, as they continued to be relevant.

Noting the increase in particular types of incidents, such as unauthorised money transfers, unauthorised access and scams which involve buying, selling and donated goods, CERT NZ published a list of Top Tips for Consumers and Businesses on how to best protect themselves.

2022 CASE STUDY - INVOICE SCAMS

Business compromise leads to advisory

An IT provider noticed that one of its clients was receiving emails pretending to be a recognised supplier.

The emails contained fake invoices and were attempting to trick the client into paying the invoiced amount into the attacker's account.

The affected business investigated and discovered that the emails and fake invoices had been sent to people within the business and to some of its external customers.


The emails seemed legitimate. For example, they included knowledge of recent goods requests and costs. However, there were small differences in the email addresses, which staff picked up on before any payments were made.

The business discovered that an employee's email account had a simple password, making it easy for the attackers to gain access and forward emails containing words like 'account', 'invoice' and 'pay' to an external address belonging to the attacker.

These emails allowed the attackers to gather information about the business's billing cycles and behaviours, helping the attackers to create invoices that looked legitimate.

The compromise went unnoticed for at least 6 months as the attacker was deleting the forwarded emails from the employee's account.

CERT NZ analysed the details from this report, and others, and published an advisory about the extent and nature of invoice scams, how to protect against them, and what to do if you've received a fake invoice.


Business email compromise

Here's what you need to know to help secure your business email.

What is business email compromise?

Business Email Compromise is when an attacker gains access to a business email account without the organisation's knowledge, and then uses that account to carry out a range of attacks or scams.




Why would anyone want to do that?

Business emails hold a lot of handy information, like details on billing cycles and bank accounts. If scammers gain access to your business email, they could issue a bill of exchange by email, pretend and financial information, or redirecting payments to their bank account instead of yours. Attackers often target Accounts Payable and Accounts Receivable teams within organisations. They do this to intercept money and change the payment details to their own bank account. This can result in payments going to the attacker, rather than the intended recipient.

How do we stop this?

There are several ways you can secure your business email to minimise the risk of attackers gaining access:

- Add an extra layer of security to your accounts with two-factor authentication (2FA)
- Use strong, long and unique passwords on all your accounts. Encourage staff to use a password manager to help them remember all their passwords
- Be careful what personal information you share online, especially on social media
- Always verify payments with a SMS or call the person who sent you the invoice

Ways to monitor your business emails

- Always monitor auto-forwarding/filtering rules on email accounts for any rules that you **did not** set up, especially those relating to accounts receivable
- Check your email access logs to look for any unusual login behaviour like unusual login times and unexpected or foreign IP addresses. This can act as an alarm if anyone is trying to access your account

What if this happens to me?

If you discover that an email account within your business has been compromised, there are some steps you can take to help reduce the impact:

- Change the passwords on all affected email accounts immediately to prevent the scammer from accessing the account and sending any further emails
- Set up 2FA for future security
- Tell your IT provider
- Ask your IT provider to check your system for any installed malware
- Report to CERT NZ
<https://www.cert.govt.nz/individuals/report-an-issue/>

For more information on business email compromise see www.cert.govt.nz/Business/compromise-email/

Advisory: Invoice scams affecting New Zealand businesses

CERT NZ recommends these simple steps to protect your business:

Strengthen your email account security – by keeping your software and systems up to date and using strong, unique passwords for each account.

Secure your network – especially when using systems that can be accessed remotely (including remote desktop protocol (RDP)). Use strong, unique passwords and enable 2FA where you can.

Review your business processes – ensure that your processes don't rely solely on email. Verify payments to new or different accounts by phone before making the transaction. This can help prevent losses.

Protect against email spoofing – this is when attackers send you emails pretending to be from legitimate businesses. Protect against this with solutions such as Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).



PAPUA NEW GUINEA



Department of Information and Communications Technology (DICT)

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

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

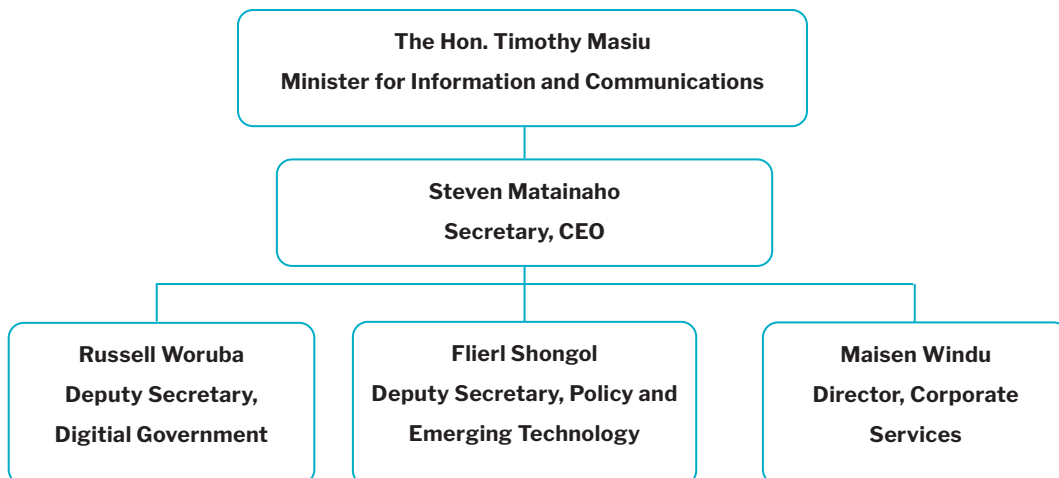
DICT achieves its mission by providing all agencies with the tools, methods, practices, and policy guidance they need to deliver effective and accessible digital services to all PNG residents. This ensures the use of appropriate and affordable digital technologies through a transformative and inclusive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

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

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

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

The current DICT organisational structure includes:



The DICT Vision

To harness the potential of ICT to make PNG become a smart networked and knowledgeable society by bringing the government closer to the people through effective governance, improved service delivery and socio-economic growth. It is envisaged that the use of ICT will:

- promote collaboration, interaction and participation
- promote innovation and learning
- provide an open and transparent government
- provide citizen-centred services, and knowledge-based industries.

This vision is one where all citizens are empowered and can interact and collaborate with the government.

The DICT Mission Statement

Our DICT mission is to transform how government learns, builds, delivers, and measures digital services in the 21st century. To do this, we provide people in the government with the tools, methods, practices, and policy guidance they need to deliver effective and accessible digital services. Moreover, it is also to ensure the use of appropriate and affordable digital technologies through a transformative and inclusive approach across sectors of the economy for benefits of all.

As the government is our department's primary constituency, DICT provides cyber security services through the National Cyber Security Centre (NCSC) and other digital, government shared services support to PNG government departments.

| Shared Services | | |
|---|--|--|
| <p>Internet</p> <p>Providing a way for data to be transferred from Internet servers to computer, high speed, reliable and affordable for all citizens to have access to government online</p> <p>READ MORE</p> | <p>Egavman Cloud</p> <p>The e-Gavman Portal sets out to build a digital platform that will provide a one-stop shop to facilitate the access to Government Information and digital services.</p> <p>READ MORE</p> | <p>Data Governance</p> <p>Collection of processes, roles, policies, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals</p> <p>READ MORE</p> |
| <p>Cyber Security</p> <p>The practice of defending computers and servers, mobile devices, electronic systems, networks and data from malicious attacks. It is also known as information technology security or electronic information security.</p> <p>READ MORE</p> | <p>API</p> <p>Enabling different services and applications to communicate and share information with each other. The transformation of the information system into service layers is at the heart of the digital transformation strategy</p> <p>READ MORE</p> | <p>Help Desk</p> <p>Help keep systems up and running, enable employees to use the technology effectively and resolve issues whilst technology and data connected, so they can operate effectively as a unit.</p> <p>READ MORE</p> |

Figure 16. Screenshot showing the Share Services provided through the NCSC.

Threat landscape

Occurrences of cyber incident reporting to DICT can be submitted through our website – www.ict.gov.pg or directly to the NCSC.

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

- malware
- ransomware attacks
- phishing attacks
- distributed denial-of-service (DDoS) attacks
- identity theft and social engineering used by cyber criminals to conduct acts of fraud and theft.

Awareness raising

To support the increasing need for cyber resilience and safety in Papua New Guinea, DICT supports several awareness-raising initiatives, the primary of which are on our website. Here, DICT promotes cyber safety awareness materials for everyday and government users.



Figure 17. Examples of social media Cybersecurity Awareness Month products.

DICT provides awareness raising through its social media pages on Facebook and LinkedIn. Some events that DICT have taken part in for cyber security and cyber safety awareness are Girls in ICT Day, Online Safety, Cyber Security Awareness Month, and a Career Expo for Youths.

DICT provides support to the PNG Government through official communication channels. DICT provides pamphlets, graphics online and participates on a radio talkback show.

2022 CASE STUDY - BITCOIN SCAM

A cyber security incident of particular note was encountered by PNG in 2022 involving a highly sophisticated Bitcoin scam. This scam used a local dialect that is native to PNG in an attempt to steal funds from its victims. The full impact of the scam campaign was lessened after the affected individual's banking institution noticed irregularities in the victim's transactions and intervened to halt the transactions on the affected accounts.

National CERT of Papua New Guinea

The National CERT of Papua New Guinea (PNGCERT) operates within the National Information & Communications Technology Authority (NICTA).

Our primary constituency is the country of Papua New Guinea.

Threat landscape

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

Email: report@pngcert.org.pg

Website: <https://www.pngcert.org.pg>

The top 5 most common cyber security threats that are facing the citizens of PNG are:

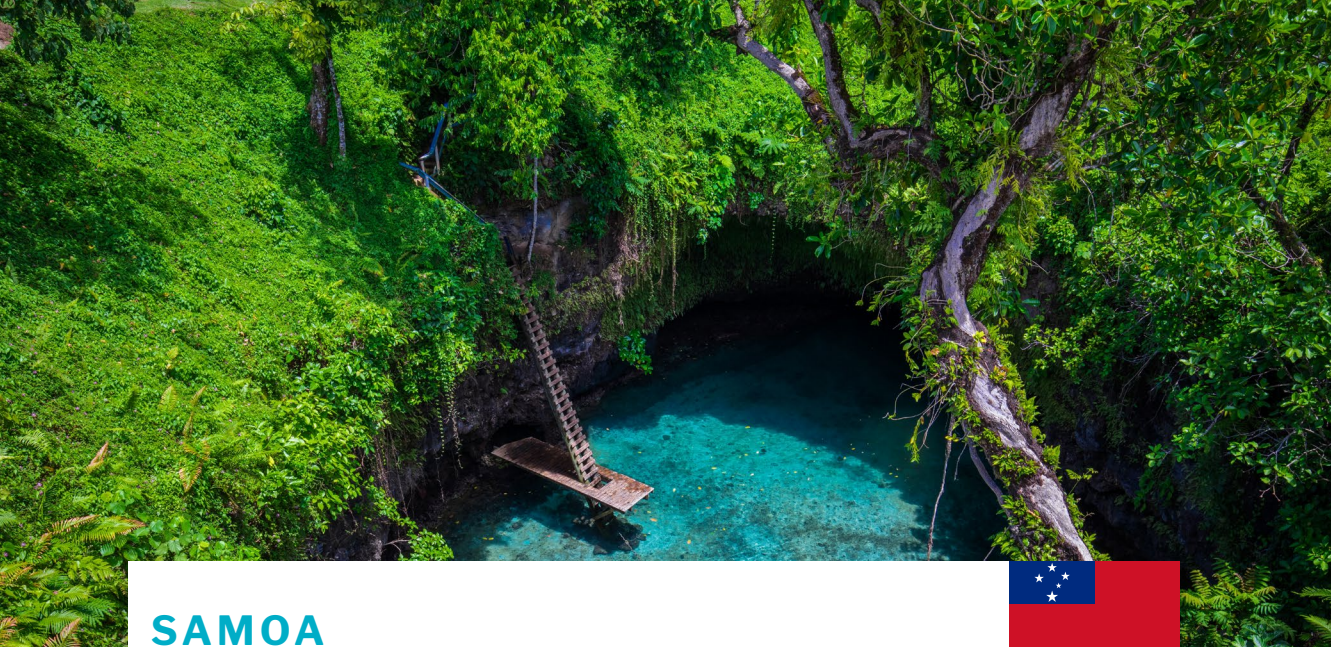
- ransomware
- phishing
- DDoS
- malware
- website defacement.

NICTA only provides advice to bodies on how be safe online; it is up to each entity to implement safeguards, based on their budget.

Awareness raising

The Safer Internet Day is an awareness-raising initiative conducted by NICTA to encourage internet users in our country to practice safer behaviours when using the internet.

NICTA also uses the awareness-raising materials provided by PaCSON as part of our community engagement activities.



SAMOA



Samoa Computer Emergency Response Team

Samoa Computer Emergency Response Team (SamCERT) is a division of the Ministry of Communications and Information Technology, Government of Samoa. SamCERT consists of a 4-member team: the Chief Cybersecurity Officer, the Principal Awareness and Engagement Officer, the Principal Incident Handling Officer, and an intern. SamCERT serves the Government and people of Samoa.

SamCERT just recently completed a website that people and organisations can use to report incidents. They can also reach us through email and social media.

Our website is <https://www.samcert.gov.ws>

Threat landscape

One of SamCERT's main focuses is incident handling, currently mostly for systems environments and infrastructure for government organisations. Incidents that occur at the ministry level are escalated, especially for ministries without internal ICT support. SamCERT is expected to respond and help consult or provide training and capacity building for these organisations.

SamCERT is fairly new, but has already encountered incidents about cyberbullying, spam emails, ransomware. Our team has been able to respond and give information to help victims. We also set up training for staff and management in ministries if they need further awareness.

The 5 most common cyber threats that we encountered in 2022 were:

- malware (ransomware, Trojans)
- phishing attacks
- Internet of Things (IOT) attacks
- drive-by download attacks
- URL manipulation.

Awareness raising

SamCERT conducts awareness raising through a number of different avenues, these include:

- talkback shows on the radio and television
- national events such as ‘Samoa Cyber Smart Week’
- training for both the government and private sectors
- social media and website information about awareness
- our website www.samcert.gov.ws.

Our team also produces advisories for IT experts on information security policy.



Figure 18. SamCERT team members at awareness raising events.



SOLOMON ISLANDS



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

Solomon Islands Government Information Communication Technology Services (SIG ICT Services) is under the Ministry of Finance Corporates Services reporting to the Deputy Secretary Corporate Services. SIG ICT Services is mandated to provide ICT service delivery to the Solomon Islands Government, making it the primary constituency. This also includes all ministries, provincial governments and related agencies. Currently, SIG ICT Services has 30 technical staff and 5 in management and administration positions. We provide services on 3 fronts: client support, information systems and project management, and infrastructure services.

There have been huge developments for the Government's ICT environment; however, there is still a huge resource gap in terms of capacity, and an organisational structural review is in progress to clearly ascertain roles and responsibilities. This includes the establishment of Digital Transformation & Projects and Cyber Security Teams reporting to respective deputy directors.

With a whole-of-government approach to digital transformation, an institutional framework has been developed (currently in draft). Below is the proposed structure of the Digital Transformation Authority (DTA), within which SIG ICT Services sits under the Government Digital Transformation Sub-Committee, reporting to the Solomon Islands Digital Transformation Committee with leaders from the Office of the Prime Minister.

In line with SIG's 5-year *ICT Strategic Plan 2019–23*, 2022 also saw the development of the Solomon Islands Government Security Operations Centre (SIG SOC) with the assistance of the Australian Government and Trustwave. This included installation and configuration

of a security incidents events management system and development of internal security operations policies (in draft). The assistance also resulted in the development of a Cyber Security Foundational Course for the Government, which is now facilitated by the Institution of Public Administration and Management (IPAM) under the Ministry of Public Service. IPAM is the internal training institute of SIG.

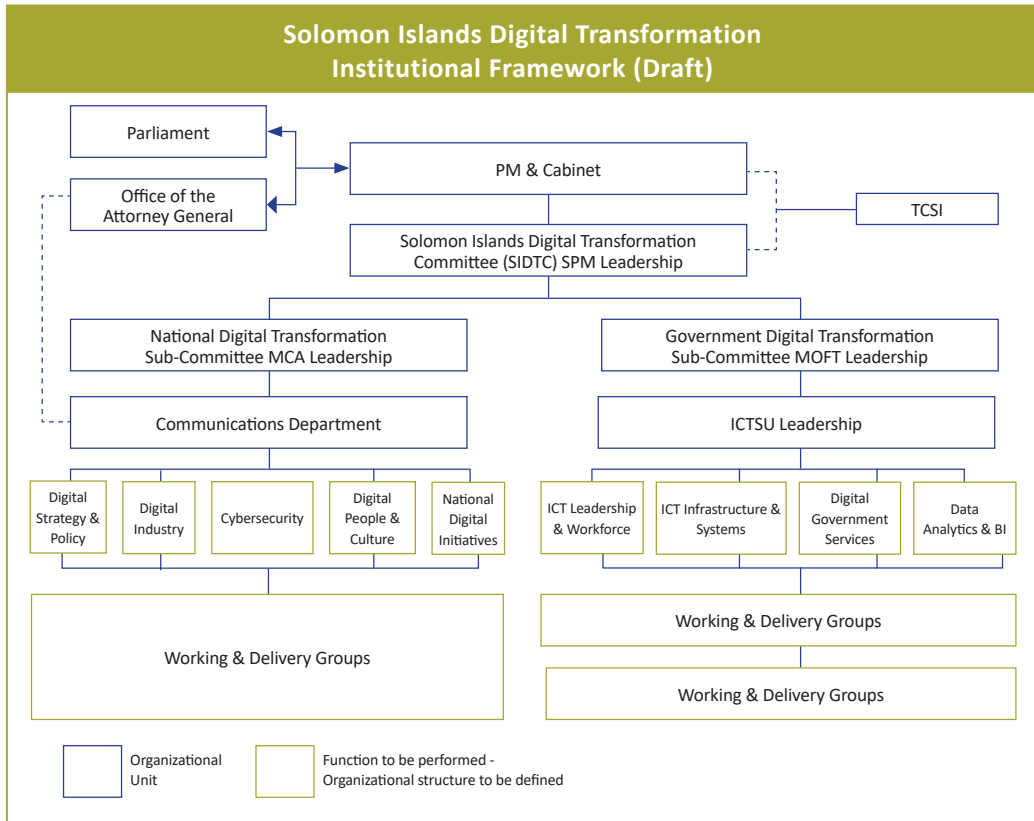


Figure 19. Solomon Islands Digital Transformation Institutional Framework.

SIG SOC, at this stage, comprises 4 positions: Deputy Director Cyber Security, Security Standards Officer, Security Operations Analyst and Service Monitoring Officer. The primary role of the SOC is to ensure compliance of ICT operations and developments with a security operations standard yet to be decided.

Threat landscape

The implementation of a Security Operations Centre within SIG ICTS is still at an infant stage and the internal security operational policies are at drafting stage at the time of writing this report.

Incident reporting is conducted via our helpdesk support system through:

- emails
- phone calls
- direct engagement with stakeholders
- monitoring and addressing incidents through our SIEM.

The most commonly experienced cyber-related security threats that face the people of the Solomon Islands, and how we work to defeat them, are as follows:

- **phishing**
 - » identify
 - » analyse links and report to portals, such as virus total
 - » block domain and emails through our email security gateway
 - » awareness to end users
- **malware**
 - » identify
 - » patch and upgrade/update system
 - » awareness to end users
- **information leakage/insider threats**
 - » log analysis and email audit
 - » identify and report
- **ransomware**
 - » files were infected with the .maql file extension
 - » identify the infected machines and take them offline for further analysis
 - » send sample of infected files for further analysis by anti-virus team vendor (Eset).

During the reporting period, SIG ICT responded to, and provided assistance or advice to, several cyber events.

Phishing emails targeting government employees became a major source of concern during 2022, as the number of attempts to compromise government systems via this method saw a noticeable rise. The majority of them came in the form of false update email types, which attempt to lure users to click a malicious link to update their inbox. Others targeted human resources group emails and financial groups, such as financial controllers.

Awareness raising

SIG ICT conducts awareness raising via newsletters that are sent through emails regarding phishing simulations and links to updates from related sites. We also send regular emails to our users on specific issues.

In 2022, SIG ICT continued to participate in the PaCSON Cyber Smart Pacific Campaign. This effort allowed SIG ICT to facilitate direct constituent engagement and has helped to improve the Solomon Islands' cyber smart capacity.

Our organisation also produces articles and security advice that is released via email, and plans are in place to have a dedicated page via the Solomon Islands' government portal.

2022 CASE STUDY - RANSOMWARE

An incident identified as .maql ransomware affected a government department's network file sharing capability. The initial infection source was believed to have originated through an email link that an employee clicked on. The victim user's computer was taken offline and reformatted to remove the harmful program, and the affected files were recovered from a backup system.



TOKELAU



Telecommunication Tokelau Corporation

Telecommunication Tokelau Corporation, also known as Teletok, is the sole provider of telecommunications services to the nation of Tokelau. Teletok is mandated for the development of communications in Tokelau, and serves 2 roles as a public corporation and also as the Government of Tokelau. Teletok also serves as the national regulator of ICT services within the nation's borders.

Our organisation comprises 21 employees. Teletok's Board of Directors is also the Council of the Government of Tokelau. There are also elders from the 3 island Taupulega who are policymakers on village administration and management of development.

Threat landscape

A cyber communication rule has been documented under the laws of Tokelau which will go for consultation with the villages. It was supposed to be consulted in 2020 but the pandemic prevented this from happening.

Currently, Tokelau is unattractive to cyber criminals as a target due to the small number of internet users, and the perception of limited financial gains from conducting activities in our nation. However, with the imminent opening of a new undersea cable that will connect Tokelau more closely with the wider world, we anticipate an increase in cyber security-related incidents in the near future.

Awareness raising

The cyber communication rule has clear guidance on cyber attacks and threats to ensure internet users will understand their risks. CERT NZ and PaCSON have provided our nation with awareness-raising materials that we have placed in areas of high public presence to maximise their effectiveness.

Our customers and stakeholders can access updates on our services from our website www.teletok.tk





TONGA

CERT Tonga

CERT Tonga is the national Computer Emergency Response Team for the Kingdom of Tonga.

CERT Tonga consists of the Director, Senior Engagement Officer and Security Analyst; 2 contracted staff under the Cyber Security Workforce Development Program (CWDP) with CERT NZ (secondment and internship); and 3 staff from the Media Division that were previously under the Information Department. The Digital Transformation Department is responsible for the management of e-government and data centre services.

CERT Tonga, however, operates under the Ministry of Meteorology, Energy, Information (that is, the Media Division which is now under CERT Tonga), Disaster Management (NEMO), Environment, Communications and Climate Change (MEIDECC).

CERT Tonga's constituents are government ministries, the private sector, public enterprises and NGOs.

Threat landscape

Cyber incidents can be reported to us via the CERT Tonga Hotline number 2378, email report@cert.gov.to, and our website <https://www.cert.gov.to/>

Our 5 most common cyber threats to Tonga are:

- phishing e-mails
- unpatched and updates not done regularly
- no proper backups
- passwords not secured or managed appropriately
- unlicensed software (OS, MS Office, AV, etc.).

CERT Tonga routinely responds to instances of IP compromises, MedusaLocker ransomware, International Revenue Fraud Services (IRFS), web defacements, and malicious IP activities. Our team responded to more than 10 incidents between August 2022 and January 2023.

Awareness raising

There was a Cybersecurity Awareness Program to high schools from October 2022 up to the first quarter of 2023. In February, we provided a Cybersecurity Refresher Awareness presentation to the critical government ministries and public enterprises.

The below information relates to awareness programs we conducted from October 2022 to February 2023.



Figure 20. Awareness sessions for secondary schools.



Figure 21. Government - Ministry of Revenue and Custom.



Figure 22. Government - Ministry of Land and Natural Resources.

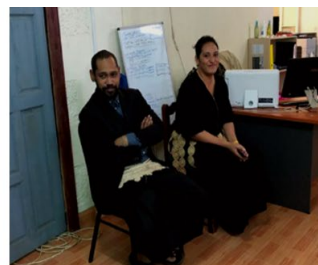


Figure 23. Public enterprises - National Retirement Fund Board.



Figure 24. Exhibitions - Cyber Smart Day 2022.

We use Facebook, Twitter and the government portal to share the below information.

- monthly security bulletin
- monthly security advisory
- cyber security tips
- press release on CERT Tonga events.



TUVALU



Department of Information and Communications Technology (ICT)

The Department of ICT is under the Ministry of Justice, Communications and Foreign Affairs. The department is led by the Director of ICT together with 2 senior officers looking after networking and applications development. The department reports to the Permanent Secretary and the Assistant Secretary of the Ministry. Other functions include coordinating cyber security capacity developments, regulation of the telecommunications sector, and implementing the wider digital transformation goals of the Government.

The current organisational structure for the Ministry of Justice, Communications and Foreign Affairs includes:

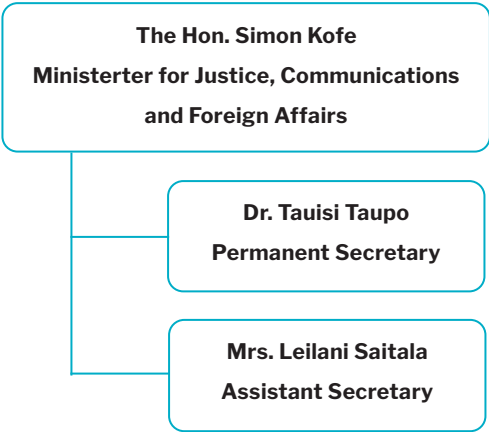


Figure 25. Organisational structure for the Ministry of Justice, Communications and Foreign Affairs.

As there is currently no official CERT in place for Tuvalu, the ICT department works together with the cyber team from the Tuvalu Police, legal advisors appointed by the Attorney-General's Office, and personnel from Tuvalu Telecom, which is the sole internet service provider in the country.

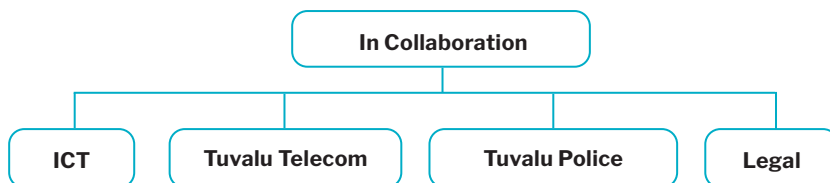


Figure 26. Tuvalu key cyber organisations.

In 2022 our department launched our new website (ict.gov.tv) to allow our citizens to better understand our role and mission in keeping them safe online.

The Department of ICT supports Tuvalu Government's IT services. As its primary constituency, the Department of ICT provides support to all government departments. The department does offer support to the private sector in terms of capacity building and cyber safety for schools and the general public.

Threat landscape

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

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

- malware
- phishing attacks
- identity theft and fraud.

Awareness raising

The Department of ICT, in collaboration with the Tuvalu Police, supported various community engagement and awareness-raising efforts during the reporting period, including through community outreach, visits to schools and engagement via social media. The newly launched Get Safe Online website in Tuvalu is a huge boost for Tuvaluans especially with translations to the local language.

The Department of ICT uses our social media accounts as a platform to share cyber security and cyber safety updates. The Department of ICT tries to share Security Advisories from PaCSON Members like CERT Tonga, CERT VU, CERT NZ and PaCSON Partner CISA, on various social media outlets like news pages and the Facebook pages of the Government.



VANUATU



CERT Vanuatu

CERT VU is the cyber security arm of the Government of Vanuatu established under the Office of the Government Chief of Information Officer (OGCIO), within the Ministry for the Prime Minister. CERT VU currently has 4 dedicated staff, 3 of which are employed on a full-time basis and one on a contracted basis.

CERT VU is a national CERT therefore it serves the entire nation of Vanuatu – the Government, businesses, and the civil society.

CERT VU has a reporting portal built into the CERT website which people can use to report incidents directly to CERT VU. CERT VU also operates an open-door policy in which people can freely walk into the office anytime to report an incident to us in person, or for any advice related to cyber security. People can also reach out to CERT VU to report cyber incidents by phone or email incident response team directly.

Threat landscape

The 5 greatest cyber security threats facing Vanuatu in 2022 were:

- phishing
- spear phishing
- online scam
- ransomware
- malware.

CERT VU responds to all cyber incident reports to the office by our constituents and our international partners. In the 2022 reporting period, CERT VU responded to 450 reported cyber incidents across the spectrum of threats.

Awareness raising

Our yearly awareness-raising program involves the following:

- radio talkback shows
- social media platforms
- open-air awareness talks
- dissemination of flyers and brochures
- one-to-one awareness sessions with organisations
- video clips awareness
- music (cyber security songs)
- regular rural community awareness initiatives
- school educational awareness talks
- press releases on the 2nd National ISO/IEC 27001 Information Security Management System Standards Capacity Building Workshops
- press releases on Vanuatu attending the Cybercrime Conventional Committees' 26th Plenary Meeting at the Council of Europe Hemicycle
- 5 advisories on the different cyber threats and vulnerabilities.

2022 CASE STUDY

On November 6th 2022, CERT VU received a report of a cyber incident involving a ransomware attack.

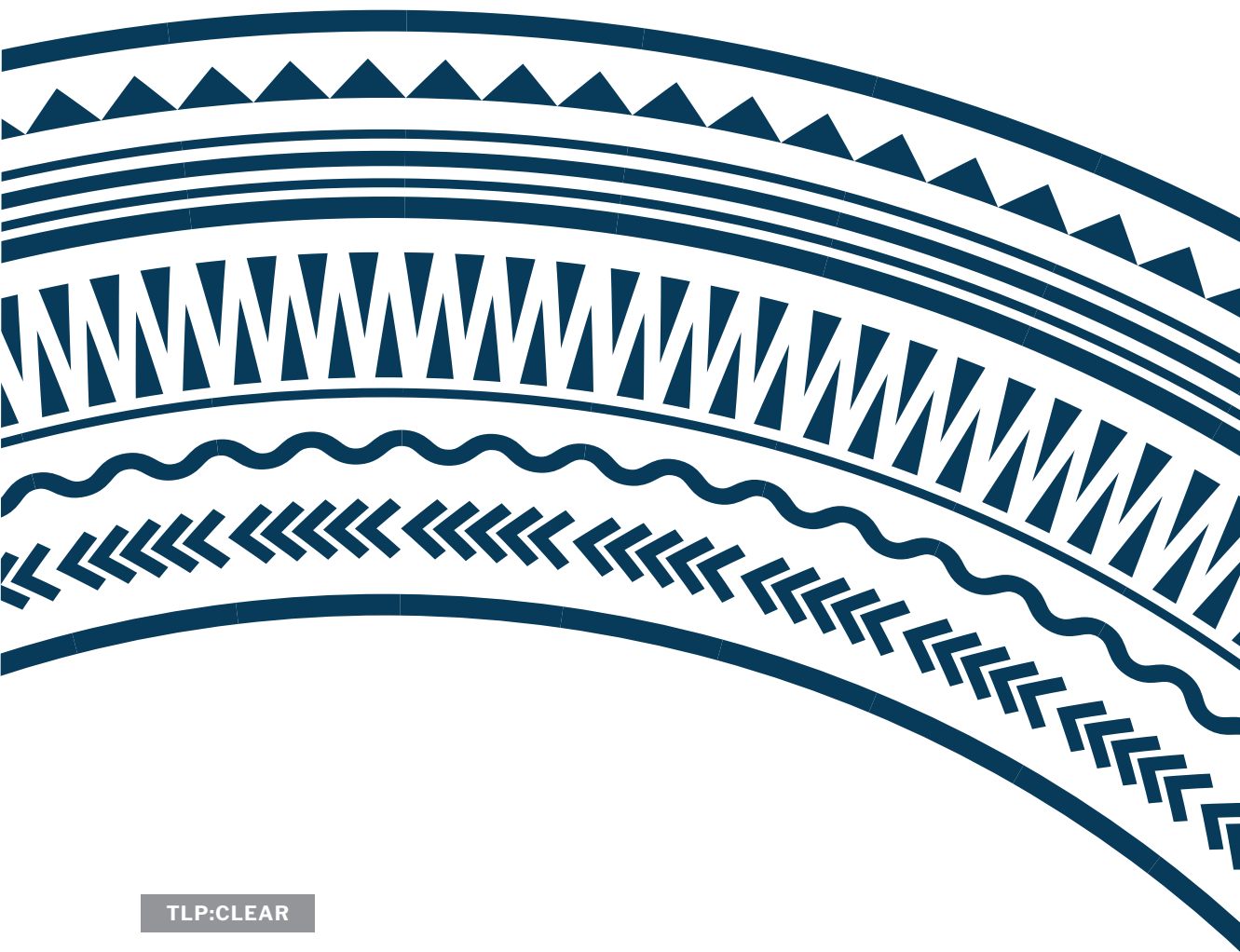
The CERT VU response team mobilised and activated its response plan with specific procedures to attend to the ransomware incident. This response team consisted of the CERT VU, and the systems and network teams within the OGCIIO.

The team performed a quick triage investigation and confirmed that the attack was a ransomware attack. The OGCIIO–CERT VU team worked in collaboration with key critical technical IT teams – forming a Technical Advisory Group (TAG) – comprising representatives from various organisations to map out all critical services which needed to be restored based on their criticality. These services were measured as high, medium, and low priority.

Given the nature of that ransomware attack, OGCIIO–CERT VU had to brief and advise the Vanuatu National Security Council and the Council of Ministers on the organised and/or state-sponsored attack on Vanuatu. Based on the assessment, external support and assistance were paramount for decisions and directions to respond and recover from this attack. International partners responded positively to the request for support which helped the overall incident response operation. CERT VU and the local technical group, in collaboration with international partners, managed to restore all critical services to a confined state with very limited access. This aids continued investigation of the point of compromise and implementation of additional security-hardening measures.

Once the team is satisfied with the amount of security work done in the new environment, it will advise for increases in access to allow all employees to be allowed back in so that the organisation can perform its normal operations. CERT VU is still keeping very close contact with the organisation, and continues to work closely with the local technical team to completely implement all necessary planned security measures.

Partner Updates



CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA), the US Department of Homeland Security (DHS)



Overview

CISA is organised into 6 divisions:

Cybersecurity Division

The Cybersecurity Division (CSD) is responsible for CISA's cyber security mission to defend and secure domestic cyberspace, lead efforts to protect the federal .gov domain of civilian government networks, and collaborate with the private sector to increase the security of critical networks. CSD performs the mission through collaborative, proactive risk reduction and by working with partners to continually prioritise the most significant risks and address them before harm occurs. CSD conducts operations to actively defend cyberspace and help the nation respond to significant incidents, build resilience by addressing systemic risk and helping organisations operate safely and reliably even when being targeted by adversary activity, and set the conditions that contribute to the vitality and health of the cyber ecosystem. CSD also provides a wealth of cyber security resources to help stakeholders identify their critical assets, protect them, detect threats and vulnerabilities, and, when necessary, respond to and recover from cyber events.

In 2021, Congress established the Joint Cyber Defense Collaborative (JCDC) within CSD to create one US government platform for cyber defence planning and operations. It is still early days for the JCDC, but since its creation, for the first time, the government, the private sector, and international partners came together to develop joint cyber defence plans and enable real-time information sharing.

Emergency Communications Division

The Emergency Communications Division (ECD) was established in 2007 in response to communications challenges faced during the attacks on September 11, 2001, and Hurricane Katrina in 2005. ECD supports and promotes communications used by emergency responders and federal, state, local, tribal, and territorial (FSLTT) government officials to keep America safe, secure, and resilient. ECD leads the

nation's operable and interoperable public safety and national security and emergency preparedness (NS/EP) communications efforts, and provides training, coordination, tools, and guidance to help its FSLTT and industry partners develop their emergency communications capabilities. ECD's programs and services coordinate emergency communications planning, preparation, and evaluation to ensure safer, better-prepared communities nationwide.

Infrastructure Security Division

The Infrastructure Security Division (ISD) leads the infrastructure security mission. The division conducts cyber and physical exercises with FSLTTs, the private sector, and international partners to enhance security and resilience of critical infrastructure. These exercises provide stakeholders with effective and practical mechanisms to examine plans and procedures, identify areas for improvement, and share best practices. The exercises inform future planning, technical assistance, training, and education efforts. CISA offers a suite of free exercise services, resources, and materials. ISD conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and FSLTT partners understand and address risks to critical infrastructure. ISD also provides information on emerging threats and hazards, such as unmanned aircraft systems and cyber security and physical convergence, so that appropriate actions can be taken. Among other critical infrastructure security and resilience programs and services, the division also facilitates vulnerability and consequence assessments, and provides tools and training to help partners in government and industry manage the risks to their assets, systems and networks.

Integrated Operations Division

The Integrated Operations Division (IOD) provides a national capability to deliver CISA services to our stakeholders and partners across state and local governments and the critical infrastructure community. Via CISA's 10 regional offices around the nation, IOD delivers cyber and physical vulnerability assessments, architecture review and design, subject matter expertise, incident response support, exercise planning and support, national special security event planning and support, and chemical facility inspections and site security planning to implement Chemical Facility Anti-Terrorism Standards.

Stakeholder Engagement Division

The Stakeholder Engagement Division (SED) develops partnerships, facilitates dialogue, convenes stakeholders, and promotes awareness to help CISA achieve a secure and resilient infrastructure for the American people. SED coordinates stakeholder engagements and partnerships to support the agency's efforts to reduce national risk. SED focuses on 3 lines of effort: strategic partnerships, stakeholder engagement strategy, and stakeholder relationship management.

National Risk Management Center

The National Risk Management Center (NRMCC) is a planning, analysis, and collaboration center within CISA, leading risk reduction efforts and working to identify and address the most significant risks to our nation's critical infrastructure. Guiding the NRMCC's risk management efforts are the National Critical Functions (NCF)—the functions of government and the private sector that are so vital to the US that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety. NRMCC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to identify, analyse, prioritise, and manage these risks to help advance our nation's collective defense.

CISA leads the national effort in understanding, managing, and reducing risk to our cyber and physical infrastructure. We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.

CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers technical assistance and assessments to FSLTT stakeholders as well as critical infrastructure owners and operators nationwide. In addition, CISA pursues collaboration with international partners to promote an open, interoperable, reliable, and secure interconnected world within a global, operational and policy environment where network defenders and risk managers can collectively prevent and mitigate threats to critical infrastructure.

SED's CISA International is committed to collaborating with our international partners to strengthen the security of our global digital infrastructure. In recognition of the importance of international partnerships, we launched our first international strategy in 2020. CISA Global outlines how CISA will work with international partners to fulfill our responsibilities, execute our work, and create unity of effort within our mission areas. The strategy details

CISA's international vision commits the agency to 4 goals:

- advancing operational cooperation
- building partner capacity
- strengthening collaboration through stakeholder engagement and outreach
- shaping the global policy ecosystem.

Threat landscape

The top 3 most common cyber security threats faced by CISA are:

- ransomware
- supply chain compromises
- phishing.

Awareness raising

CISA provides robust publicly accessible communications daily, weekly, and as needed operationally, to keep stakeholders up to date with timely and actionable information. CISA products are tailored for network defenders, C-suite level executives, or the general public as appropriate to ensure all stakeholder sets have information relevant to them. Most recently, we have shared critical technical guidance and protective measures related to Russian threat actors, ransomware threats, destructive malware, and DDoS attacks across the entire cyber security community and all critical infrastructure sectors. Key product types include:

Current activities

Short, real-time communications drafted and published immediately with high-level, actionable information on observed high-impact security activity affecting the community at large. Multiple notifications of patch releases for significant vulnerabilities may be published daily.

Cybersecurity Advisories (CSAs)

In-depth analysis of new or evolving cyber threats that include cyber security threat information, and best practices and actionable mitigation recommendations for network defenders. CSAs provide indicators of compromise and tactics, techniques, and procedures when available. Data and information reflect consolidated cyber data, insights, and analysis from CISA's public-private sector partners and international partners.

Industrial Control Systems (ICS) Cybersecurity Advisories

Timely and relevant information on cyber security vulnerabilities and threats with the potential to impact ICS and critical infrastructure computing networks. ICS Advisories provide ICS security best practices and mitigations for cyber security network defenders to action. Data and information reflect consolidated cyber data, insights and analysis to reduce risks within and across all critical infrastructure sectors, and provide control systems-related security mitigation recommendations from CISA's public-private sector, international partners, and vendors.

ICS Medical Advisories (ICSMAs)

Timely and relevant information on cyber security vulnerabilities and threats related to ICS healthcare information technology systems and medical devices. Includes notification of patch releases and proposed mitigation strategies associated with vulnerabilities in the medical device ecosystem.

Vulnerability bulletins

Weekly summaries of new vulnerabilities that do not pose immediate risk to systems but are significant enough that non-compliance with suggested actions and mitigation guidance may pose risk to your network.

Alerts

Provide timely information about current security issues, vulnerabilities, and exploits.

Tips

Describe and offer advice about common security issues for non-technical computer users.

Analysis reports

Provide in-depth analysis on a new or evolving cyber threat.

CISA often creates dedicated web pages for critical ongoing activity to establish easy-to-access, one-stop resources for all related information. CISA continues to update these web pages in real-time with CISA products and partner resources. Examples include:

[CISA.gov/Shields-Up](https://www.cisa.gov/Shields-Up)

To help stakeholders protect their most critical assets ahead of Russia's invasion of Ukraine, CISA launched the Shields Up Campaign on CISA.gov with current and regularly updated guidance to help organisations of every size adopt a stronger cyber security posture. The webpage includes steps that organisations can take, free cyber security resources available to critical infrastructure partners, and guidance on how organisations can prepare themselves to mitigate the impact of potential foreign influence operations and misinformation, disinformation, and malinformation. Shields Up provides concrete actions for CISA's broad range of stakeholders, to include guidance for all organisations, recommendations for corporate leaders and CEOs, steps individuals can take to protect themselves and their families, ransomware response, and additional resources. This information is intended to be a high-level roadmap to help stakeholders heighten their cyber security posture and prepare for disruptive cyber incidents.

[StopRansomware.gov](https://www.stopransomware.gov)

A one-stop resource where public and private sector entities can find US government tools, information, and resources that can help site visitors reduce their risk of ransomware attacks and improve resilience. This website is a coordinated initiative across the federal government, pooling publicly available federal resources into one location to help organisations better find the information they want on ransomware. The website includes tools and resources from the Department of Homeland Security—CISA and Secret Service—as well as from the FBI, Department of Commerce's National Institute of Standards and Technology (NIST), and the Departments of the Treasury and Health and Human Services. CISA led the design, development, and launch of the new website and continues to work collaboratively with federal partners to add more resources to the website.

[Known Exploited Vulnerabilities Catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

A living catalog of exploited vulnerabilities that carry significant risk to the US federal enterprise. Though required remediation deadlines are for US federal executive civilian branch agencies only, CISA strongly recommends that all organisations monitor and remediate newly listed vulnerabilities to increase resilience.

CISA also recommends reviewing the *National Emergency Communications Plan, Goal 6: Cybersecurity: Strengthen the cyber security posture of the Emergency Communications Ecosystem*, which provides guidance on the nation's strategy to strengthen the cyber security posture of the emergency communications ecosystem. SAFECOM provides technology tools for practitioners that support communications and cyber resilience that can be referenced as a great public resource. These resources can be found at this link:

<https://www.cisa.gov/safecom/technology>

CISA's *Strategic Plan for 2023–25* (Strategic Plan | CISA) describes CISA's international vision and outlines our approach for working with international partners to fulfill our responsibilities, execute our work and create unity of effort within our mission areas.

If you are interested in learning more, please email us at:

CISAInternationalAffairs@hq.dhs.gov

Mailing lists:

<https://www.cisa.gov/subscribe-updates-cisa>

<https://www.cisa.gov/uscrt/mailling-lists-and-feeds>

<https://www.cisa.gov/social-media-directory>

https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=COD_E_RED

About the agency:

<https://www.cisa.gov/>

<https://www.cisa.gov/about-cisa>

Additionally, please find below URLs which link directly to our free catalogue of CISA cyber security tools and resources:



URLs

| | | | |
|---|--|---|--|
|  <p>Cybersecurity Evaluation Tool (CSET)</p> |  <p>Industrial Control Systems (ICS) training</p> |  <p>Incident Response Training</p> |  <p>Free Cybersecurity Services and Tools</p> |
|---|--|---|--|

FEDERAL BUREAU OF INVESTIGATION (FBI)

Overview

The Federal Bureau of Investigation (FBI) is the domestic intelligence and security service of the US and the principal federal law enforcement agency. The FBI operates under the US Department of Justice (DOJ), and is also a member of the US Intelligence Community. It reports to both the Attorney-General and the Director of National Intelligence.



The FBI workforce includes more than 35,000 people, including special agents and support professionals such as intelligence analysts, language specialists, scientists, and information technology specialists.

We work around the globe. Along with our headquarters in Washington DC, we have 56 field offices located in major cities throughout the US – about 350 satellite offices called resident agencies in cities and towns across the nation – and more than 60 international offices called legal attachés in US embassies worldwide.

Resourcing and constituency

The FBI's primary constituency is the citizens of the United States, and our second constituency would include United States allies and partners.

Threat landscape

The top 3 common cyber security threats reported to the FBI are:

- phishing
- internet enabled fraud (non-delivery of items)
- and data breaches.

The FBI also sees significant reporting of romance scams, BEC, and ransomware.

Awareness raising

The FBI produces a number of publications and advisories specific to cyber and law enforcement. These include Private Industry Notifications (PINs), FBI Flashes, and Joint Cyber Security Advisories with partners in the community. The FBI also releases an annual Internet Crime Report through the FBI's Internet Crime Complaint Center at [ic3.gov](https://www.ic3.gov).

RESERVE BANK OF FIJI

Overview

The Reserve Bank of Fiji (RBF) is the central bank of the Republic of Fiji, established in 1984 under the *Reserve Bank of Fiji Act*.

The RBF employs a little over 200 staff that operate from central Suva, the capital of Fiji. There are a total of 7 departments that function together under the leadership of the Board, governors and executive management to deliver our statutory responsibilities.



Resourcing and constituency

The RBF's primary constituency is the Republic of Fiji.

Threat landscape

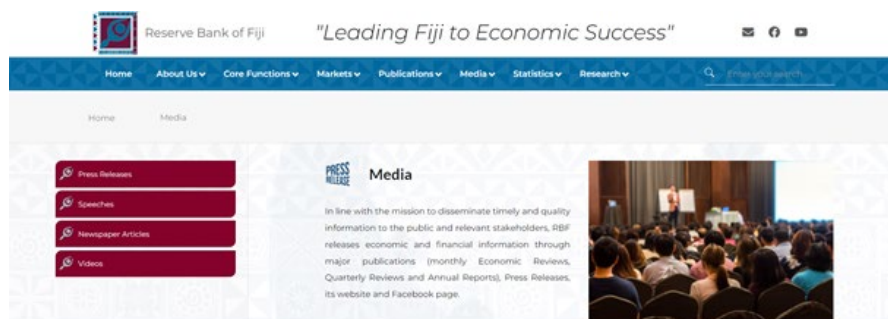
The top 3 common cyber security threats reported to the RBF are:

- insider threats
- phishing and ransomware attacks
- threats to payments systems.

Awareness raising

The RBF produces a number of cyber publications and advisories. These are available at <https://www.rbf.gov.fj/media/>

The RBF also sends direct regulatory requirements to the licensed financial institutions regarding cyber security.



Updates



AWARENESS RAISING WORKING GROUP

The challenge impacting low cyber security literacy brings risks to any organisation. Thus, 'Awareness Raising' is critical for increasing cyber security knowledge.

Since the establishment of PaCSO^N in 2018, the PaCSO^N Awareness Raising Working Group (ARWG) serves the primary objective of acting on behalf of the PaCSO^N Community and taking the lead on the following key initiatives:

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

The aims translated through the above initiatives are also supported by the outlined Working Group's Terms of Reference.

The ARWG is responsible for raising awareness on behalf of the PaCSO^N Community. The purpose of the ARWG is to advocate the PaCSO^N Vision and Mission on behalf of the Community.



Figure 27. 2022 campaign material centred on the theme 'Cyber Up Pacific with PaCSO'.

2022 activities

During the reporting period, the ARWG successfully re-launched the PaCSO^N awareness-raising campaign – the Cyber Smart Pacific Campaign (<https://pacson.org/cyber-smart-pacific>). Held throughout October 2022, as part of National Cyber Security Awareness Month, the Cyber Smart Pacific Campaign centred on 4 simple yet impactful actions designed to improve the individual user’s cyber security. As part of the campaign rebrand, 4 simple and impactful actions capitalised on visual infographics of ocean creatures (our mascots) that people are familiar with and interact with frequently. This aimed to help the audience remember and translate critical and valuable knowledge around cyber security regardless of their level of cyber literacy and capability.

In 2022, the campaign centred on the theme ‘Cyber Up Pacific with PaCSO^N,’ with the campaign tagline being ‘Cyber security threats are on the rise, so let’s Up our digital safety and security.’ Continuing the support from CERT NZ and with CERTVU being the Convenor, the 2022 campaign developed mascots and promotional material that assisted PaCSO^N Members in educating and raising awareness in their local community.



Figure 28. Products from the 2022 ‘Cyber Up Pacific with PaCSO^N’ campaign.

The reporting year 2022 ended Vanuatu’s term as the Convenor for the ARWG, which it had held for 3 years since the establishment of the ARWG in 2019. The ARWG Convenor position and responsibilities have been handed to Samoa. On behalf of the former convenor of the ARWG, CERT VU takes this opportunity to thank all active members of the working group and the PaCSO^N Community for their continued support in ensuring the AWG achieves all its objectives.

We are preparing and looking forward to a successful ‘Cyber Smart Pacific Campaign – 2023’, #PaCSO^NARWG

CYBER SMART PACIFIC ///

CYBER UP PACIFIC

JUST LIKE IN THE OCEAN, YOU CAN ENCOUNTER UNKNOWNNS IN THE ONLINE ENVIRONMENT. SO LET'S REDUCE THE RISK - CYBER UP WITH THESE FOUR SIMPLE STEPS TO HELP BE SECURE ONLINE.



SO THEY'RE LONG, STRONG AND HARD TO CRACK.

Long, strong and unique passwords are much harder for attackers to crack.

Try creating a passphrase that's a string of four or more words, this is much stronger than a random mix of letters, numbers and symbols.



SO YOUR ONLINE ACCOUNTS HAVE DOUBLE PROTECTION.

Enable two-factor authentication (2FA) for your online accounts by turning it on in privacy settings.

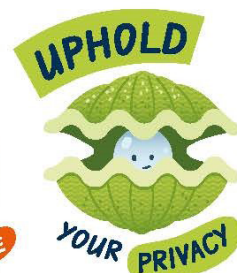
When you next log in you'll use a second step such as your thumbprint, facial ID or one time code from an app to verify it's really you.



TO KEEP BUGS AND VIRUSES OUT.

As well as providing new features, updates also fix security risks that attackers can use to gain access to your personal information.

Ensure automatic updates are enabled on all your devices to keep yourself secure.



TO KEEP YOUR PERSONAL INFORMATION SECURE.

Before you share any personal information online, check your social media settings to ensure they are switched to 'Friends only' and that any requests for personal information are legitimate.

LEARN MORE FROM YOUR LOCAL PACSON PARTNER AT [CERT.GOV.VU/CYBERSMART/](https://cert.gov.vu/cybersmart/)

CAPACITY BUILDING WORKING GROUP

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

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

2022 activities

In 2022, the CBWG continued to deliver the Remote Session Series, organised by CERT NZ. Originally established in June 2020 to maintain community engagement in the face of the COVID-19 Pandemic, the series provides a monthly opportunity for the PaCSO^N Community to connect. From February 2022 to April 2023, the CBWG hosted 12 remote sessions with a total of 317 attendees from 18 economies.

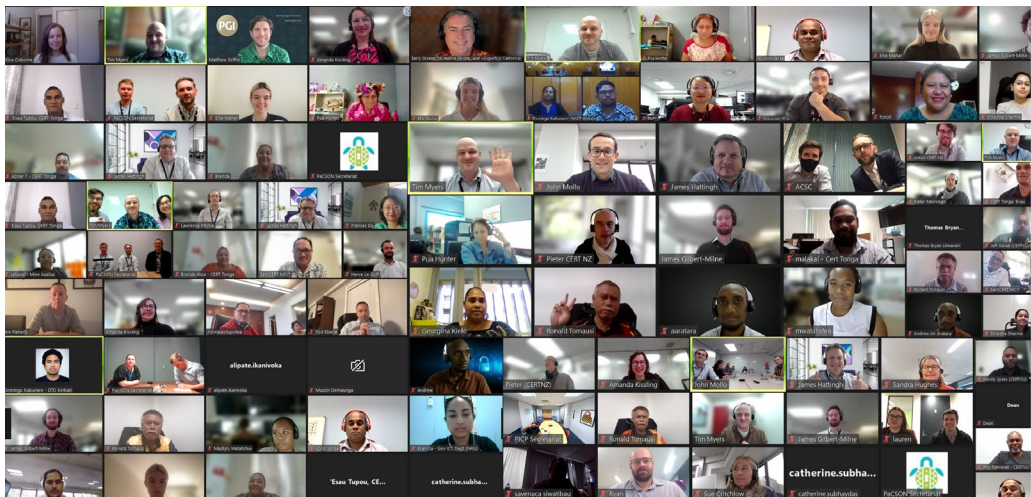


Figure 29. Screenshot of one of the 12 Remote Session Series.

The Remote Sessions were further supported by operational partnerships with Cyber Safety Pasifika, PILON, with invitations sent to their respective members for select sessions throughout the year.

Like last year's efforts, external guests and PaCSO^N Partners were invited to provide sessions to the community – presentations included Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) through APCERT, APNIC, FS-ISAC, Akamai, the FBI and Shadowserver.

The presentations covered a wide range of topics, including incident communications (by SamCERT), and ransomware trends in New Zealand (by CERT NZ), with the most popular sessions being the Shadowserver Q4 reporting presentation closely followed by a talk on coordinated vulnerability disclosure by JPCERT/CC. It was encouraging to see the level of engagement and interest from the PaCSO Community within these sessions, and it is something to build on as the program continues into 2023.

A new effort for 2022 was the introduction of the Pacific Cyber Security Data & Insights Project. Announced at last year's PaCSO AGM, this new project introduces Shadowserver to the Community to share data and insights relevant to each member. To date, 5 country sessions have been completed and work has begun on the regional insights report. The CBWG looks forward to continuing this effort.

The CBWG appreciates the efforts and engagement from the whole of PaCSO as well as our regional and global partners throughout the year. We are looking forward to continuing this momentum and developing new and exciting projects in the coming year.

A goal for the Remote Session Series going into 2023 is to see more of our PaCSO Members presenting their learnings and experience to the Community. The CBWG will work closely with Members to help organise and schedule these presentations.

Capacity Building Working Group Membership:

- Australia
- the Cook Islands
- Fiji
- Nauru
- Papua New Guinea
- the Solomon Islands
- Tonga
- Vanuatu
- New Zealand – Working Group Convener.

COMMUNICATIONS WORKING GROUP

The aim of the Communications Working Group is to improve information sharing and the communication tools for the PaCSO^N Community. During the life of the Communications Working Group, its members will work towards achieving a collective of tools and processes which enable better communication and information sharing within the PaCSO^N Community. The Communications Working Group will be responsible for improving the communication outlets and information sharing processes on behalf of the PaCSO^N Community.

2022 activities

In 2022, the Communications Working Group was proud to publish the *PaCSO^N Annual Report 2021* for distribution to our Members, Partners and Stakeholders. This was our main deliverable for this period and we would like to thank our Members and Partners for their contributions in order to make this edition possible.

The *PaCSO^N Annual Report 2021* builds upon the previous year's publication, instilling readers with a clear understanding of the cyber security issues and challenges faced by the Pacific community, from the voices of those community members themselves.



In addition to publishing the annual report, the Working Group is also pleased to have published 3 news articles over the course of 2022. These articles serve the dual purpose of publicising the important work that PaCSO^N does, along with promoting awareness of key initiatives delivered by our Members and Partners.

The Communications Working Group also continues to maintain and sustain the PaCSO^N website, pacson.org, and we are excited to report that planned expansions of the website are progressing on schedule. During 2022, the website continued to be a central source of cyber security news and information. The website provides the PaCSO^N 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.

The Working Group was pleased to continue supporting the ARWG and CBWG throughout 2022, and looks forward to continuing our collaborations in 2023.

PaCSO 2022 Annual General Meeting 26 – 30 September 2022

Published: November 24, 2022

The 2022 PaCSO Annual General Meeting (AGM) was held in person for the first time since 2019 in Suva, Fiji.

[READ THE ARTICLE](#) 



Cyber Smart Pacific 2022 campaign – Cyber UP Pacific

Published: October 17, 2022

Just like in the ocean, you can encounter unknown threats in an online environment. PaCSO is pleased to welcome back its annual public awareness raising campaign – Cyber Smart Pacific.

[READ THE ARTICLE](#) 



International Girls in ICT Day 2022

Published: April 28, 2022

On 28 April 2022, the International Telecommunication Union (ITU) recognises International Girls in ICT Day. The ITU identified “Access and Safety” as this year’s theme.

[READ THE ARTICLE](#) 



Figure 30. Screenshot from the PaCSO website.

PARTNERS WORKING GROUP

The PaCSON Partners Working Group (PPWG) was established with the aim of providing PaCSON Partners with opportunities to support and collaborate with the PaCSON primary Working Groups – Awareness Raising, Capacity Building, and Communications – on their planned activities. The PPWG is driven by the aspiration to provide a whole-of-community benefit to PaCSON, working with all PaCSON Members to increase their knowledge, capacity, and resilience in matters of cyber security.

2022 activities

In 2022, the PPWG and the PaCSON Community was proud to welcome the FBI as the newest organisation to attain Partner status within PaCSON. The FBI hit the ground running in its partnership with PaCSON, delivering a presentation to the PaCSON Community at the 2022 AGM that was well received by all attendees. It also delivered its first remote session in November 2022, presenting a case study on a criminal group using a botnet, and the complex investigation that followed. The FBI brings with it a huge wealth of knowledge and experience in the cyber domain, and PaCSON looks forward to continuing to work with the bureau's representatives to achieve the PaCSON mission of strengthening the Pacific's resilience to cyber threats.

Throughout 2022 and beyond, the PPWG will continue to support the PaCSON Community to deliver against its mission of working 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.

In 2023, the PPWG hopes to provide further support to the information sharing, awareness raising and cyber security capacity needs of the PaCSON Community.



Future Plans 2023



In 2023, PaCSO^N will remain committed and responsive to the needs and wants of the Community. It is expected that our PaCSO^N Community may continue to experience an increasing pace and frequency of cyber security events. We will continue to support each other and improve regional cyber security capabilities and readiness through cooperation and collaboration.

Our PaCSO^N Community will continue to maintain an awareness of the risks and threats which impact the safety and security of the Pacific region. PaCSO^N is assisting our governments, businesses, and constituents to prioritise cyber security, remain safe online, and be prepared against cyber events. More than ever, cyber security continues to be a shared responsibility, a responsibility that PaCSO^N is addressing through our commitment to coordinating activities that benefit the Pacific region's cyber security posture.

As part of the continued operation of PaCSO^N in 2023, in a collaborative spirit, our Community will:

- continue the publication of the *PaCSO^N Annual Report 2022*
- continue to support and promote the Cyber Smart Pacific Campaign
- contribute content to pacson.org and ensure the Community Portal is being used as an information repository and historical catalogue for the PaCSO^N Community
- leverage our network to advocate for the Pacific region and improve coordination and collaboration with stakeholders.
- develop content for the PaCSO^N CUP and continue to support the monthly Remote Session Series.

At the 2022 AGM, PaCSO^N endorsed the priorities for 2022–23. These priorities will guide PaCSO^N's engagement and goals for the next 12 months and allow the Community to track progress and advances made over the 2023 reporting period.

Success for PaCSO^N in 2023 will consist of:

- building the PaCSO^N brand as a trusted partner and source of truth among Pacific cyber security and IR professionals
- strengthening the resilience of the Pacific region's cyber security posture by welcoming new Members and Partners and promoting PaCSO^N to the wider CERT, capacity building and cyber security communities
- ensuring that the PaCSO^N Community supports training opportunities that reflect the small-island context of the Pacific and the unique needs of our Community
- continuing to deliver a contextualised and tailored Cyber Smart Pacific Campaign that addresses the unique needs and wants of our PaCSO^N Community and constituents
- supporting increased capacity building initiatives, including incident response training, technical secondments, support and advice for cyber and technical career streams, and engaging the university and education sectors to support the cyber security and cyber literacy needs of the next generation.



Acknowledgments



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

This report and the activities of PaCSO are made possible thanks to the support and advice of many individuals and organisations. The PaCSO Executive Committee, on behalf of the entire PaCSO Community, would like to thank everyone who contributed to PaCSO in 2022, with special thanks to:

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 [APCERT](https://www.apcert.org/).
<https://www.apcert.org/>

ASIA PACIFIC NETWORK INFORMATION CENTRE (APNIC)



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

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

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

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

To learn more, please visit [APNIC](https://www.apnic.net/).
<https://www.apnic.net/>



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 [Cyber Safety Pasifika](https://www.cybersafetypasifika.org/).
<https://www.cybersafetypasifika.org/>

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE (DFAT)



Australia's Cyber and Critical Tech Cooperation Program (CCTCP) works in partnership with countries in Southeast Asia and the Pacific to enhance cyber resilience. Established in 2016, the CCTCP plays an important role in supporting Australia's international cyber engagement which champions an open, free and secure internet that protects national security and promotes international stability, while driving global economic growth and sustainable development.

The CCTCP supports Australia's commitment to deliver on the United Nations 2030 Agenda for Sustainable Development, which recognises the vital role of digital technologies to achieve a better and more sustainable future for all.

PaCSON acknowledges the support and funding provided by the DFAT CCTCP.

To learn more, please visit [DFAT Cyber and Critical Tech Cooperation Program](https://www.internationalcybertech.gov.au/).
<https://www.internationalcybertech.gov.au/>

GLOBAL CENTRE FOR CYBER EXPERTISE (GFCE), PACIFIC HUB

The Global Forum on Cyber Expertise (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.

PACIFIC ISLANDS LAW OFFICERS NETWORK (PILON)

**PACIFIC ISLANDS
LAW OFFICERS' NETWORK**

PILON works to ensure a safe and secure Pacific by advancing key law and justice issues. PILON is an association of senior law officers from 19 Pacific Island Countries and territories.

To learn more, please visit [PILON](https://pilonsec.org/).

<https://pilonsec.org/>

Glossary

| | |
|---------|--|
| 2FA | Two-Factor Authentication |
| ACSC | Australian Cyber Security Centre |
| AGM | Annual General Meeting |
| APCERT | Asia Pacific Computer Emergency Response Team |
| APNIC | Asia Pacific Network Information Centre |
| ARWG | Awareness Raising Working Group |
| ASD | Australian Signals Directorate |
| BAU | Business as Usual |
| BEC | Business Email Compromise |
| CALD | Culturally and Linguistically Diverse |
| CBWG | Capacity Building Working Group |
| CCTCP | Cyber and Critical Tech Cooperation Program |
| CEO | Chief Executive Officer |
| CERT | Computer Emergency Response Team |
| CERT VU | Computer Emergency Response Team Vanuatu |
| CERTNZ | Computer Emergency Response Team New Zealand |
| CISA | Cybersecurity Infrastructure & Security Agency (US) |
| CMM | Cyber Security Capacity Maturity Model for Nations |
| CSA | Cybersecurity Advisories |
| CSD | Corporate Services Department (PNG) |
| CSD | Cyber Security Division (US, CISA) |
| CSIRT | Computer Security Incident Response Team |
| CSP | Cyber Safety Pasifika |
| CWDP | Cyber Security Workforce Development Program (Tonga) |
| DDoS | Distributed Denial-of-Service |
| DFAT | Department of Foreign Affairs and Trade (Aust) |
| DGTO | Digital Government Transformation Office (Fiji) |
| DHS | Department of Homeland Security (US) |
| DICT | Department of Information and Communications Technology (Papua New Guinea) |
| DKIM | Domain Keys Identified Mail |

| | |
|-----------|---|
| DMARC | Domain-based Message Authentication, Reporting and Conformance |
| DOJ | Department of Justice (US) |
| DTA | Digital Transformation Authority (the Solomon Islands) |
| DTO | Digital Transformation Office (Kiribati) |
| EC | Executive Committee (PaCSO) |
| ECD | Emergency Communications Division (CISA, US) |
| ECIA | Economics, Consumer and International Affairs (PNG) |
| ERPD | Engineering & Resource Planning Department (PNG) |
| FBI | Federal Bureau of Investigation (US) |
| FICAC | Fiji Independent Commission Against Corruption |
| FIU | Fiji Financial Intelligence Unit |
| FSC | Financial Supervisory Commission |
| FSLTT | Federal, State, Local, Tribal, and Territorial |
| FTA | File Transfer Appliance |
| GFCE | Global Forum on Cyber Expertise |
| ICS | Industrial Control Systems |
| ICSMA | ICS Medical Advisories |
| ICT | Information & Communication Technology |
| IOD | Integrated Operations Division (US, CISA) |
| IoT | Internet of Things |
| IPAM | Institution of Public Administration and Management (the Solomon Islands) |
| IR | Incidence Response |
| IRFS | International Revenue Fraud Services |
| ISD | Infrastructure Security Division (CISA, US) |
| IT | Information Technology |
| ITCS | Department of Information Technology and Computing Services (Fiji) |
| JCDC | Joint Cyber Defense Collaborative (CISA, US) |
| JPCERT/CC | Japan Computer Emergency Response Team Coordination Center |
| LED | Licensing & Enforcement Department (PNG) |
| MEIDECC | Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (Tonga) |

| | |
|----------|---|
| MCIT | Ministry of Communications and Information Technology |
| MICT | Ministry of Information, Communications and Transport (Kiribati) |
| MIPD | Marshall Islands Police Department |
| MSAN | Multi-Service Access Node |
| MSP | Managed Service Providers |
| NCF | National Critical Functions (CISA, US) |
| NCSC | National Cyber Security Centre (PNG) |
| NGO | Non-Government Organisation |
| NICTA | National Information and Communications Technology Authority |
| NRMC | National Risk Management Center (CISA, US) |
| OCSC | Oceanic Cyber Security Centre |
| OGCIO | Office of the Government Chief Information Officer (Vanuatu) |
| OPM | Office of the Prime Minister (the Cook Islands) |
| OSC | Online Safety Commission (Fiji) |
| PaCSO | Pacific Cyber Security Operational Network |
| PILON | Pacific Islands Law Officer's Network |
| PIN | Private Industry Notifications |
| PMU | Project Management Unit |
| PMO | Prime Minister's Office (Tonga) |
| PNGCERT | Papua New Guinea Computer Emergency Response Team |
| PPWG | PaCSO Partners Working Group |
| PSTN | Public Switched Telephone Network |
| RBF | The Reserve Bank of Fiji |
| RDP | Remote Desktop Protocol |
| SamCERT | Samoa Computer Emergency Response Team |
| SED | Stakeholder Engagement Division (CISA, US) |
| SIG | Solomon Islands Government |
| SIG ICTS | Solomon Islands Government (SIG) Information Communication Technology Services (ICTS) |
| SIG SOC | Solomon Islands Government Security Operations Centre |
| SMMD | Social Media Management Desk (PNG) |
| Teletok | Telecommunication Tokelau Corporation |
| TOR | Terms of Reference |
| UAS | Universal Access Scheme Secretariat (PNG) |



Disclaimer

The contents of the Membership and Partnerships updates are written by each PaCSON Member or Partner based on their individual analysis and experience. Responsibility for the information and views expressed in each update lies entirely with the Member or Partner.



PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

pacson.org