1. INTRODUCTION

1.1. PURPOSE AND OBJECTIVE OF THE REVIEW

1.1.1. The Mapping and Analysis of National cybercrime laws in the Commonwealth forms part of the comprehensive legal reform embarked upon by some Commonwealth countries, in support of the implementation of the Commonwealth Cyber Declaration (CCD). This project is funded by the United Kingdom Foreign, Commonwealth and Development Office (FCDO). The project which falls under the purview of the Commonwealth Secretariat’s Rule of Law section, is designed to comprehensively review all national laws to determine their direct and indirect impact on cybercrime in the Commonwealth.

1.1.2. The Terms of Reference (TOR) provide that the main objective of this assignment is to conduct a mapping of the entire cybercrime legal landscape of the Commonwealth. This would include all statutes and legislative instruments, executive orders, administrative regulations, case law and other relevant and related government texts. It is expected that the mapping and analysis will be in line with the Commonwealth Heads of Government commitments via the Commonwealth Cyber Declaration and other international and regional treaty obligations. The comprehensive mapping will form the basis of future work to provide technical assistance and build consensus on cybercrime across the Commonwealth.

1.2. CONTEXT IN THE COMMONWEALTH

1.2.1. The digital age is being accelerated by the unfolding COVID-19 global pandemic. New opportunities and challenges have arisen, including (a) threats to peace and
security; (b) emergence of new trade and economic patterns; (c) contestations on democracy, human rights, rule of law, and other political values; and (d) and the growth of new economic models. Previously unimagined access to information and communication between individuals and both state and non-state entities across the globe is driving economic and social development in the 21st century. Cyberspace is already serving as a global central nervous system, enabling hyper-connectivity, helping both to bridge and extend digital divides and influencing every aspect of economic and social life. Cyberspace continues to develop at a pace unparalleled in human history - growth in the cyber economy rose from USD 112.01 billion in 2019 and is projected to reach USD 281.74 billion by 2027 (Forbes 2020). Much of this growth will be in developing countries. This pace of change necessitates urgent action in reaching consensus on rules-based governance frameworks for Cyberspace.

1.2.2. Cyberspace’s open, decentralised and distributed nature, that empowers the individual, has fostered innovation, collaboration and rapid development. Enjoyment of those benefits relies upon its safety, security and resilience. Cyberspace has also opened opportunities for crime, extremism and other social ills. Governments, industry, civil society and users have a shared responsibility to tackle those threats to society. Necessary security measures may be in tension with the very features that have made Cyberspace a success and, in determining an equitable balance, our behavior in Cyberspace will benefit from the shared Commonwealth values that govern many aspects of our lives.

1.2.3. Cybercrime is, of course, not new. But increased interconnectivity and growth in the digital economy is exponentially opening opportunities for complex transnational crime. The UK Association of Chief Police Officers (ACPO) has defined cybercrime as - the "use of networked computers, telephony or internet technology to commit or facilitate the commission of crime". Robust and up to date strategic plans, legislation, policies, and institutions to counter cybercrime are a sine qua non to Commonwealth countries’ ability to effectively deter and tackle cybercrime. In addition to the legal framework, countries need to have law enforcement and criminal justice systems that are equipped to enforce anti-cybercrime policy and legislation. The trans-national nature of cybercrime heightens the need for common legal standards and cooperation frameworks that facilitate cross-border cooperation in criminal investigations.

1.2.4. The Commonwealth Cyber Declaration (CCD) endorsed by Commonwealth Heads of Government in 2018 is an important expression of the Heads’ desire to maintain a free, open, inclusive and secure cyber space. The Declaration sets out, for the first time, a common vision for ensuring the internet remains free, open and inclusive across the Commonwealth. It is a call to action for countries to exploit the Commonwealth “advantage” namely, the common law, a common official language, similarity of public institutions, shared values and the convening powers of the Commonwealth Secretariat to harness the benefits of and lessen the challenges associated with the use of cyberspace.
2. KEY ISSUES

2.1. Upon consideration of the Commonwealth Cyber Declaration, and in accordance with the TOR, the following issues will be addressed in the Mapping Report:

a. Relevant national cybercrime policies, strategies, legislation and institutional frameworks.

b. Barriers to cybercrime prosecutions and mutual legal assistance in international criminal matters

c. Number of cybercrime prosecutions and applicable caselaw

d. Institutional strengthening that is required to build capacity to tackle cybercrime.

e. Current status of awareness and online behaviors

f. Protection of online rights and status of gender based online crimes including violence against women and girls and other vulnerable groups

g. The role of stakeholders such as academia, civil society including consumer protection and human rights organisations.

3. METHODOLOGY OF THE REVIEW

3.1.1. The nature of the assignment requires in-depth research into current legislation and legal provisions, for the development of a comprehensive cybercrime Legislative Mapping Report which will provide Commonwealth countries with an adequate guide, which will help to inform law reform processes. The laws and legal provisions to be considered in the Mapping Report are those relevant to cybercrime, including computer misuse, electronic evidence and cybersecurity and other international cybercrime commitments related to these instruments. In fulfilling the TOR, the outline of the Report is as detailed below.

3.1.2. The introductory part of the report will contain brief background information on the plural legal, political, social, economic and cultural context relating to cybercrime.

3.1.3. Part I of the Mapping Report will consider the Commonwealth’s collective international cybercrime treaty obligations (including the Commonwealth Cyber Declaration) and the steps taken by Commonwealth Governments to domesticate international instruments or legal frameworks ratified by Commonwealth Heads of Government. In addition to these, the Secretariat will also consider the steps that Governments have taken to implement the recommendations made in the Commonwealth Cyber Declaration.

3.1.4. The following international instruments will be highlighted under Part I of the Report:

a. Council of Europe Convention on Cybercrime (2001) - (Budapest Convention)

3.1.5. Part II of the Report will cover an in-depth analysis of domestic legislations such as the Constitution, statutes, sectoral laws, and the role played by the Courts in addressing cybercrime. The in-depth review will help determine how far Commonwealth countries have gone in complying with the international obligations highlighted in Part I above, and map out and identify gaps and shortfalls in the legal and legislative framework. This would enable the Secretariat to provide a consolidated picture of the state of cybercrime policy and legal framework across the Commonwealth.

3.1.6. Part III of the Report will entail comprehensive recommendations based on the analysis of Commonwealth countries’ commitment to the Commonwealth Cyber Declaration and other listed international instruments and the domestication of these provisions in national legislation. The recommendations will outline steps taken to implement the Declaration, the gaps in the current legislations and relevant or related policy documents, and the basis of the conclusions made. This would serve as a guide to Commonwealth countries in the development of domestic laws in line with international obligations and best practices. The details of the specific recommendation on the provisions of statutes, relevant to the subject matter and thematic areas highlighted above will be provided in the Mapping Table in the Annex to the Report.

4. CONSULTATION WITH STAKEHOLDERS

4.1.1. To ensure a participatory and inclusive process for the execution of this assignment, an Expert Review Committee should be established by the Commonwealth Secretariat, consisting of a small group of stakeholders to provide input and review all deliverables under this assignment, prior to publication. The Expert Review Committee would be constituted by key stakeholders directly involved in combatting cybercrime. This Expert Review Committee will include:

a. Two representatives from Commonwealth Member Countries
b. One representative from a Commonwealth Judiciary, nominated by the Commonwealth Magistrates and Judges Association
c. Two Representatives from Commonwealth Law Associations
d. One representative from the United Kingdom Foreign and Commonwealth Office Cyber Programming
e. One representative from UNODC
f. One representative from The Council of Europe
g. Two representatives from Commonwealth Secretariat Governance and Peace Directorate (Good Offices and Human Rights Unit).

4.1.2. The Review Committee will hold one hybrid meeting. The Committee meeting will review and provide comments on the drafts of the Mapping Report, prior to
publication. Comments received from the Committee will be incorporated in the drafts. This would ensure that the appropriate recommendations are made in the final Mapping Report.

5. OUTLINE OF THE NATIONAL LAWS MAPPING REPORT

5.1.1. The following outline will be used in the Mapping Report:

INTRODUCTION:

a. **Background**: The plural legal, political, social, economic and cultural context of The Commonwealth and its implications on the management of cybercrime.

PART I:

a. The Commonwealth’s commitments to international cybercrime legal instruments/treaties/frameworks

PART II: DOMESTIC LAWS (Identifiable gaps in the law, gaps in implementation and the reasons for such gaps)

a. **CONSTITUTION** - provisions advancing cybercrime prosecution and the protection of rights online
b. **STATUTES** - Impact on cybercrime
c. **SECTORAL LAWS** - Impact on cybercrime
d. **JUDICIAL DECISIONS** - role that courts and tribunals have played in: (a) advancing cybercrime prosecutions; (b) reinforcing rights online

6. METHODOLOGY

6.1.1. The Consultant(s) - in close consultation with the Project Manager - will be expected to:

a) conduct desk reviews of literature and materials from across the respective region of the Commonwealth.

b) Write and present a detailed report to the Secretariat

7. SPECIFIC TASKS TO BE PERFORMED BY THE CONSULTANT

7.1.1 Under the guidance of the Project manager the following outputs and deliverables are expected for the completion of this assignment:

a. Review existing literature on cybercrime and the laws, policy and institutional framework in the respective region of the Commonwealth.

b. A draft outline of the report and methodology to be applied and sources of information used by the Consultant 3rd **MARCH 2021**.
c. Submission of first draft of the Mapping Report to the Commonwealth Secretariat 26th MARCH 2021.


e. To deliver by no later than 30th APRIL 2021 the final Mapping Report to the Commonwealth Secretariat.

Note: The above-mentioned tasks to be performed are intended as a guide and should not be viewed as an inflexible specification as it may be modified following discussion with the selected consultant.

8. EXPECTED TANGIBLE AND MEASURABLE OUTPUT(S)/DELIVERABLE(S):

<table>
<thead>
<tr>
<th>Deliverables</th>
<th>Timelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Draft outline of the report and methodology</td>
<td>19th March 2021</td>
</tr>
<tr>
<td>2. Presentation draft version of the report</td>
<td>16th April 2021</td>
</tr>
<tr>
<td>3. Receipt of comments from the Expert Review Group</td>
<td>7th May 2021</td>
</tr>
<tr>
<td>4. Presentation of satisfactory final version of the report that takes into account the Secretariat’s feedback.</td>
<td>28th May 2021</td>
</tr>
</tbody>
</table>

9. INDICATORS TO EVALUATE THE CONSULTANT’S PERFORMANCE

All outputs shall be assessed in accordance with the following indicators:

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>a, b, c and d</td>
<td>• Technical precision of the proposal</td>
</tr>
<tr>
<td></td>
<td>• Clear and policy-relevant analysis</td>
</tr>
<tr>
<td>a, b, c and d</td>
<td>• All Secretariat comments reflected appropriately</td>
</tr>
<tr>
<td></td>
<td>• Excellent English drafting style</td>
</tr>
<tr>
<td></td>
<td>• Political nuances fully considered</td>
</tr>
<tr>
<td></td>
<td>• Technical excellence</td>
</tr>
</tbody>
</table>

10. QUALIFICATIONS/EXPERTISE SOUGHT (REQUIRED EDUCATIONAL BACKGROUND, YEARS OF RELEVANT WORK EXPERIENCE, OTHER SPECIAL SKILLS OR KNOWLEDGE REQUIRED)

- Qualified lawyer in a Commonwealth jurisdiction.
- Advanced degree(s) in law, politics, social science, or international relations;
- Minimum of 10 years of professional expertise in criminal justice and international cooperation in criminal matters, with a focus on electronic evidence and cybercrime;
- Practical professional experience in provision of advice and training to justice system officials;
- Proven ability to network and establish collaborative relationships with a variety of actors;
- Strong research design skills, including capacity to prepare logical, coherent, and consistent reports.
- Prior demonstrated experience from designing and conducting research for institutional donors and for multilateral, bilateral and vertical funding sources.
- Proven ability to work well under pressure and meet strict deadlines.
- Flexibility to adapt to any subsequent changes in the terms of reference.
- Excellent English speaking/writing skills required.
- Strong interpersonal and communication skills.
- Strong analytical, reporting and writing abilities.
- Very good understanding on using MS Word and Excel as well as other relevant MS office software.
- Openness to change and ability to receive/integrate feedback.
- Positive, constructive attitude to work.
- Displays cultural, gender, religion, race, nationality and age sensitivity and adaptability.
- Demonstrates integrity and ethical standards.

11. ADMINISTRATIVE ARRANGEMENTS

The tasks associated with this Terms of Reference are expected to be completed through a home-based preparatory and coordination work. Virtual conference calls will be the main mode of meetings with the Secretariat and other key stakeholders.

The consultant will receive payments on a payment schedule and in accordance with the terms of the consultancy offer letter.

12. ASSUMPTIONS

a. Full cooperation of the identified government institutions, civil society organizations and other stakeholders in providing feedback and input during the review process.

b. Timely feedback from the Commonwealth Secretariat through its Rule of Law Section, to avoid delays in the production of the deliverables.

13. RISKS

a. That the duration within which this assignment is to be completed would be inadequate for a comprehensive mapping and analysis in the manner envisaged by the Commonwealth Secretariat.

b. Any delay in receipt of comments from the Commonwealth Secretariat, and the Review Committee, would affect the delivery of the revised report by the stated deadline.
14. TEAM OF EXPERTS

TBD Consultant

The Consultant will be assisted in this assignment, mainly, by Ms. Elizabeth Bakibinga Legal Adviser, and other professional staff supporting the Consultant.