STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE

Review Report on the Convention on Cybercrime

PARLIAMENT OF THE REPUBLIC OF FIJI
Parliamentary Paper No. 53 of 2023

June 2023

Published and Printed by the Department of Legislature, Parliament House, SUVA

Table of Contents

Chairperson's Foreword

This report is a review of the Convention on Cybercrime also known as the Budapest Convention that was tabled in Parliament on 1st September 2022. The review report was still at the Committee deliberation phase when Parliament was dissolved on 30th October, 2022. The previous Committee had received eighteen (18) submissions, both oral and written and had begun formulating the Review Report. This pending report on the Convention on Cybercrime was reinstated in this new term of Parliament. The Standing Committee on Foreign Affairs and Defence reviewed the verbatim reports from the last Committees deliberations and called three (3) other submissions and received a second oral submission from the Ministry of Home Affairs and Immigration which was in addition to their written submission that was submitted to the previous Committee.

The submissions were from a wide range of backgrounds including government agencies, regional bodies, non-government organisations, private ICT companies, private individuals, universities, commercial banks, UN Agencies, a treaty specialist, Fiji Financial Intelligence Unit, legal practitioners and law enforcement. I thank them for their submissions and the Committee is grateful for their contribution towards the completion of this review report.

The Committee has also included in this report some consequential actions that need to be taken after Fiji ratifies the Convention as recommended by some of the submissions, which are mostly amendments to some existing legislations and the recommendation from the Ministry of Home Affairs to reassign the Cybercrime Act from the Ministry of Communications to the Ministry's portfolio. The Committee understands that these recommendations are beyond its Cybercrime Convention review mandate as they deal with national legislations however, the Committee has highlighted them in this report to reflect the views and concerns of agencies that have a role to play in dealing with cybercrime.

Suffice to say that there was overwhelming support for the ratification of the Convention given the opportunity it provides to build capacity and to cooperate with countries that are leading the fight against cybercrime. Because of the cross-border nature of cybercrime, cooperation between States and private industry is critical therefore, Fiji's accession to the Convention will greatly contribute to the overall development of cyber security for Fiji.

As such, the Committee recommends to Parliament that Fiji ratifies the Convention without reservations, and that Parliament take note of the Committee's comments under *Other Recommendations*.

I take this opportunity to thank members of the current and previous Standing Committees on Foreign Affairs and Defence and the Secretariat for compiling this bipartisan report.

On behalf of the Standing Committee on Foreign Affairs and Defence, I submit this report to the Parliament.

Hon. Lenora Qereqeretabua
Deputy Chairperson

Acronyms

CI	Critical Infrastructure
DPP	Office of the Director of Public Prosecutions
EU	Exclusive Economic Zone
FWCC	Fiji Women's Crisis Centre
GA	General Assembly
GDPR	General Data Protection Regulation
GLACY+	Global Action on Cybercrime Extended project
ILO	International Labour Organization
MS Teams	Microsoft Office 365 Teams Application
OECD	Organisation for Economic Co-operation and Development
OSG	Office of the Solicitor-General
PICs	Pacific Island Countries
SDGs	Sustainable Development Goals
SO	Standing Orders
T-CY	Cybercrime Convention Committee
UN	United Nations
UN GA	United Nations General Assembly
USP	The University of the South Pacific

Recommendation

The Committee recommends to Parliament that Fiji ratifies the Convention without reservations.

1.0 Introduction

1.1 Committee Remit and Composition

Pursuant to Standing Order 109 (2) (e), the Standing Committee on Foreign Affairs and Defence is mandated to look into matters related to Fiji's relations with other countries, development aid, foreign direct investment, oversight of the military and relations with multi-lateral organisations. The members of the Standing Committee on Foreign Affairs and Defence are as follows:

Hon. Viliame Naupoto
Chairperson of the Standing Committee on Foreign Affairs and Defence

Hon. Lenora Qereqeretabua
Deputy Chairperson
Deputy Speaker of Parliament
Assistant Minister for Housing and Local Government

Hon. Jovesa Vocea
Member
Assistant Minister for Rural and Maritime Development and National Disaster Management

Hon. Isikeli Tuiwailevu
Member
Assistant Minister for i-Taukei Affairs

Hon. Ioane Naivalurua
Member

Committee Secretariat Team

Supporting the Committee in its work is a group of dedicated Parliament Officers who make-up the Committee Secretariat, and are appointed and delegated by the Secretary-General to Parliament pursuant to Standing Order 15 (3) (i). The Secretariat team is made of the following Parliament officers:

- Ms. Susana Korovou – Senior Committee Clerk
- Mrs. Darolin Vinisha – Acting Deputy Committee Clerk

1.2 Background and Terms of Reference

The Standing Committee on Foreign Affairs and Defence, hereinafter referred to as the Committee, was referred the Convention on Cybercrime for review on 1st September 2022. Due to the dissolution of Parliament on 30 October 2022, this Convention was reinstated on 13th February 2023 in the new term of Parliament. The Convention was referred to the Committee pursuant to Standing Order 130 of the Standing Orders of the Parliament of the Republic of Fiji, where the Committee was assigned with reviewing the Convention and to report back on the Convention in a subsequent Parliament Sitting.

1.3 Procedure and Program

(i) Initial Reading of the Convention

The Committee commenced its review by reading through the Written Analysis and Verbatim Reports of the previous Committee. An in-depth deliberation of the Convention was undertaken by the Committee, whereby pertinent issues were identified.

(ii) Public Consultation (written submission and verbal submissions)

In relation to Standing Order 111 (1), the Committee is committed to upholding public trust in Parliament, by ensuring that there is public participation and that all such participation is given due consideration. The previous Committee called for written and verbal submissions from the public and other interested stakeholders by placing an advertisement through the Parliament website and social media platforms (Facebook and Twitter). The Committee ensured that its meetings were open to the public and media, except during Committee deliberations and discussions.

The previous Committee received numerous written submissions on the Convention from relevant stakeholders. The current Committee had called for further submissions from three other stakeholders to provide a more clear position on whether Fiji should ratify the Convention. A summary of these submissions is provided in a latter part of this report, under the heading 'Committee's Deliberation and Analysis of the Convention' and copies of the written submissions can be obtained from the online Appendices of this report, which can be accessed from the Parliament website: www.parliament.gov.fj.

2.0 An Introduction to the Convention on Cybercrime

Recent developments in information and communication technology (ICT) across Pacific Island Countries (PICs) have spawned a rapid increase in access to the Internet and social media, which has greatly influenced the economic, social and political systems in the region. While one may agree that the benefits are enormous, the potential detrimental effects on the countries are significant. Cybercrime has been perceived as one of the greatest threats to national and regional security, economic prosperity and public safety.

The international standardization of communication technology and services allows users to have access to the same worldwide internet services from anywhere around the world, thus cybercrime acts have no physical national borders. Developing countries with inadequate legal and technical foundation are more vulnerable to cyber-attacks.

Adequate and effective safeguards against cybercrime, of which the national legal framework is a fundamental component, should be required in all countries. Every country should enact comprehensive cybercrime legislation that can be enforced to eliminate 'havens' for cyber-criminals and Fiji amongst the many is fortunate that it has enacted its Cybercrime Act in 2021 which came into force on 14 November 2022.

The Budapest Convention ('Convention') is the only legally binding international instrument that provides a comprehensive and coherent framework on cybercrime offences and electronic evidence. It serves as a guideline for any State developing comprehensive national legislation against cybercrime. It is the only international framework for cooperation amongst State Parties ('Parties').

Pursuant to Article 37 of the Convention, any other State, such as Fiji, can become a Party by accession if the State is prepared to implement the provisions of the Convention.

In December 2021, Fiji was invited to accede to the Budapest Convention. The Council of Europe has indicated that the domestic legislation of Fiji "is now broadly in line with the Budapest Convention on Cybercrime." This assessment was recently was supported by the Fiji Law Society, which indicated that many of the Articles of the Convention were reflected in the Cybercrime Act 2021.

At present, the Convention has 67 member States which include Australia and Tonga from the South Pacific region. As of October 2022, twenty two (22) non-State Parties including Canada and the United States of America have ratified the Convention. Besides Fiji, Vanuatu and New Zealand have also been invited with New Zealand considering joining after implementing some incremental changes to legislation.

Cyberspace is a domain that uses the electronic and electromagnetic spectrum to store, modify, and exchange data through network and system-related physical infrastructures. Cybercrime and cybersecurity are two separate issues, Cybercrime under the Budapest Convention deals with illegal access, illegal interception, data interference, system interference, misuse of devices, computer related forgery, and computer related fraud, child pornography and copyright breaches. Cybersecurity are policies, procedures and processes that secure computers, networks, programs and data from unauthorised access, usage or exploitation.

Cybercrime has been around for more than 40 years. The Council of Europe has been dealing with this topic from a criminal law perspective from the mid-1980s onwards. By 2001, the issue had become sufficiently important to warrant a binding international treaty. Negotiated by the member States of the Council of Europe together with Canada, Japan, South Africa and the United States of America, the Convention on Cybercrime was opened for signature in Budapest, Hungary, in November 2001. Since then, information and communication technologies (ICT) have transformed societies worldwide. They have also made them highly vulnerable to security risks such as cybercrime. There are two additional Protocols to the Convention which are the *First Additional Protocol to the Convention on Cybercrime*, also known as the Protocol on Xenophobia and Racism and *Second Additional Protocol on Enhanced Co-operation and Disclosure of Electronic Evidence*.

2.1 Benefits of the Budapest Convention

Any country may make use of the Budapest Convention as a guideline, check list or model law and a large number already make use of this opportunity. Becoming a Party to this treaty entails additional advantages:

1. The Convention provides a legal framework for international cooperation on cybercrime and electronic evidence. Chapter III of the treaty makes general and specific provisions for cooperation among Parties "to the widest extent possible" not only with respect to cybercrime (offences against and by means of computers) but with respect to any crime involving electronic evidence.
2. Parties are members of the Cybercrime Convention Committee (T-CY) which currently is the most relevant intergovernmental body dealing with cybercrime. Parties share information and experience, assess implementation of the Convention, or interpret the Convention through Guidance Notes.
3. The T-CY may also prepare additional Protocols to this treaty. Thus, even if a State did not participate in the negotiation of the original treaty, a new Party is able to participate in the negotiation of future instruments and the further evolution of the Budapest Convention.
4. Parties to the Convention engage with each other in trusted and efficient cooperation. Indications are that private sector entities as well are more likely to

cooperate with criminal justice authorities of Parties to the Convention given that Parties need to have a domestic legal framework on cybercrime and electronic evidence in place, including the safeguards of Article 15.

5. States requesting accession or having acceded may become priority countries for capacity building programmes. Such technical assistance is to facilitate full implementation of the Convention and to enhance the ability to cooperate internationally.

2.2 An Experience from Tonga

In 2003, Tonga adopted its Computer Crimes Act which covers broadly the provisions of the Budapest Convention. In December 2013, Tonga requested accession to the Budapest Convention and in 2017 it became a Party. Following its request for accession in December 2013, Tonga became immediately a priority country of the Global Action on Cybercrime Extended (GLACY+) project. This is a joint project of the European Union and the Council of Europe with an objective to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence, and enhance their abilities for effective international cooperation in this area. In 2016, Tonga became a regional hub for the South Pacific region under the GLACY+ project. This is clear indication that consistent multi-year support is available to permit such States to apply this treaty in practice and to engage in effective international cooperation.

3.0 Committee Deliberation and Analysis

3.1 Oral and Written Evidence Received

The Committee received oral and written submissions from stakeholders and the public as listed in *Appendix A*.

3.2 Evidence received via written and verbal submissions

The previous Committee received eighteen (18) written and verbal submissions and the current Committee received three (3) from invited stakeholders who have direct interest in cybercrime and cybersecurity. All the submissions received were extensively considered and deliberated upon by the Committee. It was noted that submissions received stipulated a range of comments and suggestions which cover various issues pertaining to the Articles of the Convention.

3.2.1 The Fiji Law Society pointed out that terms and definitions in Article 1 of the Convention including *computer system, computer data, service provider and traffic data* are similar to the definitions in the Cybercrime Act 2021. However, it is prudent to note that there is no definition for the terms "cybercrime" and "content data" in the Act.

3.2.2 The submission from the Fiji Women's Crisis Centre supported Fiji's accession to the Convention and recommended that Fiji should consider other Conventions that offer more protection to women and girls such as the Istanbul Convention. This would ensure better protection of our women and girls and recognise that online Gender Based Violence (GBV) is a violation of a woman's human rights. The Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) is the first instrument in Europe to set legally binding standards specifically to prevent gender-based violence, protect victims of violence and punish perpetrators.

3.2.3 In the UNOCHR Submission to the Committee, it was stated that the UN Member States are currently negotiating a new Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. On 26 May 2021, the UN General Assembly (GA) adopted resolution 75/282, according to which a draft convention is to be provided to the GA at its 78th session, which will begin in September 2023 and conclude in September 2024.

3.2.4 The Office of the Director of Public Prosecution was of the view that the Convention represents a progressive move towards the facilitation of greater international co-operation in dealing with cybercrime. It is their submission that Fiji should accede to the Convention with reservations to Articles 27(9) (a-e) and

Article 31 as is allowed for under the Convention. It was also suggested that the Cybercrimes Act and the Juveniles Act require further amendments:

3.2.4.1 Cybercrimes Act should be amended to ensure that all requests from requesting countries go through the Attorney-General as they currently do under Mutual Legal Assistance in Criminal Matters Act (MACMA); and

3.2.4.2 The Juveniles Act should be amended to criminalise the possession of child pornography.

3.2.5 The DPP's Office further recommended that appropriate budgetary resources be allocated to the office of the DPP and other agencies in order to prepare for Fiji's accession to the Convention, particularly with respect to the 24/7 network establishment.

3.2.6 The Citizens' Constitutional Forum Limited had submitted that Freedom of expression and right to privacy are fundamental human rights that are recognized under section 24 of the 2013 Constitution of the Republic of Fiji and the ratified international conventions United Nations International Covenant on Civil and Political Rights (ICCPR) and the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. While these fundamental rights are defined and recognized under the two international instruments, CCF notes that these definitions are not specifically defined within the context of cybercrime i.e. there is no specific definition for privacy and what constitutes freedom of expression. CCF also notes that the current domestic legislation, the Cybercrime Act 2021 does not define these terms. Ambiguous cybercrime laws can give rise to its abuse as the interpretation of its provisions will be dependent on those who are enforcing it.

3.2.7 The Fiji Revenue and Customs Service (FRCS) also indicated their support for the ratification of the Cybercrime Convention. However, the FRCS Act of 1998 allows FRCS to obtain data only for exercising its powers in administrating of tax, and customs and excise laws. It does not provide specific provisions that deal directly with cybercrime. Section 52 of the Act limits FRCS capability to share information for the purpose of combating cybercrime in Fiji as certain conditions need to be met in order for such information to be shared to the relevant enforcement agency. In terms of monitoring and dealing with Cybercrime, FRCS requires the following:

3.2.7.1 Amendment to its existing tax, and customs and excise legislations to ensure that they are compliant with the requirements of the Cybercrime Convention.

3.2.7.2 Provision of more training opportunities for their staff in terms of identifying, monitoring and combating cybercrime.

3.2.7.3 Continuous enhancement of FRCS's current technology to be able to identify, monitor and prevent cybercrime.

3.2.7.4 Increased collaboration with other law enforcement agencies who are responsible for handling any cybercrime issues in Fiji.[1]

3.2.8 The then Ministry of Defence and National Security in their submission in 2022 was of the view that Fiji accede and ratify the Convention without reservation. It recommended more collaborative work and action between the Ministry of Communications and the Critical Infrastructure (CI) agencies on the formulation of a cyber-security legislation and policy framework which would govern CI agencies. The current Ministry of Home Affairs and Immigration proposed that the Cybercrime Act 2021 be reassigned to the portfolio of the Minister of Home Affairs and Immigration.

3.2.9 Mr. Alexander Horne, a Visiting Professor at the Durham University, England submitted that the Convention includes offences that are internationally understood, and which affect all societies. The Convention does not include offences in relation to freedom of expression, political views, national security, or terrorism, which do not have generally accepted definitions. The Convention is strongly rooted in human rights, ensuring that powers are used proportionately. Finally, the Convention is intended as an independent template for co-operation, and its design is clearly focused on supporting investigation and prosecutions.

3.2.10 The Fiji Financial Intelligence Unit (FIU) fully supports the Convention on Cybercrime as it addresses the key gaps that have been experienced in its daily operations. These include cybercrime offences under the Crimes Act, the Proceeds of Crimes Act, the Financial Transactions Reporting Act and the Cybercrime Act. FIU highlighted that it continues to receive information on cybercrime that involves internet banking, ATM skimming, email spoofing, compromised business emails, phishing, spear phishing, identity theft and social media scams. FIU provided a list of case studies related to cybercrime. One such case was from December 2019 to April 2020 where 73 Fijians conducted 163 remittance transactions to 41 individuals in Benin, Africa. The remittance transactions totalled $98,658.00.

3.2.11 The Pacific Islands Forum Secretariat (PIFS) highlighted in their submission that they want the region to be a hard-target for cybercriminals. PIFS in their 2050 Strategy for the Blue Pacific Continent and the Boe Declaration recognises the challenge posed by cybercriminals and the importance of cybersecurity. It is of the

[1] Fiji Revenue and Customs Service (FRCS) Submission

view, that such emerging security threats should be addressed in order to ensure the safety and security of people and the viability of economies, critical infrastructure, data and information.

3.2.12 Fiji's accession to the Budapest Convention would provide further momentum and inspiration for fellow Forum Members to continue their own national efforts to accede. PIFS believed that acceding to the convention is not just in Fiji's interest, but by extension, it is in the region's interest also. They indicated that the Forum Secretariat is aware of a range of support that is available to Forum Members to aid their efforts to accede to the Budapest Convention and want to underscore that Fiji is not alone in its efforts to accede. From the region, Australia and Tonga have acceded to the Convention whilst New Zealand and Vanuatu have being invited to accede.

3.2.13 Mr. Semi Tukana, the founder and owner of SOLE Fintech emphasized that Fiji needs effective encryption for the protection of citizen's data and maintaining economic health. General Data Protection Regulation (GDPR) is now being passed and enforced worldwide to mandate the use of encryption to protect citizen's data. He recommended similar legislation for Fiji. The following steps would need immediate actions by relevant authorities and private companies:

3.2.13.1 Separate storage and management for Keys and Data
3.2.13.2 Clearly segregate duties in certain areas of IT
3.2.13.3 Minimise access rights
3.2.13.4 Tighten encryption

3.2.14 The Online Safety Commission (OSC) reiterated that since establishment, the OSC has witnessed the rise of online abuse primarily as it relates between persons, such as cyberbullying, image based abuse, doxing and more. It is clear that women and girls are disproportionately targeted and abused through online platforms and tools making them more susceptible to gender based online violence.

3.3 Analysis

The Budapest Convention is the only legally binding international instrument that provides a comprehensive and coherent framework on cybercrime offences and electronic evidence.

Fiji's ratification will allow Fiji to partner with countries that are leading the fight against cybercrime, which in turn can only improve the country's capacity for dealing with cybercrime.

Fiji's ratification would assist the region in becoming a hard-target for cybercriminals.

Tonga and Australia have ratified

Submissions from government agencies, law enforcement, private ICT companies, Fiji Financial Intelligence Unit, a treaty specialist, universities, commercial banks and regional bodies made strong recommendations that Fiji should ratify the Convention without any reservations. However, national laws must be consistent with its provisions and the government must consider the most appropriate means of promoting compliance with the treaty.

Other stakeholders including Legal Practitioners and Non-Government Organisations had agreed to the ratification with a few reservations as highlighted.

Fiji is already in a good position with the enactment and enforcement of the Cybercrime Act 2021 and acceding to the Budapest Convention would place Fiji in a better position to meet the challenges of the "twenty fast century". Given the above findings, the Committee strongly recommends that Fiji ratifies the Convention without reservations.

3.4 Other Recommendations

During the consultation process, the Committee noted some of the important issues raised which are highlighted below:

1. That appropriate budgetary resources are allocated and training provided to the relevant agencies to support the implementation of Fiji's ratification to the Convention.
2. That more advocacy and education on cybercrime and cybersecurity are provided to the general public including students.
3. That Fiji carefully consider and amend relevant national laws including the Cybercrimes Act 2021, Juveniles Act and the Online Safety Act 2018 to address issues highlighted in this report.
4. That Fiji clarifies the role and responsibility of existing law enforcement and state agencies in relation to dealing with cyber-attacks and cybercrime.
5. That Fiji considers the recommendation from the Ministry of Home Affairs and Immigration that the Cybercrime Act 2021 be under its portfolio.
6. That Fiji should consider other Conventions that offer more protection to women and girls such as the *Istanbul Convention.*
7. That Fiji should anticipate the release of the new *United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes* that will be tabled in the 2023 United Nations General Assembly in September to see if it will complement the benefits provided by the Budapest Convention.

8. That to better guard against Cybercrime, companies, authorities and individuals need to implement Cyber Hygiene to keep sensitive data secure and protect it from theft or attacks.
9. That Fiji recognises the capabilities and expertise of local system designers and developers to see if they can be utilised to design and develop critical data and systems infrastructures.

4.0 Gender Analysis

Whilst reviewing the Convention, the Committee was mindful of the impacts of cybercrime activities on Fiji's efforts in achieving the UN Sustainable Development Goals (SDGs) and the efforts towards its National Development Plan (NDP). At the initial stage, the Committee has considered the importance of the Convention which is to enhance Fiji's ability to combat cybercrime, with international support and assistance particularly in relation to continued capacity building, to better equip Fiji's criminal justice authorities, including the judiciary, prosecution and law enforcement agencies.

This objective relates to the ambitious development plan and goal by the Government of Fiji regarding information and communication technology (ICT) and its utilisation and adoption of new and better technology for and enhancing services in Fiji. In order to improve productivity and ensure better service delivery, there were plans to improve universal access to information and competitive telecommunication services, which are delivered on a secured platform.

This then brings to the forefront the Fijian Government's priority of creating a safe cyber environment. The Committee was mindful of the requirements of the Standing Orders of Parliament regarding gender, which is also a key goal in the sustainable development goals.

The Committee ensured that full consideration were given to the principle of gender equality so as to ensure all matters are considered with regard to the impact and benefit on both men and women equally. Despite the lack of gender-related information during the review, it is evident from the deliberations on the Articles of the Convention that it was designed to impact all Fijians, irrespective of gender.

Therefore, the ratification of the Convention on Cybercrime takes into consideration the implications of information and communication technology on development and that it is designed to impact every person, irrespective of gender.

If Fiji decides to accede or ratify this Convention, then we urge that Fiji integrates a gender perspective in the implementation and enforcement of the Convention in our domestic context. This will help us to create effective laws, policies and procedures to efficiently prevent and combat cybercrime.

We also urge that Fiji also considers other conventions which offer more protection to women and girls such as the Convention on Preventing and Combatting Violence Against Women and Domestic Violence (Istanbul Convention), to work hand in hand with the Budapest Convention to ensure better protection of our women and girls and the recognition of online GBV being a violation of a woman's human rights.[2]

[2] FWCC submission

5.0 Conclusion

The Standing Committee on Foreign Affairs and Defence has fulfilled its mandate approved by Parliament which is to review the Convention on Cybercrime and recommends that Fiji ratifies the Co

6.0 Members' Signature

Hon. Viliame Naupoto
Chairperson

Hon. Lenora Qereqeretabua
Deputy Chairperson

Hon. Jovesa Vocea
Member

Hon. Isikeli Tuiwailevu
Member

Hon. Ioane Naivalurua
Member

7.0 Appendices

All other written and transcribed evidences gathered during the public submissions and public consultations will be made accessible on the Parliament website on: http://www.parliament.gov.fj/committees/standing-committee-on-foreign-affairs-and-defence/

No.	Date	Time	Ministries/Agencies
1.	Tuesday 20.09.2022	10.14am	University of Fiji
2.	Monday 26.09.2022	9.58am	Ministry of Communications
3.	Tuesday 27.09.2022	9.30am	University of the South Pacific
4.		10.30 am	Fiji Women's Rights Movement (FWRM)
5.		11.00am	Fiji Law Society
6.	Monday 03.10.2022	9.31am	Fiji Independent Commission Against Corruption (FICAC)
7.		11.24am	Fiji Intelligence Unit (FIU)
8.		12.22pm	Citizens Constitutional Forum (CCF)
9.	Tuesday 04.10.2022	9.30am	Ms. Salanieta Tamanikaiwaimaro
10.		10.30am	Datec Fiji Limited
11.		10.50am	Fiji Police Force
12.		11.20am	Fiji Human Rights and Anti-Discrimination Commission
13.		10.25am	Office of the Director of Public Prosecutions
14.		11.01am	Fiji Women Crisis Centre
15.	Monday 17.10.2022	10.05am	Fiji Revenue and Customs Service (FRCS)
16.		11.00am	Bank of the South Pacific (BSP)
17.		Written Submission	Ministry of Defence, National Security and Policing
18.		Written Submission	Mr. Alexander Horne

19.	Thursday 13.04.2023	Oral Submission	Mr. Semi Tukana – Founder and Chairman of SOLE Fintech
20.		Oral Submission	Pacific Islands Forum Secretariat (PIFS)
21.	Thursday 27.04.2023	Oral Submission	Online Safety Commission
22.	Tuesday 02.05.2023	Oral Submission	Ministry of Home Affairs and Immigration