SCHEDULE A

PART & SECTION	CURRENT NARRATION	COMMENTS & RECOMMENDATIONS
PART 1 **Section 2 Interpretation**	**Definition of 'authorised person'** is "*includes*" any person that is authorised by FICAC.	The current definition is ambiguous. The definition needs to specify who the authorised persons are. The penalties and offences in the Bill are serious, therefore certainty must be provided. FICACC was not set up to prosecute criminal matters concerning all citizens. FICACC is a special vehicle agency set up to investigate corruption related charges concerning public servants and offices and not offences between private citizens. This Bill is not limited to public servants and offices. Therefore, criminal prosecution under this Bill must be vested with the ODPP whose officers are qualified lawyers experienced in prosecutions of a wide range of criminal activities. Cybercrimes and activities included under this definition are serious crimes that must be handled by the criminal prosecutions specialised agency the ODPP and not FICACC. FICACC has no business prosecuting criminal matters which the ODPP was set up to do. **Recommendations:** **1. Set up of a Fiji High Tech Crime Centre as part of the Fiji Police Force for investigations (similar to Australian High tech Crime Centre);** **2. Delete FICACC and insert ODDP** **3. Suggested redraft: "authorised person" includes any person authorised and appointed by the ODPP.**
	No definition of *"person"*.	The Interpretation Act defines "person" to include legal entities, we recommend that a specific definition should be included for "person" in the context of the Bill to avoid confusion. Also, the implications of the Bill on institutions and entities whose entire business is electronically stored and implemented, such as a bank, are serious. More clarity is supportive rather than harmful to the purposes of this law. **Recommendation:** **4. Include a definition of person for purposes of this Act**

	No definition of "*cybercrime"*	Cybercrime is a terminology that is usually associated with the internet but this Bill does not concentrate only on the internet. In fact, it include a wide range of activities and even a hybrid of traditional crimes e.g. organised crime or online money laundering as well as new types of crimes that committed on cyberspace such as hacking and contaminating online storages/databases. Similar laws in other jurisdictions provide extensive lists of acts that constitute cybercrime. The absence of a definition, or some guidance as to what it includes is important for the number of reasons: i. A definition provides clarity for citizens and for charged persons, allows clarity with regards to mounting their defences ensuring safeguards against the abuse of fundamental rights of all Fijians. ii. The inclusion of acts that constitute cybercrime also provides a perimeter for the police and investigating agencies of government so that they do not have unfettered powers as to what constitutes a cybercrime or use it to go on a fishing expedition against targeted persons. **<u>Recommendations</u>:** **5. Include a definition of "Cybercrime".** ***Refer to examples of provisions from Philippines, provided on pages 5-7.***
PART 2	**Sections 5, 6, 7, 8**	Division 6 of the Crimes Act of Fiji already deals with authorised access, modification, impairment, possession and control, production and supplying of computer data, communications and program. Any expansion of the offences by the Bill can be incorporated into the current Crimes Act instead of creating a whole new Act.

Section 5	Unauthorised access to computer systems	The provision makes the unauthorised access the offence. The provision should also provide for the purpose of the access. It is possible for a person to gain unauthorised access into a system for the sole purpose of finding out information which is not used for any criminal purposes. This is the reason it is important to include a definition of cybercrime because the access must be tied to the purpose of committing a cybercrime. This provision must provide certainty as to its application so it is not used by police or prosecuting agencies of government for a fishing expedition which can ruin a person's reputation. There is likely to be unintended consequences of the current wording of this provision. For example, a whistle-blower who gains unauthorised access to his company's system for the purposes of whistle blowing criminal activities of company is caught under s.5, 6 and 7 even though his intention was not to commit a crime but to expose a crime. Note also that it is possible to have authorised access and commit a cybercrime using that access. **<u>Recommendations</u>:** **6. Include a definition of cybercrime;** **7. Delete references to unauthorised access** **8. Amend ss (1) as follows: ….***any person who intentionally causes a computer system to perform a function or series of functions to secure access to the computer system for the purposes of committing a cybercrime, commits an offence ….* Please refer to wording in s9-12 for similar wording **9. Include excluded persons e.g. a whistle-blower**
Section 6	Unauthorised interception of computer data and computer systems	Comments on Section 5 above relevant. Please refer to comments on Section 5.
Section 7	Unauthorised acts in relation to computer data or computer systems	Comments on Section 5 above relevant. Please refer to comments on Section 5.

PART 3 **Sections 9, 10**	Computer related and content related offences	These sections deals with computer related *forgeries*, *extortion* and *fraud*. These sections can be incorporated to Division 6 of the Crimes Act to expense the scope of the said Division.
	Penalties against entities/ body corporates	Offences in these sections are offences that individual persons commit. To prove that the body corporate knew of the acts of the individual or condoned the actions requires a separate provisions. **<u>Recommendation</u>:** **10. Insert new provision as follows….*a body corporate who is possessing, dealing, handling any sensitive information ad is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or gain to any person shall be guilty of an offence under this section …..etc.*****
PART 4 **Sections 11,12**	Penalties against entities/ body corporates	Please refer to comments for sections 9,10 above
Section 13	Disclosure during an investigation	This section is confusing. Subsection (1) needs to clarify whom the disclosure need to be made to for that act to become and offence – the current wording may include disclosing such order to an investigator is also an offence? In addition, a person who is being investigated must be allowed to disclose details of the investigation to his legal counsel for the purposes of obtaining legal advice. **<u>Recommendation</u>:** **11. Clarify wording of ss(1): …any person who, without unlawful or reasonable excuse, discloses <u>to another person</u> during an investigation …..** **12. Make provision to allow disclosure to legal counsel for purposes of legal advice.**

PART 5 **Section 16**	Search and seizure	The Bill does not provide guidance to the Court. The provision must provide the minimum requirements the police must present to the Court when applying under this section. This not only provides clarity but also assists the Court who may have very little experience and knowledge in cybercrime offences to make a ruling. Section 20(5) of the Bill is an excellent example of a guideline. This prevents the abuse of the warrant and seizure of legal and lawful confidential information. It also prevents the seizure of personal information or data that does not relate in any way to an investigation. The section must provide for strict confidential to the police for any information seized under this section except such information, data or system that proves an offence. In addition, the police must be prohibited from using any information they find under a warrant to charge a person for another offence. In the event that police refused to give access or provide copies to the owner of any seized property under this section, the section must provide reason for refusal and such refusal can be appealed. **<u>Recommendation</u>:** **13. The provision to specify the evidence to be produced by police, specific list of information to be seized under the warrant and reasons** **14. Include a strict confidential clause for police from using any other information seized under this section except such information, data or system that proves an offence;** **15. Include a clause that prohibits the police from using any unrelated information they find under a warrant to charge a person for another offence;** **16. Where police refused to give access or provide copies to the owner of any seized property under this ss(6), specific reasons for refusal and such refusal can be appealed.**

Section 18, 19	Expedited preservation of stored computer data Expedited preservation and partial disclosure of traffic data	While we understand the need to expeditiously preserve, however more strict guidelines for the issuance of such notice that is not sanctioned by a court. The balance of individual rights and the need for investigation must have a balance. **<u>Recommendation</u>:** **17.** Police or authorised person must obtain a warrant before the seizure of such information or system.
Section 20	Production order	**<u>Recommendation</u>:** **18. Make provision for an interim order to be granted to preserve the data or system until final determination of whether to grant the production order.**
Section 21(3)	Search and seizure of stored computer data	**<u>Recommendation</u>:** **19.** This provision be deleted. A scope of any search should be confined to the order of the court and not extended at the discretion of the police or authorised officer. Tis can lead to an abuse of power that can cause irreparable damage to reputation and business,.
PART 6 **Section 24**	International Cooperation	**The FLS agrees with the inclusion of this Part**

ANNEXURE

Philippines Republic act no.10175

CHAPTER II
PUNISHABLE ACTS

SEC. 4. *Cybercrime Offenses.* — The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

(1) Illegal Access. – The access to the whole or any part of a computer system without right.

(2) Illegal Interception. – The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

(3) Data Interference. — The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

(4) System Interference. — The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

(5) Misuse of Devices.

(i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

(aa) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or

(bb) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.

(ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section.

(6) Cyber-squatting. – The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

(i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration:

(ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

(iii) Acquired without right or with intellectual property interests in it.

(b) Computer-related Offenses:

(1) Computer-related Forgery. —

(i) The input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; or

(ii) The act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

(2) Computer-related Fraud. — The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: *Provided,* That if no

damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(3) Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: *Provided,* That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(c) Content-related Offenses:

(1) Cybersex. — The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

(2) Child Pornography. — The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: *Provided,* That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

(3) Unsolicited Commercial Communications. — The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:

(i) There is prior affirmative consent from the recipient; or

(ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or

(iii) The following conditions are present:

(aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject. receipt of further commercial electronic messages (opt-out) from the same source;

(bb) The commercial electronic communication does not purposely disguise the source of the electronic message; and

(cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

(4) Libel. — The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

SEC. 5. *Other Offenses.* — The following acts shall also constitute an offense:

(a) Aiding or Abetting in the Commission of Cybercrime. – Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

(b) Attempt in the Commission of Cybercrime. — Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: *Provided,* That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

SEC. 7. *Liability under Other Laws.* — A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.