

PROPOSED AMENDMENTS TO THE NATIONAL CRIME AGENCY BILL 2026

Volume I — Clause-by-Clause Comparative Text and Legislative Rationale

PHASE III — CLAUSES 31 TO 59

Prepared by	Dave Kissoondoyal, MBA, LL.M (Cyberlaw), MBCS, MCMI
Purpose	Phase III technical submission for parliamentary scrutiny and consideration
Source text	The National Crime Agency Bill 2026 as circulated
Date	27 September 2026
Submitted to	Leader of the Opposition
Copy to	Opposition Whip
Scope	Clauses 31–59: whistleblowing, investigative powers, digital evidence, surveillance, arrest/detention and prosecution safeguards

This Phase III follows the institutional and governance amendments transmitted in Phase II. It sets out the detailed clause-by-clause proposed amendments to clauses 31–59, covering whistleblowing, allocation of investigative responsibility, compulsory questioning, search and seizure, financial and digital information powers, preservation and production of electronic evidence, interception and surveillance, arrest and detention, and the role of the Director of Public Prosecutions. Subsequent phases will address clauses 60–85 and the National Crime (Interim) Agency Bill 2026.

Drafting Key and Method

BLACK	Government text retained or reproduced for comparison.
RED STRIKETHROUGH	Government wording proposed for deletion or replacement.
BLUE BOLD	New or replacement legislative wording proposed.
BLUE SHADED RATIONALE	Reason for the amendment, including independence, accountability, due-process, privacy or drafting considerations.

The document uses the Government Bill as the baseline. Clauses are classified as RETAIN, AMEND or REWRITE / INSERT. The purpose is not to alter provisions unnecessarily, but to identify where additional safeguards, precision, judicial control or institutional separation may be warranted.

Legal reference points used in this Phase include sections 3, 5, 9 and 10 of the Constitution of Mauritius; the Data Protection Act 2017, including necessity, proportionality, security and accountability requirements; the statutory recognition of law-practitioner/client privilege in the Law Practitioners Act; and Articles 15–21 of the Budapest Convention on Cybercrime as comparative safeguards for preservation, production, traffic-data collection and content interception. These references guide the proposed safeguards but do not replace the need for Parliamentary Counsel to reconcile the final text with all related enactments.

Clauses 31–46: Amendment Matrix

Cl.	Subject	Status	Principal issue
31	Reporting obligations	AMEND	Protect judicial/prosecutorial independence, privilege and voluntary public reporting.
32	Procedure for making disclosure	AMEND	Anonymous/secure channels, identity protection and electronic reporting.
33	Protection against victimisation	AMEND	Broader retaliation protection and reasonable-belief standard.
34	Report to Independent Advisory Panel	AMEND	Secure complaints, representation and urgent interim protection.
35	Enquiry by Independent Advisory Panel	AMEND	Fair procedure, written reasons and time discipline.
36	Other whistleblower measures	AMEND	Independent reporting protocol and anonymised annual accountability.

Cl.	Subject	Status	Principal issue
37	Determination of complex, serious and organised crime	REWRITE	Objective jurisdictional threshold; PEP/public-interest factors not sufficient alone.
38	Investigation by NCA or other investigative body	REWRITE	No unilateral displacement of other bodies; remove blanket importation of Police powers.
39	Investigation not void or impeachable	REWRITE	Preserve court supervision; incidental offences referred unless integral.
40	NCA investigative officer	AMEND	Written designation, identification, training and accountable use of force.
41	Questioning and production of evidence	REWRITE	Notice safeguards, counsel, privilege, review and proportionate offences.
42	Refusing to give evidence	REWRITE	Self-incrimination, privilege and DPP-controlled use/derivative-use immunity.
43	Warrant for entry, search and seizure	REWRITE	Judicial warrant for private searches; digital and privileged-material safeguards.
44	Judge's Order for financial institution	AMEND	Necessity, proportionality, scope limits, inventory and privilege protocol.
45	Seizure of property	REWRITE	Judicial confirmation, return/review rights and third-party safeguards.
46	Disclosure of account and customer information	REWRITE	Remove public-interest-alone test; narrow orders; strengthen legal privilege and preservation limits.

CLAUSE 31 — REPORTING OBLIGATIONS

STATUS	AMEND	Protected reporting and institutional independence
--------	-------	--

Government text

31. Reporting obligations

(1) Notwithstanding any enactment, where, in the discharge of his functions –

- (a) a judicial officer;
- (b) the Director of Public Prosecutions;
- (c) the Commissioner of Police;
- (d) the Director-General of the Mauritius Revenue Authority;
- (e) the Governor of the Bank of Mauritius;
- (f) the Director of the Financial Intelligence Unit;
- (g) the Ombudsman;
- (h) the Director of Audit;
- (i) any other public official;
- (j) any other person,

has reasonable grounds to believe that –

- (i) a financial crime, a cybercrime or other complex, serious and organised crime has been, is being, or is likely to be, committed;
 - (ii) a person has in his possession properties which are suspected to be proceeds, instrumentalities or terrorist properties; or
 - (iii) a person has acquired unexplained wealth,
- he shall make a disclosure of impropriety to the NCA.

(2) For avoidance of doubt, a declaration of impropriety may be made by an NCA officer to the NCA.

Proposed amendment

~~(1) Notwithstanding any enactment, where, in the discharge of his functions –~~

~~(a) a judicial officer;~~

~~(b) the Director of Public Prosecutions;~~

~~(c) the Commissioner of Police;~~

~~(d) the Director-General of the Mauritius Revenue Authority;~~

~~(e) the Governor of the Bank of Mauritius;~~

~~(f) the Director of the Financial Intelligence Unit;~~

~~(g) the Ombudsman;~~

~~(h) the Director of Audit;~~

~~(i) any other public official;~~

~~(j) any other person;~~

~~has reasonable grounds to believe that –~~

~~(i) a financial crime, a cybercrime or other complex, serious and organised crime has been, is being, or is likely to be, committed;~~

~~(ii) a person has in his possession properties which are suspected to be proceeds, instrumentalities or terrorist properties; or~~

~~(iii) a person has acquired unexplained wealth;~~

~~he shall make a disclosure of impropriety to the NCA.~~

(1) Subject to subsections (1A) to (1C), where the Commissioner of Police, the Director-General of the Mauritius Revenue Authority, the Governor of the Bank of Mauritius, the Director of the Financial Intelligence Unit, the Ombudsman, the Director of Audit or any other public official, in the discharge of official functions, has reasonable grounds to believe that a matter referred to in paragraph (a), (b) or (c) below has occurred, is occurring or is likely to occur, that person shall, as soon as reasonably practicable and to the extent permitted by law, make a disclosure of impropriety to the NCA –

- (a) a financial crime, cybercrime or other complex, serious and organised crime;**
- (b) possession of property reasonably suspected to constitute proceeds, an instrumentality or terrorist property;**
or
- (c) acquisition of unexplained wealth.**

(1A) A judicial officer or the Director of Public Prosecutions may make a disclosure under this section only where such disclosure is permitted by the Constitution and any other applicable law and is compatible with judicial or prosecutorial independence and any duty of confidentiality attaching to the office.

(1B) Any other person may voluntarily make a disclosure of impropriety to the NCA.

(1C) Nothing in this section shall compel the disclosure of material protected by legal professional privilege, judicial confidentiality or any other privilege or immunity recognised by law.

(2) For avoidance of doubt, a declaration of impropriety may be made by an NCA officer to the NCA. (2) For the avoidance of doubt, an NCA officer may make a disclosure to the NCA and, where the disclosure concerns the Director-General, Deputy Director-General, Director of the Internal Affairs Division or conduct reasonably capable of compromising an internal NCA inquiry, directly to the Independent Advisory Panel or other independent authority designated by law.

Rationale

The circulated clause imposes a single mandatory route to the NCA on judicial officers, the DPP, public officials and even any other person. The amendment preserves mandatory reporting for public authorities while protecting judicial/prosecutorial independence, legal professional privilege and other protected duties. It also creates an independent reporting route where the alleged impropriety concerns senior NCA leadership.

CLAUSE 32 — PROCEDURE FOR MAKING DISCLOSURE

STATUS	AMEND	Anonymous, secure and confidential disclosure
--------	-------	---

Government text

32. Procedure for making disclosure

- (1) A disclosure of impropriety may be made in writing or orally.
- (2) The disclosure of impropriety shall contain, as far as practicable –
 - (a) the full name, address and occupation of the whistleblower;
 - (b) the nature of the impropriety in respect of which the disclosure is made;
 - (c) the particulars of the person who is alleged to have committed, is committing or will commit, the impropriety;
 - (d) the time and place where the alleged impropriety took place, is taking place or is likely to take place; and
 - (e) the full name, address and description of the person, if any, who witnessed the commission of the impropriety.
- (3) (a) Where a whistleblower makes a disclosure orally, the person to whom the disclosure is made shall cause the disclosure to be recorded in writing.
- (b) The disclosure referred to in paragraph (a) shall contain the information required under subsection (2).

Proposed amendment

- ~~(1) A disclosure of impropriety may be made in writing or orally.~~ **(1) A disclosure of impropriety may be made in writing, orally, electronically or through any secure reporting channel approved under this Act, and may be made anonymously.**
- ~~(2) The disclosure of impropriety shall contain, as far as practicable –~~
~~(a) the full name, address and occupation of the whistleblower;~~ **(2) A disclosure shall contain, as far as practicable and without invalidating an anonymous disclosure –**
(a) the name and secure contact details of the whistleblower, where the whistleblower chooses to provide them;
 (b) the nature of the impropriety in respect of which the disclosure is made;
 (c) the particulars of the person who is alleged to have committed, is committing or will commit, the impropriety;
 (d) the time and place where the alleged impropriety took place, is taking place or is likely to take place; and
 (e) the full name, address and description of the person, if any, who witnessed the commission of the impropriety.
- (3) (a) Where a whistleblower makes a disclosure orally, the person to whom the disclosure is made shall cause the disclosure to be recorded in writing.
 (b) The disclosure referred to in paragraph (a) shall contain the information required under subsection (2).
- (4) The NCA or other authority receiving a disclosure shall assign a confidential reference number, maintain a secure audit trail and, where contact details are available, acknowledge receipt without requiring the whistleblower to reveal more identifying information than is reasonably necessary.**
- (5) The identity of a whistleblower and information capable of identifying that person shall not be disclosed except with the whistleblower's consent, by order of a Court, or where disclosure is strictly necessary for the fair determination of proceedings and appropriate protective measures have been considered.**

Rationale

A disclosure regime should not fail merely because a person fears providing a residential address or identifying details. The amendment permits anonymous and electronic reports, creates a secure audit trail and makes confidentiality the default while preserving court-controlled disclosure where fairness requires it.

CLAUSE 33 — PROTECTION AGAINST VICTIMISATION

STATUS	AMEND	Broad anti-retaliation protection
--------	-------	-----------------------------------

Government text

33. Protection against victimisation

- (1) An NCA officer who makes a disclosure of impropriety shall not be subjected to victimisation by the NCA or any other NCA officer.
- (2) An NCA officer, as a whistleblower, shall be considered as having been subjected to victimisation where as a result of making the disclosure, he is dismissed, suspended, declared redundant, denied promotion, transferred to another Division or Unit against his will, harassed, intimidated, subjected to a discriminatory or other adverse measure by the NCA or another NCA officer, or otherwise threatened by another NCA officer.
- (3) An NCA officer, as a whistleblower, shall not be considered as having been subjected to victimisation if the NCA officer against whom the complaint is directed has the legal right to take the action complained of and the action taken is shown to be unrelated to the disclosure made.

Proposed amendment

- (1) An NCA officer who makes a disclosure of impropriety shall not be subjected to victimisation by the NCA or any other NCA officer.

(1A) The protection under subsection (1) applies where the NCA officer honestly and reasonably believed, at the time of the disclosure, that the information tended to show impropriety, whether or not the allegation is ultimately substantiated.

~~(2) An NCA officer, as a whistleblower, shall be considered as having been subjected to victimisation where as a result of making the disclosure, he is dismissed, suspended, declared redundant, denied promotion, transferred to another Division or Unit against his will, harassed, intimidated, subjected to a discriminatory or other adverse measure by the NCA or another NCA officer, or otherwise threatened by another NCA officer.~~ **(2) Victimisation includes any direct or indirect detrimental act or omission connected with a disclosure, including dismissal, suspension, disciplinary action, redundancy, denial of promotion or training, adverse appraisal, involuntary transfer, harassment, intimidation, discrimination, threat, interference with duties, or any other disadvantage affecting employment, professional standing or safety.**

- (3) An NCA officer, as a whistleblower, shall not be considered as having been subjected to victimisation if the NCA officer against whom the complaint is directed has the legal right to take the action complained of and the action taken is shown to be unrelated to the disclosure made.

(4) Where facts are established from which victimisation may reasonably be inferred, the NCA or person responsible for the adverse action shall bear the burden of showing, on the balance of probabilities, that the action was taken for legitimate reasons unrelated to the disclosure.

(5) Nothing in this section protects a person who knowingly makes a false disclosure or fabricates evidence; however, a disclosure shall not lose protection merely because it is mistaken or unsubstantiated.

Rationale

The protection should turn on reasonable belief and retaliation, not on whether the allegation is eventually proved. The amendment broadens the forms of prohibited retaliation and creates a practical burden-shifting rule once a credible causal link is shown, while excluding knowingly false disclosures.

CLAUSE 34 — REPORT TO INDEPENDENT ADVISORY PANEL

STATUS	AMEND	Secure complaint and urgent protection
--------	-------	--

Government text

34. Report to Independent Advisory Panel

- (1) An NCA officer, as a whistleblower, who honestly and reasonably believes that he has been, is being, or is likely to be, subjected to victimisation, may make a complaint to the Independent Advisory Panel.
- (2) A complaint made under subsection (1) shall contain the following particulars –
- (a) the name, description and address of the NCA officer as whistleblower;
 - (b) the name, description and address of the NCA officer he claims has subjected, is subjecting or might subject, him to victimisation; and
 - (c) the specific acts complained of as constituting victimisation.

Proposed amendment

- (1) An NCA officer, as a whistleblower, who honestly and reasonably believes that he has been, is being, or is likely to be, subjected to victimisation, may make a complaint to the Independent Advisory Panel.

(1A) A complaint may be made through a secure channel, directly or through a legal representative or other authorised representative, and may include a request for urgent interim protection.

~~(2) A complaint made under subsection (1) shall contain the following particulars –~~

~~(a) the name, description and address of the NCA officer as whistleblower;~~ **(2) A complaint shall contain, so far as practicable –**

(a) the name, description and secure contact details of the NCA officer, without requiring disclosure of a residential address where another reliable means of contact is available;

~~(b) the name, description and address of the NCA officer he claims has subjected, is subjecting or might subject, him to victimisation;~~ **(b) sufficient particulars to identify the person or persons alleged to have subjected, be subjecting or be likely to subject the whistleblower to victimisation;**

(c) the specific acts complained of as constituting victimisation.

(3) The Independent Advisory Panel shall protect the confidentiality of the complaint and shall restrict access to identifying information to persons for whom access is necessary for the fair and lawful conduct of the enquiry.

Rationale

The clause should facilitate rather than discourage complaints. Requiring residential addresses may expose whistleblowers unnecessarily. Secure contact details, representation and urgent interim protection provide a safer route while preserving sufficient information for a fair enquiry.

CLAUSE 35 — ENQUIRY BY INDEPENDENT ADVISORY PANEL

STATUS	AMEND	Fair, timely and reasoned determination
--------	-------	---

Government text

35. Enquiry by Independent Advisory Panel

- (1) The Independent Advisory Panel shall, on receipt of a complaint made under section 34(1), conduct an enquiry into the complaint at which the whistleblower and the person against whom the complaint is made shall be heard.
- (2) The Independent Advisory Panel may, in the course of conducting an enquiry under subsection (1), make such interim order as it considers fit.
- (3) After hearing the parties and other persons considered necessary, the Independent Advisory Panel shall make any order which is just and fair in the circumstances, including an order for reinstatement, reversal of a transfer or transfer of the whistleblower to another establishment, where applicable.

Proposed amendment

- (1) The Independent Advisory Panel shall, on receipt of a complaint made under section 34(1), conduct an enquiry into the complaint at which the whistleblower and the person against whom the complaint is made shall be heard.

(1A) The enquiry shall be conducted fairly, impartially and, so far as consistent with procedural fairness, confidentially. Each party shall be given reasonable notice of the substance of the case and an opportunity to respond and may be represented by a law practitioner.

- (2) The Independent Advisory Panel may, in the course of conducting an enquiry under subsection (1), make such interim order as it considers fit.

(2A) Where urgent protection is reasonably necessary to prevent continuing or imminent victimisation, the Panel may make an interim order before the conclusion of the enquiry after giving such opportunity to be heard as is practicable in the circumstances.

- (3) After hearing the parties and other persons considered necessary, the Independent Advisory Panel shall make any order which is just and fair in the circumstances, including an order for reinstatement, reversal of a transfer or transfer of the whistleblower to another establishment, where applicable.

(4) The Panel shall give written reasons for its determination and shall endeavour to conclude an enquiry within 90 days of receipt of the complaint; where that period is exceeded, the Panel shall record the reasons for the delay and inform the parties.

(5) A determination under this section is subject to the supervisory jurisdiction of the Supreme Court and shall not exclude any other remedy available by law.

Rationale

The Bill gives the Panel broad remedial power but says little about procedure. The amendment adds natural-justice safeguards, urgency powers, written reasons, a target timeframe and express preservation of judicial supervision.

CLAUSE 36 — OTHER MEASURES TO PROTECT NCA OFFICER AS WHISTLEBLOWER

STATUS	AMEND	Independent whistleblower protocol
--------	-------	------------------------------------

Government text

36. Other measures to protect NCA officer as whistleblower
 The Governance Advisory Board shall take such other measures as may be necessary to protect NCA officers as whistleblowers under this Act, and such measures shall be communicated to NCA officers.

Proposed amendment

~~The Governance Advisory Board shall take such other measures as may be necessary to protect NCA officers as whistleblowers under this Act, and such measures shall be communicated to NCA officers.~~

(1) The Governance Advisory Board shall, after consultation with the Independent Advisory Panel, adopt and publish an internal whistleblower protection protocol providing for confidential and anonymous reporting channels, protection against retaliation, secure record-keeping, conflict-of-interest arrangements and regular staff training.

(2) The protocol shall provide an external reporting route to the Independent Advisory Panel where the disclosure concerns senior leadership, the Internal Affairs Division or any person responsible for administering the internal reporting channel.

(3) The NCA shall publish annually anonymised statistics on disclosures received, categories of alleged impropriety, protective measures taken and outcomes, without revealing operationally sensitive information or the identity of any whistleblower or person under investigation.

Rationale

Whistleblower protection should not depend solely on discretionary internal measures. A published protocol, an independent route for conflicts of interest and anonymised reporting improve credibility without exposing sensitive investigations.

CLAUSE 37 — DETERMINATION OF COMPLEX, SERIOUS AND ORGANISED CRIME

STATUS	REWRITE	Objective scope and recorded jurisdiction
--------	---------	---

Government text

37. Determination of complex, serious and organised crime

A crime may be considered to be complex, serious and organised by the Director-General where –

- (a) the crime is connected, or is ancillary, to a financial crime;
- (b) the crime is connected, or is ancillary, to any investigation that has been, or is being conducted, by the NCA;
- (c) investigation into the crime requires significant international cooperation;
- (d) the crime involves a politically exposed person, whether as a victim or suspect;
- (e) the crime is one in which the suspect may be engaged in cybercrime or computer-based crime;
- (f) the crime is suspected to have been committed by, or is connected to, an organised group;
- (g) the crime is connected, or ancillary, to money-laundering, financing of terrorism or proliferation financing;
- (h) given the nature, scope, gravity, complexity or seriousness of the crime, or significant harm caused, it would be in the interests of the efficient conduct of investigation into the crime, or in the public interest, that the NCA investigates into the crime.

Proposed amendment

~~37. Determination of complex, serious and organised crime~~

~~A crime may be considered to be complex, serious and organised by the Director-General where –~~

- ~~(a) the crime is connected, or is ancillary, to a financial crime;~~
- ~~(b) the crime is connected, or is ancillary, to any investigation that has been, or is being conducted, by the NCA;~~
- ~~(c) investigation into the crime requires significant international cooperation;~~
- ~~(d) the crime involves a politically exposed person, whether as a victim or suspect;~~
- ~~(e) the crime is one in which the suspect may be engaged in cybercrime or computer-based crime;~~
- ~~(f) the crime is suspected to have been committed by, or is connected to, an organised group;~~
- ~~(g) the crime is connected, or ancillary, to money-laundering, financing of terrorism or proliferation financing;~~
- ~~(h) given the nature, scope, gravity, complexity or seriousness of the crime, or significant harm caused, it would be in the interests of the efficient conduct of investigation into the crime, or in the public interest, that the NCA investigates into the crime.~~

37. Determination of complex, serious and organised crime

(1) The Director-General may determine that a crime is a complex, serious and organised crime for the purposes of this Act only where he is satisfied on reasonable grounds that –

- (a) the conduct falls within, is connected with, or is ancillary to financial crime, cybercrime, money-laundering, financing of terrorism, proliferation financing or organised criminal activity; and
- (b) having regard to its scale, gravity, complexity, sophistication, cross-border character, organised structure, significant harm or the specialist capability required for its investigation, investigation by the NCA is reasonably necessary.

(2) In making a determination under subsection (1), the Director-General may take into account –

- (a) the need for significant international cooperation;
- (b) the use of sophisticated digital, financial or corporate structures;
- (c) a substantial risk of dissipation, concealment or cross-border movement of proceeds or evidence;
- (d) the involvement of an organised group; and
- (e) any other objectively relevant factor relating to complexity, seriousness or organised criminality.

(3) The fact that a person is a politically exposed person, whether as a victim, witness or suspect, shall not of itself be sufficient to bring a matter within the jurisdiction of the NCA.

- (4) The fact that a matter is connected or ancillary to an existing NCA investigation, or that investigation by the NCA is considered to be in the public interest, shall not of itself be sufficient unless the requirements of subsection (1) are satisfied.**
- (5) A determination under this section shall be recorded in writing with sufficient reasons to demonstrate the statutory basis for NCA jurisdiction, subject to such lawful redactions as may be necessary to protect an ongoing investigation, intelligence source or third party.**
- (6) Nothing in this section excludes the jurisdiction of a Court to determine whether a power under this Act was exercised within the lawful jurisdiction of the NCA.**

Rationale

The circulated clause permits NCA jurisdiction to expand on broad grounds, including PEP status, connection to any NCA investigation and a general public-interest assessment. The rewrite requires an objective seriousness/complexity threshold, written reasons and court supervision, and makes clear that political exposure alone cannot trigger NCA jurisdiction.

CLAUSE 38 — INVESTIGATION BY NCA OR OTHER INVESTIGATIVE BODY

STATUS	REWRITE	Coordinated jurisdiction; no blanket Police powers
--------	---------	--

Government text

38. Investigation by NCA or other investigative body

- (1) Subject to this section, the NCA shall investigate into financial crime, cybercrime and other complex, serious and organised crime.
- (2) Notwithstanding subsection (1), where the NCA considers, in the interests of the efficient conduct of an investigation into a financial crime, a cybercrime or other complex, serious and organised crime, or in the public interest that –
- (a) the Police or another investigative body should investigate into that crime, the NCA shall refer the matter to the Police or that investigative body for investigation;
 - (b) there should be a joint investigation by the NCA and the Police or another investigative body, the NCA shall conduct the investigation jointly with the Police or that investigative body; or
 - (c) there should be a joint investigation by the NCA, the Police and another investigative body, the NCA shall conduct the investigation jointly with the Police and that investigative body.
- (3) Where the Police or another investigative body is investigating into a financial crime, a cybercrime or other complex, serious and organised crime, the NCA may –
- (a) take over the investigation from the Police or investigative body; or
 - (b) conduct a joint investigation with the Police or that investigative body.
- (4) Where, in the course of an investigation conducted by the Police or another investigative body, a financial crime, a cybercrime or other complex, serious and organised crime is suspected, the Commissioner of Police or the Head of that investigative body shall, in accordance with the Operational Protocol, make an interim report to the NCA as expeditiously as possible.
- (5) On receipt of an interim report under subsection (4), the NCA shall proceed in accordance with subsection (2) or (3).
- (6) Where there is a joint investigation, the Director-General, the Commissioner of Police and the Head of that investigative body, as the case may be, shall make suitable arrangements for the efficient conduct of the joint investigation.
- (7) Where the NCA investigates into a financial crime, a cybercrime or other complex, serious and organised crime, the NCA, the Director-General and any investigative officer may, with such modifications and adaptations as may be necessary, exercise such powers as are conferred to the Police, the Commissioner of Police and any police officer under any other relevant enactment.

Proposed amendment

38. Investigation by NCA or other investigative body

- ~~(1) Subject to this section, the NCA shall investigate into financial crime, cybercrime and other complex, serious and organised crime.~~
- ~~(2) Notwithstanding subsection (1), where the NCA considers, in the interests of the efficient conduct of an investigation into a financial crime, a cybercrime or other complex, serious and organised crime, or in the public interest that –~~
- ~~(a) the Police or another investigative body should investigate into that crime, the NCA shall refer the matter to the Police or that investigative body for investigation;~~
 - ~~(b) there should be a joint investigation by the NCA and the Police or another investigative body, the NCA shall conduct the investigation jointly with the Police or that investigative body; or~~
 - ~~(c) there should be a joint investigation by the NCA, the Police and another investigative body, the NCA shall conduct the investigation jointly with the Police and that investigative body.~~
- ~~(3) Where the Police or another investigative body is investigating into a financial crime, a cybercrime or other complex, serious and organised crime, the NCA may –~~
- ~~(a) take over the investigation from the Police or investigative body; or~~
 - ~~(b) conduct a joint investigation with the Police or that investigative body.~~
- ~~(4) Where, in the course of an investigation conducted by the Police or another investigative body, a financial crime, a~~

~~cybercrime or other complex, serious and organised crime is suspected, the Commissioner of Police or the Head of that investigative body shall, in accordance with the Operational Protocol, make an interim report to the NCA as expeditiously as possible.~~

~~(5) On receipt of an interim report under subsection (4), the NCA shall proceed in accordance with subsection (2) or (3).~~

~~(6) Where there is a joint investigation, the Director-General, the Commissioner of Police and the Head of that investigative body, as the case may be, shall make suitable arrangements for the efficient conduct of the joint investigation.~~

~~(7) Where the NCA investigates into a financial crime, a cybercrime or other complex, serious and organised crime, the NCA, the Director-General and any investigative officer may, with such modifications and adaptations as may be necessary, exercise such powers as are conferred to the Police, the Commissioner of Police and any police officer under any other relevant enactment.~~

38. Investigation by NCA or other investigative body

(1) Subject to this Act, the NCA shall investigate financial crime, cybercrime and other complex, serious and organised crime falling within its lawful jurisdiction.

(2) Where the NCA considers that an investigation should be conducted by the Police or another investigative body, or jointly with such body, the Director-General shall record the decision and reasons and proceed in accordance with the Operational Protocol, after consultation with the Commissioner of Police or the head of the other investigative body concerned.

(3) The NCA shall not take over an investigation being lawfully conducted by the Police or another investigative body unless –

(a) the Commissioner of Police or the head of that body agrees in writing; or

(b) the matter is otherwise transferred in accordance with an express provision of an enactment.

Where agreement is not reached, the agencies may conduct coordinated or parallel investigations within their respective lawful jurisdictions in accordance with the Operational Protocol.

(4) Where, during an investigation, the Police or another investigative body reasonably suspects that conduct falls within the jurisdiction of the NCA, it shall notify the NCA as expeditiously as practicable, without being required to disclose material where disclosure would be unlawful or would materially prejudice an urgent operational step.

(5) Where an investigation is transferred or conducted jointly, the participating bodies shall make written arrangements for leadership, decision-making, evidence custody, disclosure obligations, information security, arrest and search responsibilities, and preservation of the continuity and integrity of evidence.

(6) Nothing in this section authorises the NCA or the Director-General to direct the Commissioner of Police or the head of another investigative body in the exercise of powers conferred independently by the Constitution or another enactment.

(7) An NCA investigative officer may exercise only a coercive, search, seizure, arrest, detention, interception or other investigative power expressly conferred on that officer by this Act or by another enactment which expressly applies that power to the NCA or an NCA investigative officer.

Rationale

The original subsection (7) would import, with unspecified 'modifications and adaptations', the powers of the Police, Commissioner of Police and police officers under any relevant enactment. The rewrite requires coercive powers to be expressly conferred by law and prevents unilateral displacement of constitutionally or statutorily independent investigative bodies while preserving joint and parallel investigations.

CLAUSE 39 — INVESTIGATION NOT VOID OR IMPEACHABLE

STATUS	REWRITE	Incidental offences and judicial supervision
--------	---------	--

Government text

39. Investigation not void or impeachable

- (1) Where, during the course of an investigation, any other crime, other than a financial crime, a cybercrime or other complex, serious and organised crime is detected, the NCA investigative officer shall also investigate into that other crime.
- (2) Notwithstanding any other enactment, no investigation shall be void or impeachable by reason that a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime, that is detected pursuant to subsection (1) should have been investigated by the NCA, the Police or another investigative body.

Proposed amendment

~~39. Investigation not void or impeachable~~

- ~~(1) Where, during the course of an investigation, any other crime, other than a financial crime, a cybercrime or other complex, serious and organised crime is detected, the NCA investigative officer shall also investigate into that other crime.~~
- ~~(2) Notwithstanding any other enactment, no investigation shall be void or impeachable by reason that a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime, that is detected pursuant to subsection (1) should have been investigated by the NCA, the Police or another investigative body.~~

39. Incidental offences and effect of allocation errors

- (1) Where, during an NCA investigation, an offence outside the ordinary jurisdiction of the NCA is detected, the NCA may investigate that offence only to the extent that it is inseparable from, or reasonably necessary to advance or preserve evidence in, the principal investigation; otherwise the matter shall be referred promptly to the Police or other competent investigative body.**
- (2) A defect in the administrative allocation of an investigation between the NCA, the Police or another investigative body shall not, by itself, invalidate an investigation or evidence lawfully obtained where no substantial prejudice has resulted.**
- (3) Subsection (2) shall not validate an act done without lawful authority, cure a breach of a constitutional right, exclude judicial review, prevent a Court from excluding unlawfully obtained evidence, or restrict any remedy otherwise available by law.**

Rationale

The circulated 'not void or impeachable' language is very broad and could be read as insulating unlawful exercises of power. The rewrite protects investigations from purely administrative allocation errors while expressly preserving constitutional remedies, judicial review and the Court's control over unlawfully obtained evidence.

CLAUSE 40 — NCA INVESTIGATIVE OFFICER

STATUS	AMEND	Designation, identification and accountable force
--------	-------	---

Government text

40. NCA investigative officer

(1) A warrant card shall be issued to every NCA investigative officer and shall be evidence of his authorisation as an investigative officer.

(2) Where this Act confers a power to an NCA investigative officer, the officer may, where necessary, use reasonable force, provided that such power is exercised justifiably, reasonably and proportionately.

Proposed amendment

(1) A warrant card shall be issued to every NCA investigative officer and shall be evidence of his authorisation as an investigative officer.

(1A) No officer shall exercise a coercive power under this Act unless designated in writing for that class of power and trained in the lawful, proportionate and rights-respecting exercise of that power.

(1B) Before exercising a coercive power, an NCA investigative officer shall, unless impracticable because of an immediate operational risk, identify himself by warrant card and state the statutory authority and general purpose for which the power is exercised.

~~(2) Where this Act confers a power to an NCA investigative officer, the officer may, where necessary, use reasonable force, provided that such power is exercised justifiably, reasonably and proportionately.~~ **(2) Where this Act expressly authorises the use of force, an NCA investigative officer may use no more force than is strictly necessary and proportionate to achieve a lawful purpose, having regard to the circumstances and the rights and safety of all persons affected.**

(3) Any use of force shall be recorded as soon as practicable, including the reason for its use, the nature and degree of force used, any injury reported or observed and any medical assistance provided or offered.

(4) Force shall not be used for the sole purpose of compelling a person to make a statement, answer a question or surrender material which that person is lawfully entitled to withhold.

Rationale

The clause should distinguish possession of a warrant card from authority to exercise particular coercive powers. Written designation, training, identification and a record of force create accountability and align the exercise of coercive authority with constitutional liberty and due-process safeguards.

CLAUSE 41 — QUESTIONING AND PRODUCTION OF EVIDENCE

STATUS	REWRITE	Notice, counsel, privilege and proportionate enforcement
--------	---------	--

Government text

41. Questioning and production of evidence

(1) For the purpose of an investigation, an NCA investigative officer may, by written notice, order any person concerned with the investigation to –

(a) attend before him for the purpose of being examined orally or to give a written statement under oath or solemn affirmation; or

(b) give any material evidence which may assist him in the investigation.

(2) A person on whom a notice is served under subsection (1) shall attend before the NCA and, subject to section 42, answer any question, give any written statement or give any material evidence which may be required for the investigation.

(3) Where an NCA investigative officer has reasonable grounds to suspect that any material evidence may be relevant to the investigation, he may –

(a) where the material evidence is not reasonably required for the purpose of performing any duty under any enactment, retain the material evidence until its production in Court or until such earlier time as may be required; or

(b) make certified copies of, or take records from, the material evidence.

(4) The NCA investigative officer may require the attendance of a person served with a notice under subsection (1) on such other days as he may direct until the examination is completed.

(5) Any person who, after having been served with a notice under subsection (1) –

(a) fails, subject to section 42 or without reasonable excuse, to comply with any term of the notice; or

(b) conceals, destroys, alters, tampers with, removes from the place where it is habitually kept, or otherwise disposes of, any material evidence referred to in the notice or in relation to the investigation,

shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Proposed amendment

41. Questioning and production of evidence

~~(1) For the purpose of an investigation, an NCA investigative officer may, by written notice, order any person concerned with the investigation to –~~

~~(a) attend before him for the purpose of being examined orally or to give a written statement under oath or solemn affirmation; or~~

~~(b) give any material evidence which may assist him in the investigation.~~

~~(2) A person on whom a notice is served under subsection (1) shall attend before the NCA and, subject to section 42, answer any question, give any written statement or give any material evidence which may be required for the investigation.~~

~~(3) Where an NCA investigative officer has reasonable grounds to suspect that any material evidence may be relevant to the investigation, he may –~~

~~(a) where the material evidence is not reasonably required for the purpose of performing any duty under any enactment, retain the material evidence until its production in Court or until such earlier time as may be required; or~~

~~(b) make certified copies of, or take records from, the material evidence.~~

~~(4) The NCA investigative officer may require the attendance of a person served with a notice under subsection (1) on such other days as he may direct until the examination is completed.~~

~~(5) Any person who, after having been served with a notice under subsection (1) –~~

~~(a) fails, subject to section 42 or without reasonable excuse, to comply with any term of the notice; or~~

~~(b) conceals, destroys, alters, tampers with, removes from the place where it is habitually kept, or otherwise disposes of, any material evidence referred to in the notice or in relation to the investigation,~~

~~shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.~~

41. Questioning and production of evidence

(1) For the purpose of an investigation within the lawful jurisdiction of the NCA, an NCA investigative officer may by written notice require a person reasonably believed to possess relevant information or material –

- (a) to attend for examination or provide a written statement; or
- (b) to produce specified material evidence relevant to the investigation.

(2) A notice under subsection (1) shall state –

- (a) the statutory authority under which it is issued and sufficient particulars of the investigation to enable the recipient to understand the requirement without prejudicing the investigation;
- (b) the information or material required with reasonable specificity;
- (c) the date, time and place for compliance, allowing a reasonable period except where urgency is justified and recorded;
- (d) the right to consult and be accompanied by a law practitioner;
- (e) the rights preserved by section 42 and legal professional privilege; and
- (f) the consequences of non-compliance.

(3) A person served with a notice shall comply, subject to section 42, legal professional privilege and any other lawful privilege or immunity, and may apply to a Judge in Chambers to vary or set aside a notice that is unlawful, unduly burdensome, disproportionate or insufficiently specific.

(4) Material produced may be retained only for so long as is reasonably necessary for the investigation, prosecution or related proceedings. The NCA shall provide a receipt, preserve integrity and chain of custody, permit reasonable access to copies where lawful, and return original material when continued retention is no longer necessary or authorised by a Court.

(5) Further attendance may be required only by a further written notice or by agreement, and questioning shall be conducted at reasonable times and for reasonable periods with appropriate breaks.

(6) A person who wilfully and without reasonable excuse fails to comply with a lawful notice, after having been given a reasonable opportunity to comply, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 500,000 rupees and to imprisonment for a term not exceeding 2 years.

(7) A person who, knowing that material is relevant to an investigation or is required by a lawful notice, intentionally conceals, destroys, alters, tampers with, removes or disposes of that material for the purpose of obstructing the investigation shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Rationale

The circulated clause combines compulsory attendance, sworn statements, document production, indefinite retention and serious criminal penalties with limited procedural detail. The rewrite gives the notice recipient clear information, access to counsel, privilege and judicial review, limits retention and distinguishes ordinary non-compliance from deliberate evidence destruction.

CLAUSE 42 — REFUSING TO GIVE EVIDENCE

STATUS	REWRITE	Self-incrimination, privilege and DPP-controlled immunity
--------	---------	---

Government text

42. Refusing to give evidence

- (1) A person may refuse to answer any question put to him, refuse to give any written statement or refuse to give any material evidence where the answer to the question, or the giving of the written statement or material evidence, may incriminate him.
- (2) Subsection (1) shall not apply where the Director-General, with the consent of the Director of Public Prosecutions, gives an undertaking in writing to a person that any answer given or any written statement or material evidence given will not be used as evidence in any criminal proceedings against him for an offence, except in proceedings for perjury.
- (3) Where an undertaking is given under subsection (2), no Court shall admit the answer, written statement or material evidence referred to in the undertaking in any criminal proceedings against the person to whom the undertaking was given, except in proceedings for perjury.

Proposed amendment

~~42. Refusing to give evidence~~

- ~~(1) A person may refuse to answer any question put to him, refuse to give any written statement or refuse to give any material evidence where the answer to the question, or the giving of the written statement or material evidence, may incriminate him.~~
- ~~(2) Subsection (1) shall not apply where the Director-General, with the consent of the Director of Public Prosecutions, gives an undertaking in writing to a person that any answer given or any written statement or material evidence given will not be used as evidence in any criminal proceedings against him for an offence, except in proceedings for perjury.~~
- ~~(3) Where an undertaking is given under subsection (2), no Court shall admit the answer, written statement or material evidence referred to in the undertaking in any criminal proceedings against the person to whom the undertaking was given, except in proceedings for perjury.~~

42. Privilege against self-incrimination and protected material

- (1) A person may refuse to answer a question, make a statement or produce material where doing so would tend to incriminate that person, and may refuse to disclose material protected by legal professional privilege or any other privilege recognised by law.
- (2) No adverse inference shall be drawn solely from the lawful exercise of a right under subsection (1).
- (3) The Director of Public Prosecutions may, on a written request setting out the reasons, give a written undertaking that a person will not have compelled answers, statements or material, or evidence derived directly or indirectly from them, used against that person in criminal proceedings, except proceedings for perjury, knowingly giving false evidence or an offence consisting of failure to comply with the terms of the undertaking.
- (4) A person shall not be compelled to provide self-incriminating information pursuant to an undertaking unless the person has been informed in writing of the scope and effect of the undertaking and has had a reasonable opportunity to obtain legal advice.
- (5) Where an undertaking is given under subsection (3), no Court shall admit against that person evidence prohibited by the terms of the undertaking, subject to the exceptions expressly stated in the undertaking and this section.

Rationale

The original mechanism gives the Director-General, with DPP consent, the role of issuing the undertaking and protects only the compelled answer or material itself. The rewrite places immunity under the control of the DPP and adds derivative-use protection, legal advice and express protection of legal professional privilege.

CLAUSE 43 — WARRANT FOR ENTRY, SEARCH AND SEIZURE

STATUS	REWRITE	Judicial warrant and digital-search safeguards
--------	---------	--

Government text

43. Warrant for entry, search and seizure

- (1) Subject to subsection (2), where an NCA investigative officer has reasonable grounds to suspect that there is, on any premises, other than on specified premises referred to in section 44, material evidence which may assist him in an investigation, the Director-General may issue a warrant authorising the officer to enter and search the premises, and to seize any material evidence.
- (2) Where an NCA investigative officer has reasonable grounds to suspect that –
- (a) stored data in a computer system is relevant for the purpose of an investigation or the prosecution of financial crime, a cybercrime or other complex, serious and organised crime, he may make an application to the Judge in Chambers for the issue of a warrant to access such data; or
 - (b) data sought is stored in another computer system or part of it in Mauritian territory, and such data is lawfully accessible from or available to the initial system, he shall expeditiously extend the search or similar access to the other system.
- (3) A warrant issued under subsection (1) or (2) shall be a search only to the extent for which the warrant was issued.
- (4) As far as practicable –
- (a) an NCA investigative officer shall, prior to a search, provide a photocopy of the warrant to the owner or occupier of the premises, or his duly authorised agent against receipt acknowledged by a signature on the original of the warrant; and
 - (b) a search shall be carried out in the presence of the owner or occupier of the premises, or his duly authorised agent.
- (5) Where a search is effected under subsection (1), the investigative officer effecting the search may search any person who is on the premises, detain him for the purpose of the search and, where he has reasonable grounds to suspect that there is material evidence in relation to a crime which he is investigating into or any other crime –
- (a) seize the material evidence; and
 - (b) in relation to data –
 - (i) seize or secure a computer system or part of it or a computer data storage medium;
 - (ii) make and retain a copy of those computer data;
 - (iii) maintain the integrity of the relevant stored computer data; or
 - (iv) render inaccessible or remove those computer data from the accessed computer system.
- (6) The investigative officer may order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in subsection (5)(b).

Proposed amendment

~~43. Warrant for entry, search and seizure~~

- ~~(1) Subject to subsection (2), where an NCA investigative officer has reasonable grounds to suspect that there is, on any premises, other than on specified premises referred to in section 44, material evidence which may assist him in an investigation, the Director-General may issue a warrant authorising the officer to enter and search the premises, and to seize any material evidence.~~
- ~~(2) Where an NCA investigative officer has reasonable grounds to suspect that –~~
- ~~(a) stored data in a computer system is relevant for the purpose of an investigation or the prosecution of financial crime, a cybercrime or other complex, serious and organised crime, he may make an application to the Judge in Chambers for the issue of a warrant to access such data; or~~
 - ~~(b) data sought is stored in another computer system or part of it in Mauritian territory, and such data is lawfully accessible from or available to the initial system, he shall expeditiously extend the search or similar access to the other system.~~
- ~~(3) A warrant issued under subsection (1) or (2) shall be a search only to the extent for which the warrant was issued.~~
- ~~(4) As far as practicable –~~
- ~~(a) an NCA investigative officer shall, prior to a search, provide a photocopy of the warrant to the owner or occupier of the premises, or his duly authorised agent against receipt acknowledged by a signature on the original of the warrant;~~

and

~~(b) a search shall be carried out in the presence of the owner or occupier of the premises, or his duly authorised agent.
 (5) Where a search is effected under subsection (1), the investigative officer effecting the search may search any person who is on the premises, detain him for the purpose of the search and, where he has reasonable grounds to suspect that there is material evidence in relation to a crime which he is investigating into or any other crime—
 (a) seize the material evidence; and
 (b) in relation to data—
 (i) seize or secure a computer system or part of it or a computer data storage medium;
 (ii) make and retain a copy of those computer data;
 (iii) maintain the integrity of the relevant stored computer data; or
 (iv) render inaccessible or remove those computer data from the accessed computer system.
 (6) The investigative officer may order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in subsection (5)(b).~~

43. Warrant for entry, search and seizure

(1) An NCA investigative officer may enter and search private premises, search a person on those premises, access or search a computer system, or seize material evidence only under a warrant issued by a Judge in Chambers, except to the extent that another enactment expressly authorises the particular act in the circumstances.

(2) An application for a warrant shall be made by an NCA investigative officer with the written approval of the Director-General or Deputy Director-General and shall be supported by an affidavit setting out the facts relied upon, the offence under investigation, the premises, person, system or data to be searched, the material sought and the reasons why the measure is necessary and proportionate.

(3) The Judge in Chambers may issue a warrant only where satisfied on reasonable grounds that –

- (a) an offence within the lawful jurisdiction of the NCA has been or is reasonably suspected to have been committed;
- (b) relevant material evidence is likely to be found at the place, on the person, or in the system specified;
- (c) the scope of the search is sufficiently particularised; and
- (d) the search and any proposed seizure are necessary and proportionate in all the circumstances.

(4) A warrant shall specify, so far as practicable, the premises, person, computer system or account to which it relates, the categories of material sought, the powers authorised, the period within which it may be executed and any conditions imposed by the Judge.

(5) Where, during an authorised search of a computer system, an officer has reasonable grounds to believe that specified data within the scope of the warrant is stored in another system in Mauritius and is lawfully accessible from the system being searched, access to the other system may occur only where the warrant expressly authorises such extension or the Judge grants a further or varied authorisation.

(6) Before a search, a copy of the warrant shall, as far as practicable and subject to any judicially authorised delay, be provided to the owner or occupier or authorised agent, and the search shall, where practicable, be conducted in that person's presence.

(7) A person on the premises may be searched only where there are reasonable grounds to believe that the person has on his person material falling within the warrant, and the search shall be conducted with due respect for dignity and privacy.

(8) In relation to digital material, an officer may seize, secure, copy or render inaccessible only material reasonably within the scope of the warrant and shall use appropriate forensic measures to preserve integrity, minimise access to unrelated personal data and maintain an auditable chain of custody.

(9) Where material reasonably appears to be subject to legal professional privilege, it shall, so far as practicable, be segregated and sealed and shall not be examined by the investigative team unless a Judge determines that the material is not privileged or otherwise lawfully permits examination subject to safeguards.

(10) The NCA shall provide an inventory or receipt for property or data seized and shall make a return to the Judge, within such period as the Judge directs, identifying the warrant executed and the material seized.

(11) A person required to provide reasonable technical assistance in executing a warrant shall not be compelled to disclose information protected by section 42 or legal professional privilege.

Rationale

The circulated Bill allows the Director-General himself to issue a warrant for entry, search and seizure of ordinary premises, while judicial authorisation is required for access to stored computer data. The rewrite applies independent judicial authorisation to private searches generally and adds specificity, proportionality, linked-system limits, digital minimisation, privileged-material handling and a post-execution inventory.

CLAUSE 44 — JUDGE’S ORDER FOR ENTRY AND SEARCH IN FINANCIAL INSTITUTION

STATUS	AMEND	Specific, proportionate financial-institution search
--------	-------	--

Government text

44. Judge’s Order for entry and search in financial institution

(1) Where an NCA investigative officer has reasonable grounds to suspect that –

(a) a bank, financial institution or cash dealer has failed to keep a business transaction record as required under section 17 of the Financial Intelligence and Anti-Money Laundering Act;

(b) a bank, financial institution, cash dealer or member of a relevant profession or occupation has failed to report a suspicious transaction as required under section 14 of the Financial Intelligence and Anti-Money Laundering Act; or

(c) a bank, financial institution, cash dealer or member of a relevant profession or occupation is in possession of any material evidence which may assist the NCA in an investigation,

he may apply to the Judge in Chambers for an Order authorising him to enter any premises belonging to, or in the possession or control of, the bank, financial institution, cash dealer or member of the relevant profession or occupation and to search the premises and any electronic device found thereat and remove therefrom any material evidence.

(2) An application under subsection (1) shall be supported by an affidavit by the NCA investigative officer disclosing the reason why an Order is sought under this section.

Proposed amendment

(1) Where an NCA investigative officer has reasonable grounds to suspect that –

(a) a bank, financial institution or cash dealer has failed to keep a business transaction record as required under section 17 of the Financial Intelligence and Anti-Money Laundering Act;

(b) a bank, financial institution, cash dealer or member of a relevant profession or occupation has failed to report a suspicious transaction as required under section 14 of the Financial Intelligence and Anti-Money Laundering Act; or

(c) a bank, financial institution, cash dealer or member of a relevant profession or occupation is in possession of any material evidence which may assist the NCA in an investigation,

~~he may apply to the Judge in Chambers for an Order authorising him to enter any premises belonging to, or in the possession or control of, the bank, financial institution, cash dealer or member of the relevant profession or occupation and to search the premises and any electronic device found thereat and remove therefrom any material evidence.~~ **he may apply to the Judge in Chambers for an Order authorising entry, search and seizure to the extent specified in the Order.**

(1A) The Judge shall not issue an Order unless satisfied that the statutory ground relied upon is supported by reasonable grounds, that relevant material is likely to be found, and that the proposed search is necessary, proportionate and sufficiently specific as to premises, electronic devices, accounts, records or categories of material.

(2) An application under subsection (1) shall be supported by an affidavit by the NCA investigative officer disclosing the reason why an Order is sought under this section.

(3) An Order may include conditions governing the time and manner of execution, forensic copying, protection of unrelated personal data, handling of material claimed to be legally privileged, and the making of an inventory or return to the Judge after execution.

(4) The safeguards in section 43 relating to identification, scope, digital integrity, privileged material and receipts shall apply, with such modifications as are necessary, to a search under this section.

Rationale

Judicial authorisation is already built into clause 44, but the scope is broad enough to permit a search of any electronic device found at the premises. The amendment retains the judicial model while requiring particularity, necessity, proportionality and a privilege/data-handling protocol.

CLAUSE 45 — SEIZURE OF PROPERTY

STATUS	REWRITE	Judicial confirmation and return rights
--------	---------	---

Government text

45. Seizure of property

(1) Where, in the course of an investigation, an NCA investigative officer is satisfied that a property is the subject matter of, or relates to, a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime, he may seize that property.

(2) The NCA shall keep a record of any property seized under subsection (1) and shall cause a copy of that record to be served on the person from whom the property was seized.

(3) A seizure under subsection (1) shall be effected by placing the property seized under the custody of such person and at such place as the Director-General may determine.

(4) Notwithstanding subsection (3), where the Director-General considers that it is not practicable to remove the property, he may leave it at the premises on which it is found under the custody of such person as he may direct for that purpose.

(5) Where the property seized under subsection (1) is under the custody of a third party, the Director-General may direct the third party not to dispose of, or otherwise deal with, the property without his consent in writing.

(6) In this section –

“property” includes any property which is reasonably believed by the NCA to be proceeds, an instrumentality or a terrorist property.

Proposed amendment

~~45. Seizure of property~~

~~(1) Where, in the course of an investigation, an NCA investigative officer is satisfied that a property is the subject matter of, or relates to, a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime, he may seize that property.~~

~~(2) The NCA shall keep a record of any property seized under subsection (1) and shall cause a copy of that record to be served on the person from whom the property was seized.~~

~~(3) A seizure under subsection (1) shall be effected by placing the property seized under the custody of such person and at such place as the Director-General may determine.~~

~~(4) Notwithstanding subsection (3), where the Director-General considers that it is not practicable to remove the property, he may leave it at the premises on which it is found under the custody of such person as he may direct for that purpose.~~

~~(5) Where the property seized under subsection (1) is under the custody of a third party, the Director-General may direct the third party not to dispose of, or otherwise deal with, the property without his consent in writing.~~

~~(6) In this section –~~

~~“property” includes any property which is reasonably believed by the NCA to be proceeds, an instrumentality or a terrorist property.~~

45. Seizure and preservation of property

(1) An NCA investigative officer may seize property where –

(a) seizure is authorised by a warrant or Order of a Court; or

(b) while lawfully present at a place, the officer has reasonable grounds to believe that the property is evidence of an offence or constitutes proceeds, an instrumentality or terrorist property and immediate seizure is necessary to prevent concealment, destruction, dissipation or removal.

(2) Where property is seized under subsection (1)(b) without prior judicial authorisation, the NCA shall, within 72 hours or as soon as reasonably practicable thereafter where exceptional circumstances are recorded, apply to a Judge in Chambers for confirmation of continued seizure. Unless confirmed, the property shall be returned, subject to any other lawful basis for detention.

- (3) The NCA shall make a contemporaneous record of property seized and provide a receipt identifying the property, the legal basis for seizure, the date and place of seizure and a contact point for applications concerning return or access.**
- (4) Property shall be stored securely and in a manner that preserves its condition, evidential integrity and chain of custody. The Director-General shall not direct the custody of property in a manner inconsistent with a Court order or statutory asset-management regime.**
- (5) A person claiming an ownership, possessory or other lawful interest in seized property may apply to a Judge in Chambers for return, access, variation of restrictions or other appropriate relief, and the NCA shall bear the burden of establishing the continuing legal basis and necessity for retention.**
- (6) Any direction to a third party not to dispose of or deal with property shall lapse after 7 days unless confirmed or replaced by an Order of a Court or by an Order made under the Asset Recovery and Unexplained Wealth Act 2026 or another applicable enactment.**
- (7) The necessity for continued retention of seized property shall be reviewed at reasonable intervals and property shall be returned when no longer required for investigation, prosecution, forfeiture or another lawful purpose.**
- (8) In this section, ‘property’ includes property reasonably believed to be proceeds, an instrumentality or terrorist property.**

Rationale

The circulated clause allows seizure and continuing restrictions on property on the view of an investigative officer or Director-General without an express judicial confirmation period or return mechanism. The rewrite distinguishes court-authorized and urgent seizures, requires prompt confirmation of urgent seizures and gives owners and third parties a clear route to challenge continued retention.

CLAUSE 46 — DISCLOSURE OF ACCOUNT AND CUSTOMER INFORMATION

STATUS	REWRITE	Narrow judicial order, privilege and preservation limits
--------	---------	--

Government text

46. Disclosure of account and customer information

(1) (a) Where an NCA investigative officer has reasonable grounds to suspect that –

(i) any property in the possession, or under the control, of a person is proceeds, an instrumentality or a terrorist property;
(ii) the customer information or account information of any person is likely to be of substantial value to any investigation being carried out; or

(iii) it is in the public interest that the customer information or account information be provided,
he may, by an ex parte application, apply to the Judge in Chambers for an Order to direct a financial institution or member of relevant profession or occupation to provide such customer information or account information, including any details pertaining to financial transactions, as it may have relating to the person specified in the application.

(b) The Judge in Chambers shall issue an Order under paragraph (a) where he is satisfied that the requested customer or account information is material to any investigation into a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime.

(c) Where any customer information or account information is contained in an electronic device, the Judge in Chambers may direct the financial institution or member of a relevant profession or occupation to provide it in a form in which it is accessible or may be retrieved.

(d) Where the Judge in Chambers issues an Order under this subsection, the financial institution or member of a relevant profession or occupation shall, within 21 days of the Order, provide the customer information or account information to the NCA.

(e) Where a financial institution or member of a relevant profession or occupation fails to comply with an Order under this subsection, it shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees.

(2) (a) Where an NCA investigative officer has reasonable grounds to suspect that a law practitioner has in his possession any material evidence, other than material evidence prepared or created in contemplation of criminal proceedings, which may assist in an investigation, he may, notwithstanding any other enactment, apply to the Judge in Chambers for an Order of disclosure of such material evidence.

(b) The Judge in Chambers shall not issue an Order under paragraph (a) unless he is satisfied that –

(i) the material evidence is required for the purpose of an investigation that the NCA is carrying out or a contemplated criminal proceedings;

(ii) having regard to the need to protect legal professional privilege, it is in the public interest that the Order be issued; or

(iii) the disclosure is otherwise necessary, in all circumstances.

(3) Notwithstanding any other enactment, the NCA may, for the purpose of an investigation, direct any person, bank, financial institution, cash dealer or member of a relevant profession or occupation, to preserve such material evidence, until such time as may be reasonably required for the investigation or where prosecution is instituted, until the determination of the case.

(4) Any person who fails to comply with a direction of the NCA under subsection (3) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees.

(5) In this section –

“account information” means information relating to the account held in a financial institution by a person solely or jointly with another person, including any details pertaining to financial transactions;

“customer information” means –

(a) information as to whether a person holds or has held an account at a financial institution solely or jointly with another person;

(b) information relating to any evidence obtained by the financial institution under, or for the purposes of, an enactment relating to a financial crime, a cybercrime or other complex, serious and organised crime; and

(c) such particulars, relating to the account or the holder as may, in the opinion of the NCA, be relevant;

“financial institution” –

(a) has the same meaning as in the Financial Intelligence and Anti-Money Laundering Act; and
 (b) includes a bank;
 “member of relevant profession or occupation” has the same meaning as in the Financial Intelligence and Anti-Money Laundering Act.

Proposed amendment

46. Disclosure of account and customer information

~~(1) (a) Where an NCA investigative officer has reasonable grounds to suspect that—
 (i) any property in the possession, or under the control, of a person is proceeds, an instrumentality or a terrorist property;
 (ii) the customer information or account information of any person is likely to be of substantial value to any investigation being carried out; or
 (iii) it is in the public interest that the customer information or account information be provided;
 he may, by an ex parte application, apply to the Judge in Chambers for an Order to direct a financial institution or member of relevant profession or occupation to provide such customer information or account information, including any details pertaining to financial transactions, as it may have relating to the person specified in the application.
 (b) The Judge in Chambers shall issue an Order under paragraph (a) where he is satisfied that the requested customer or account information is material to any investigation into a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime.
 (c) Where any customer information or account information is contained in an electronic device, the Judge in Chambers may direct the financial institution or member of a relevant profession or occupation to provide it in a form in which it is accessible or may be retrieved.
 (d) Where the Judge in Chambers issues an Order under this subsection, the financial institution or member of a relevant profession or occupation shall, within 21 days of the Order, provide the customer information or account information to the NCA.
 (e) Where a financial institution or member of a relevant profession or occupation fails to comply with an Order under this subsection, it shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees.~~

~~(2) (a) Where an NCA investigative officer has reasonable grounds to suspect that a law practitioner has in his possession any material evidence, other than material evidence prepared or created in contemplation of criminal proceedings, which may assist in an investigation, he may, notwithstanding any other enactment, apply to the Judge in Chambers for an Order of disclosure of such material evidence.
 (b) The Judge in Chambers shall not issue an Order under paragraph (a) unless he is satisfied that—
 (i) the material evidence is required for the purpose of an investigation that the NCA is carrying out or a contemplated criminal proceedings;
 (ii) having regard to the need to protect legal professional privilege, it is in the public interest that the Order be issued; or
 (iii) the disclosure is otherwise necessary, in all circumstances.~~

~~(3) Notwithstanding any other enactment, the NCA may, for the purpose of an investigation, direct any person, bank, financial institution, cash dealer or member of a relevant profession or occupation, to preserve such material evidence, until such time as may be reasonably required for the investigation or where prosecution is instituted, until the determination of the case.~~

~~(4) Any person who fails to comply with a direction of the NCA under subsection (3) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees.~~

~~(5) In this section—
 “account information” means information relating to the account held in a financial institution by a person solely or jointly with another person, including any details pertaining to financial transactions;
 “customer information” means—
 (a) information as to whether a person holds or has held an account at a financial institution solely or jointly with another person;
 (b) information relating to any evidence obtained by the financial institution under, or for the purposes of, an enactment relating to a financial crime, a cybercrime or other complex, serious and organised crime; and
 (c) such particulars, relating to the account or the holder as may, in the opinion of the NCA, be relevant;
 “financial institution”—
 (a) has the same meaning as in the Financial Intelligence and Anti-Money Laundering Act; and
 (b) includes a bank;~~

~~“member of relevant profession or occupation” has the same meaning as in the Financial Intelligence and Anti-Money Laundering Act.~~

46. Disclosure and preservation of account and customer information

(1) Where an NCA investigative officer has reasonable grounds to believe that specified account or customer information is relevant and of substantial value to an investigation within the lawful jurisdiction of the NCA, the officer may, by ex parte application supported by affidavit, apply to the Judge in Chambers for an Order directing a financial institution or member of a relevant profession or occupation to provide that information.

(2) The Judge may issue an Order only where satisfied that –

(a) the information sought is materially relevant to a specified investigation or contemplated criminal proceedings;

(b) the request is necessary and proportionate;

(c) the categories of information, account, person and relevant time period are described with reasonable specificity; and

(d) appropriate safeguards have been considered for legally privileged, confidential and unrelated personal data.

(3) An Order may require information to be provided in an accessible form, may specify the period for compliance and may prohibit notification of the subject for a period fixed by the Judge where such notification would create a substantial risk of prejudicing the investigation.

(4) A financial institution or member of a relevant profession or occupation that, without reasonable excuse, fails to comply with an Order under this section shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees.

(5) No Order shall require a law practitioner or law firm to disclose a communication, document or material protected by legal professional privilege, unless the Judge is satisfied that privilege does not attach under the law, including because the communication or material was made or used for the purpose of furthering a crime or fraud. Where privilege is disputed, the Judge may direct that the material be sealed and reviewed by an independent person or by the Court before disclosure to the investigative team.

(6) The NCA may, where there is a real risk that relevant material will be altered, destroyed, concealed or rendered inaccessible, issue a written preservation notice requiring specified material to be preserved for a period not exceeding 30 days. Any extension shall require an Order of a Judge in Chambers.

(7) A preservation notice shall not authorise the NCA to inspect or obtain the preserved material except pursuant to a lawful power or Court order.

(8) Information obtained under this section shall be processed only for a lawful investigation, prosecution or related proceeding, subject to applicable data-protection principles, access controls, audit logging and retention limits.

(9) In this section –

‘account information’ means information relating to an account held in a financial institution by a person solely or jointly with another person, including details pertaining to financial transactions;

‘customer information’ means information as to whether a person holds or has held an account, information lawfully held for financial-crime compliance purposes, and such other particulars concerning the account or holder as are specified in an Order;

‘financial institution’ has the same meaning as in the Financial Intelligence and Anti-Money Laundering Act and includes a bank;

‘member of relevant profession or occupation’ has the same meaning as in the Financial Intelligence and Anti-Money Laundering Act.

Rationale

The circulated clause includes a stand-alone ‘public interest’ ground, extends to ‘any other crime’, contains a broad non-judicial preservation power of potentially indefinite duration, and frames privilege in a way that could allow an Order on alternative grounds despite privilege concerns. The rewrite requires material relevance, necessity and proportionality, limits preservation without judicial approval, and makes legal professional privilege a substantive barrier subject only to recognised legal exceptions and judicial control.

Part C — Consolidated drafting note

Clauses 37 to 46 are interdependent. If Parliament adopts the proposed jurisdictional, questioning, search, seizure and financial-information safeguards, consequential cross-references should be checked in clauses 47–55 (data inspection and specialised investigative techniques), clauses 56–59 (arrest, detention and DPP), clauses 60–64 (flagging and operational protocol), clause 76 (confidentiality), clause 79 (protection from liability) and clause 84 (savings and transition). In particular, no later clause should recreate a broader coercive power indirectly than the safeguards proposed here permit directly.

Legal reference points for Part C

Reference	Relevance
Constitution of Mauritius	Sections 3 and 5 recognise liberty/security and protection of law; section 9 protects privacy of home and other property; section 10 secures fair-hearing protections.
Data Protection Act 2017	Section 44 permits criminal-investigation exceptions only where they constitute a necessary and proportionate measure in a democratic society; general processing principles require lawful, fair, purpose-limited and data-minimised processing.
Law Practitioners Act	Statutory framework recognises law-practitioner/client privilege, including for law firms.
Circulated NCA Bill	Clauses 31–46 reproduced in this Part are taken from the National Crime Agency Bill 2026 supplied for this review.

Clauses 47–59: Amendment Matrix

Cl.	Subject	Status	Principal issue
47	Expedited preservation and partial disclosure of traffic data	AMEND	Targeted notice, minimum partial disclosure, judicial extension, challenge and audit.
48	Production Order	AMEND	Judicial necessity/proportionality, specificity, privilege and right to vary.
49	Real-time collection of traffic data	REWRITE	Time-limited targeted collection, minimisation and no systemic weakening of security.
50	Interception of content data	REWRITE	Highest threshold, no bulk interception, strict duration, privilege and minimisation.
51	Deletion Order	REWRITE	Narrow unlawful-content test, hearing/review rights and preservation of evidence.
52	Limited use of disclosed computer data	REWRITE	Purpose limitation, remove open-ended public-interest reuse, retention/destruction controls.
53	Controlled operation and surveillance	REWRITE	Written authorisation, anti-entrapment limits and judicial control of prolonged surveillance.
54	Intrusive surveillance, covert intelligence and equipment interception	REWRITE	Strict judicial warrant, defined scope/duration, CHIS and equipment-interference safeguards.
55	Evidence gathered during investigative techniques	REWRITE	No automatic admissibility; preserve court control, legality, fairness and chain of custody.
56	Powers of arrest	REWRITE	Necessity-based arrest, rights on arrest and judicial warrant for non-attendance.
57	Detention in police cell	REWRITE	Police/court custody framework; remove DG parole power; constitutional safeguards.
58	Referral to Director of Public Prosecutions	AMEND	Complete file, exculpatory material, non-binding NCA

Cl.	Subject	Status	Principal issue
			recommendation and DPP independence.
59	Prosecution	AMEND	DPP retains charging/prosecution control; NCA counsel only under written DPP authority.

CLAUSE 47 — EXPEDITED PRESERVATION AND PARTIAL DISCLOSURE OF TRAFFIC DATA

STATUS	AMEND	Fast preservation without creating an unchecked access power
--------	-------	--

Government text

47. Expedited preservation and partial disclosure of traffic data

(1) Where an NCA investigative officer has reasonable grounds to suspect that –

(a) any specified traffic data stored in any computer system or device, or by means of a computer system, is reasonably required for the purpose of an investigation for a financial crime, a cybercrime or other complex, serious and organised crime; and

(b) there is a risk that the traffic data may be modified, lost, destroyed or rendered inaccessible,

he shall serve a notice on the person who is in possession or control of the traffic data, requiring the person to –

(i) undertake expeditious preservation of such available traffic data regardless of whether one or more service providers were involved in the transmission of that communication; or

(ii) disclose required traffic data concerning that communication in order to identify the service providers and the path through which communication was transmitted.

(2) The data specified in the notice referred to in subsection (1) shall be preserved and its integrity shall be maintained for a period not exceeding 90 days.

(3) The period of preservation and maintenance of integrity may be extended for a period exceeding 90 days if, on an application by the NCA investigative officer to the Judge in Chambers, the Judge is satisfied that –

(a) an extension of the period of preservation is reasonably required for the purpose of an investigation or prosecution for a financial crime, a cybercrime or other complex, serious and organised crime;

(b) there is a real risk that the traffic data may be modified, lost, destroyed or rendered inaccessible.

(4) The person in possession or control of the traffic data shall be responsible to preserve the data specified –

(a) for the period specified in the notice for preservation and maintenance of integrity, or for any extension thereof permitted by the Judge in Chambers; and

(b) for the period specified to keep confidential any preservation ordered under this section.

Proposed amendment

~~47. Expedited preservation and partial disclosure of traffic data~~

~~(1) Where an NCA investigative officer has reasonable grounds to suspect that –~~

~~(a) any specified traffic data stored in any computer system or device, or by means of a computer system, is reasonably required for the purpose of an investigation for a financial crime, a cybercrime or other complex, serious and organised crime; and~~

~~(b) there is a risk that the traffic data may be modified, lost, destroyed or rendered inaccessible;~~

~~he shall serve a notice on the person who is in possession or control of the traffic data, requiring the person to –~~

~~(i) undertake expeditious preservation of such available traffic data regardless of whether one or more service providers were involved in the transmission of that communication; or~~

~~(ii) disclose required traffic data concerning that communication in order to identify the service providers and the path through which communication was transmitted.~~

~~(2) The data specified in the notice referred to in subsection (1) shall be preserved and its integrity shall be maintained for a period not exceeding 90 days.~~
~~(3) The period of preservation and maintenance of integrity may be extended for a period exceeding 90 days if, on an application by the NCA investigative officer to the Judge in Chambers, the Judge is satisfied that—~~
~~(a) an extension of the period of preservation is reasonably required for the purpose of an investigation or prosecution for a financial crime, a cybercrime or other complex, serious and organised crime;~~
~~(b) there is a real risk that the traffic data may be modified, lost, destroyed or rendered inaccessible.~~
~~(4) The person in possession or control of the traffic data shall be responsible to preserve the data specified—~~
~~(a) for the period specified in the notice for preservation and maintenance of integrity, or for any extension thereof permitted by the Judge in Chambers; and~~
~~(b) for the period specified to keep confidential any preservation ordered under this section.~~

47. Expedited preservation and partial disclosure of traffic data

(1) Where an NCA investigative officer has reasonable grounds, recorded in writing, to suspect that specified traffic data in the possession or control of a person is relevant and necessary to a specified investigation into a financial crime, a cybercrime or other complex, serious and organised crime, and that there is a real risk that the data may be modified, lost, destroyed or rendered inaccessible, the officer may serve a written preservation notice on that person.

(1A) A notice under subsection (1) shall identify, so far as reasonably practicable –

- (a) the data or category of data to be preserved;
- (b) the computer system, account, service or communication to which it relates;
- (c) the investigation reference;
- (d) the period of preservation; and
- (e) any reasonable security or confidentiality requirement necessary to preserve the integrity of the data or avoid prejudice to the investigation.

(1B) A notice may require –

- (a) the expeditious preservation of the specified traffic data; and
- (b) disclosure only of the minimum traffic data strictly necessary to identify the service provider or providers and the path through which the communication was transmitted.

A notice under this section shall not of itself authorise disclosure of content data or subscriber information beyond what is strictly necessary for paragraph (b).

(2) Data preserved under this section shall be preserved, and its integrity maintained, for a period not exceeding 90 days.

(3) The Judge in Chambers may, on application supported by affidavit, extend preservation for one or more further periods not exceeding 90 days each where satisfied that the extension is necessary and proportionate for a specified investigation or prosecution and that the risk referred to in subsection (1) continues to exist.

(4) A confidentiality requirement shall apply only where necessary to avoid a material risk of prejudice to the investigation and only for the period specified in the notice or by the Judge in Chambers.

(5) Preservation under this section does not authorise the NCA to access, inspect or use the preserved data. Any further disclosure or access shall require lawful authority under section 48 or another applicable enactment or court order.

(6) A person served with a notice may apply to the Judge in Chambers to vary or discharge the notice on the ground that it is unlawful, disproportionate, technically impossible or unduly burdensome, without suspending an obligation to take reasonable steps to prevent destruction of the data pending determination.

(7) The NCA shall maintain an auditable register of preservation notices and shall provide anonymised annual statistics on their use to the Independent Advisory Panel.

Rationale

The circulated clause follows the logic of expedited preservation but permits a broad notice for up to 90 days and combines preservation with partial disclosure. The amendment keeps the speed needed to prevent volatile data from disappearing while making the notice specific, separating preservation from access, limiting partial disclosure to routing information, providing a judicial challenge and requiring auditable use. This is consistent with the Budapest Convention model, which couples preservation powers with Article 15 safeguards on proportionality, scope, duration and supervision.

CLAUSE 48 — PRODUCTION ORDER

STATUS	AMEND	Judicial specificity, privilege and proportionality
--------	-------	---

Government text

48. Production Order

(1) Where the disclosure of data is required for the purpose of an investigation or prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, an NCA investigative officer may make an application to the Judge in Chambers for an Order compelling –

(a) a person in the territory of Mauritius to submit specified data in that person's possession or control, which is stored in a computer system or device;

(b) any service provider offering its services in the territory of Mauritius to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material, to which an investigation relates, consists of computer data stored in a computer system, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is easily understood.

Proposed amendment

~~48. Production Order~~

~~(1) Where the disclosure of data is required for the purpose of an investigation or prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, an NCA investigative officer may make an application to the Judge in Chambers for an Order compelling –~~

~~(a) a person in the territory of Mauritius to submit specified data in that person's possession or control, which is stored in a computer system or device;~~

~~(b) any service provider offering its services in the territory of Mauritius to submit subscriber information in relation to such services in that service provider's possession or control;~~

~~(2) Where any material, to which an investigation relates, consists of computer data stored in a computer system, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is easily understood.~~

48. Production Order

(1) An NCA investigative officer may apply to the Judge in Chambers, by affidavit, for a Production Order compelling a person in Mauritius to produce specified computer data in that person's possession or control, or a service provider offering services in Mauritius to produce specified subscriber information.

(2) The Judge in Chambers shall not issue an Order unless satisfied that –

(a) there are reasonable grounds to believe that the specified data exists and is in the possession or control of the person to whom the Order is directed;

(b) the data is relevant and of material value to a specified investigation or prosecution for a financial crime, a cybercrime or other complex, serious and organised crime;

(c) production is necessary and proportionate to the legitimate investigative purpose pursued; and

(d) the Order is sufficiently specific and does not require the disclosure of material protected by legal professional privilege or any other privilege recognised by law.

(3) An Order shall specify the person or service provider to whom it is directed, the data to be produced, the form and manner of production, the time for compliance, any confidentiality requirement and any condition necessary to protect the rights and legitimate interests of third parties.

(4) No Order shall require a person to create data which does not exist, to develop a technical capability which the person does not possess, or to introduce a systemic weakness or vulnerability into a computer system.

(5) Where material is claimed to be privileged, it shall be placed under seal and shall not be examined by the NCA unless and until the Judge in Chambers determines that the material is not privileged or otherwise permits examination according to law.

(6) A person affected by an Order may apply to the Judge in Chambers to vary or discharge it where compliance is impossible, unduly burdensome, overbroad or otherwise unlawful.

(7) Data produced under this section shall be handled in accordance with section 52 and with applicable data-protection and evidential requirements.

Rationale

Judicial authorisation is already present in the circulated clause. The amendment strengthens the test the Judge must apply, requires specificity and proportionality, protects privileged material, provides a mechanism to vary an overbroad order and prevents a production order from being used to compel the creation of new surveillance capabilities or a systemic security weakness.

CLAUSE 49 — REAL-TIME COLLECTION OF TRAFFIC DATA

STATUS	REWRITE	Targeted, time-limited and minimised real-time collection
---------------	----------------	--

Government text

49. Real-time collection of traffic data

Where an NCA investigative officer has reasonable grounds to suspect that traffic data is relevant for the purpose of investigation and prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, he may apply to the Judge in Chambers for an Order –

- (a) authorising the collection or recording of traffic data on Mauritian territory by technical means, in real-time, associated with specified communications transmitted by means of any computer system;
- (b) compelling a service provider, within its technical capabilities, to –
 - (i) effect such collection and recording specified in paragraph (a);
 - (ii) cooperate with, and assist, the NCA to effect such collection and recording; or
- (c) compelling a service provider to keep confidential the fact of the execution of any power provided under this section and any information relating to it.

Proposed amendment

~~49. Real-time collection of traffic data~~

~~Where an NCA investigative officer has reasonable grounds to suspect that traffic data is relevant for the purpose of investigation and prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, he may apply to the Judge in Chambers for an Order –~~

- ~~(a) authorising the collection or recording of traffic data on Mauritian territory by technical means, in real-time, associated with specified communications transmitted by means of any computer system;~~
- ~~(b) compelling a service provider, within its technical capabilities, to –~~
 - ~~(i) effect such collection and recording specified in paragraph (a);~~
 - ~~(ii) cooperate with, and assist, the NCA to effect such collection and recording; or~~
- ~~(c) compelling a service provider to keep confidential the fact of the execution of any power provided under this section and any information relating to it.~~

49. Real-time collection of traffic data

(1) An NCA investigative officer may, with the written approval of the Director-General, apply by affidavit to the Judge in Chambers for an Order authorising the targeted real-time collection or recording of traffic data associated with specified communications.

(2) The Judge in Chambers shall issue an Order only where satisfied that –

- (a) there are reasonable grounds to suspect that a specified financial crime, cybercrime or other complex, serious and organised crime has been or is being committed;**
- (b) the traffic data sought is likely to be of substantial value to the investigation or prosecution;**
- (c) real-time collection is necessary and proportionate; and**
- (d) the investigative objective cannot reasonably be achieved by a less intrusive measure.**

(3) An Order shall specify –

- (a) the offence and investigation to which it relates;
- (b) the person, account, device, service or communication to be targeted, so far as known;
- (c) the categories of traffic data authorised to be collected;
- (d) the service provider, where applicable;
- (e) the technical method authorised;
- (f) the date on which collection may commence; and
- (g) a period not exceeding 30 days.

(4) The Judge may compel a service provider, within its existing technical capabilities, to effect the authorised collection or to cooperate with and assist the NCA. No Order shall require the provider to introduce a systemic weakness, vulnerability or generalised interception capability into its systems.

(5) A confidentiality requirement may be imposed only where necessary to protect the investigation and shall be limited in duration.

(6) An Order may be renewed only on a fresh application demonstrating continuing necessity and proportionality, and each renewal shall not exceed 30 days.

(7) The NCA shall apply data-minimisation measures, maintain an auditable record of collection and access, and delete or irreversibly anonymise data not relevant to the authorised purpose as soon as reasonably practicable, subject to any legal obligation to preserve evidence.

(8) Where collection is reasonably likely to capture legally privileged or otherwise legally protected confidential communications, that fact shall be disclosed to the Judge, who shall impose additional handling safeguards.

Rationale

Real-time traffic collection can reveal detailed patterns of association and movement even without content. The circulated clause contains judicial authorisation but no express necessity test, duration, renewal standard or minimisation duty. The amendment supplies those safeguards and prevents the Order from becoming a route to systemic weakening of communications infrastructure.

CLAUSE 50 — INTERCEPTION OF CONTENT DATA

STATUS	REWRITE	Strict judicial control over the most intrusive data power
---------------	----------------	---

Government text

50. Interception of content data

Where an NCA investigative officer has reasonable grounds to suspect that any content data is relevant for the investigation and prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, he may apply to the Judge in Chambers for an Order to –

- (a) collect or record content data in the territory of Mauritius by technical means in real-time of specified communications by means of a computer system;
- (b) compel a service provider, within its existing technical capabilities, to –
 - (i) collect or record content data by technical means on the territory of Mauritius;
 - (ii) cooperate with, and assist, the NCA in the collection or recording of content data, in real-time, of specified communications in the territory of Mauritius, transmitted by means of a computer system; or
- (c) compel a service provider to keep the confidentiality of the fact of the execution of any power provided for in this section and any information relating to it.

Proposed amendment

~~50. Interception of content data~~

~~Where an NCA investigative officer has reasonable grounds to suspect that any content data is relevant for the investigation and prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, he may apply to the Judge in~~

~~Chambers for an Order to—~~

- ~~(a) collect or record content data in the territory of Mauritius by technical means in real-time of specified communications by means of a computer system;~~
~~(b) compel a service provider, within its existing technical capabilities, to—~~
~~(i) collect or record content data by technical means on the territory of Mauritius;~~
~~(ii) cooperate with, and assist, the NCA in the collection or recording of content data, in real-time, of specified communications in the territory of Mauritius, transmitted by means of a computer system; or~~
~~(c) compel a service provider to keep the confidentiality of the fact of the execution of any power provided for in this section and any information relating to it.~~

50. Interception of content data

- (1) An NCA investigative officer may, with the written approval of the Director-General, apply by affidavit to the Judge in Chambers for an Order authorising the targeted interception, collection or recording in real time of specified content data.
- (2) The Judge in Chambers shall not issue an Order unless satisfied that –
- (a) there are reasonable grounds to suspect that a specified financial crime, cybercrime or other complex, serious and organised crime has been or is being committed;
 - (b) the interception is likely to obtain evidence of substantial value or information necessary to prevent the continuation of that crime;
 - (c) the interception is necessary and proportionate, having regard to the seriousness of the offence, the extent of the expected intrusion and the rights of persons not under investigation; and
 - (d) less intrusive investigative measures have been tried and failed, are unlikely to succeed, or would create a substantial risk to the investigation or to life or safety.
- (3) An Order shall identify, so far as reasonably practicable, the target, account, device, service or communication; the offence; the nature of the content data authorised to be intercepted; the technical method; the service provider, if any; and the date of commencement and duration of the interception.
- (4) An Order shall not authorise bulk, indiscriminate or untargeted interception and shall be valid for no more than 30 days.
- (5) The Judge may compel a service provider, within its existing technical capabilities, to carry out or assist with the interception. No Order shall require the introduction of a systemic weakness, vulnerability, backdoor or generalised interception capability.
- (6) A renewal shall require a fresh application showing continuing necessity and proportionality and shall not exceed 30 days.
- (7) The NCA shall employ reasonable minimisation procedures to reduce the acquisition, retention, dissemination and use of communications unrelated to the authorised purpose.
- (8) Where interception is reasonably likely to obtain legally privileged or otherwise legally protected confidential communications, the application shall expressly disclose that risk and the Judge shall impose special handling, sealing and review arrangements. Material determined to be legally privileged shall not be used for investigative or evidential purposes.
- (9) A confidentiality direction to a service provider shall be limited to what is necessary to protect the investigation and shall remain subject to variation by the Judge in Chambers.
- (10) The NCA shall maintain complete audit records of the making, renewal, execution, access, dissemination and termination of every interception Order.

Rationale

Content interception is among the most intrusive powers in the Bill. Judicial involvement alone is not a complete safeguard if the statute does not define the threshold, duration, target, collateral-data treatment and renewal test. The amendment makes interception targeted rather than general, introduces strict necessity and proportionality, protects privileged communications and requires minimisation and audit.

CLAUSE 51 — DELETION ORDER

STATUS	REWRITE	Narrow legal basis, due process and preservation of evidence
---------------	----------------	---

Government text

51. Deletion Order

The Judge in Chambers may, for the purpose of this Act, upon application by an NCA investigative officer, and on being satisfied that a computer system or any other device contains any unlawful material or activity, order that such computer data be –

- (a) no longer stored on and made available through the computer system or any other device; or
- (b) deleted or destroyed.

Proposed amendment

~~51. Deletion Order~~

~~The Judge in Chambers may, for the purpose of this Act, upon application by an NCA investigative officer, and on being satisfied that a computer system or any other device contains any unlawful material or activity, order that such computer data be –~~

- ~~(a) no longer stored on and made available through the computer system or any other device; or~~
- ~~(b) deleted or destroyed.~~

51. Deletion or disabling-access Order

- (1) The Judge in Chambers may, on application by an NCA investigative officer supported by affidavit, order specified computer data to be disabled from access, removed or, where strictly necessary, deleted only where satisfied that –
- (a) the specified data is itself unlawful to possess, publish, distribute or make available under an enactment identified in the application;
 - (b) continued availability of the data would constitute or facilitate a continuing offence or create a serious and identifiable harm; and
 - (c) the measure ordered is necessary and proportionate.
- (2) The application shall identify the data, its location, the person or service provider believed to control it, the legal basis on which it is alleged to be unlawful and the technical measure sought.
- (3) Unless the Judge is satisfied that notice would create a real risk of destruction of evidence, flight, serious harm or material prejudice to an investigation, the person whose rights are directly affected shall be given a reasonable opportunity to be heard before a final deletion Order is made.
- (4) Where an Order is made without notice, the Judge shall provide for notice as soon as the grounds for secrecy no longer apply and the affected person may apply to vary or discharge the Order.
- (5) The Judge shall prefer the least intrusive effective measure. Temporary disabling of access or preservation shall be ordered instead of permanent deletion where it would adequately meet the lawful purpose.
- (6) No data required as evidence in an investigation, prosecution, appeal or other judicial proceeding shall be destroyed. Where necessary, a verified forensic copy shall be preserved under seal or such other safeguards as the Judge directs.
- (7) An Order shall be technically specific and shall not authorise the deletion, alteration or destruction of unrelated lawful data.

Rationale

The phrase “unlawful material or activity” is too open-ended for a permanent destruction power. The rewrite ties the remedy to an identified legal prohibition, requires necessity and proportionality, gives affected persons a hearing where practicable, protects evidence needed for proceedings and requires the least intrusive technically specific measure.

CLAUSE 52 — LIMITED USE OF DISCLOSED COMPUTER DATA AND INFORMATION

STATUS	REWRITE	Purpose limitation, no open-ended public-interest reuse, and retention controls
--------	---------	---

Government text

52. Limited use of disclosed computer data and information

(1) Any computer data obtained under this Act by any person authorised, in writing, by the NCA shall be used for the purpose of an investigation or the prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, unless such computer data is sought in –

- (a) accordance with any other enactment;
- (b) compliance with an Order from a Court;
- (c) relation to the prevention of injury or other damage to the health of a person or serious loss of, or damage to, property; or
- (d) the public interest.

(2) Subject to subsections (1) and (3), any person authorised by the NCA shall, on receipt of a request, in writing, permit a person who had the custody or control of a computer system to access and copy computer data on the computer system.

(3) Any person authorised, in writing, by the NCA, may refuse to give access to computer data or provide copies of such computer data where he has reasonable grounds to suspect that –

- (a) possession of the data constitutes, or may lead to, or assist in, a criminal offence; or
- (b) giving access or copies prejudices the investigation in connection with which the search was carried out, another ongoing investigation, or any criminal proceedings that are pending or which may be brought in relation to any of those investigations.

Proposed amendment

~~52. Limited use of disclosed computer data and information~~

~~(1) Any computer data obtained under this Act by any person authorised, in writing, by the NCA shall be used for the purpose of an investigation or the prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, unless such computer data is sought in –~~

- ~~(a) accordance with any other enactment;~~
- ~~(b) compliance with an Order from a Court;~~
- ~~(c) relation to the prevention of injury or other damage to the health of a person or serious loss of, or damage to, property; or~~
- ~~(d) the public interest.~~

~~(2) Subject to subsections (1) and (3), any person authorised by the NCA shall, on receipt of a request, in writing, permit a person who had the custody or control of a computer system to access and copy computer data on the computer system.~~

~~(3) Any person authorised, in writing, by the NCA, may refuse to give access to computer data or provide copies of such computer data where he has reasonable grounds to suspect that –~~

- ~~(a) possession of the data constitutes, or may lead to, or assist in, a criminal offence; or~~
- ~~(b) giving access or copies prejudices the investigation in connection with which the search was carried out, another ongoing investigation, or any criminal proceedings that are pending or which may be brought in relation to any of those investigations.~~

52. Purpose limitation, retention and access to computer data

(1) Computer data obtained under this Act shall be collected, accessed, used and disclosed only for the specific lawful purpose for which it was obtained, except as provided in this section.

(2) Data may be used or disclosed for a different criminal investigation or prosecution only –

- (a) pursuant to an Order of a Court finding the further use necessary and proportionate; or**
- (b) where the use is immediately necessary to prevent a real and imminent risk of death or serious bodily injury, in which case written approval shall be obtained from the Director-General or Deputy Director-General and the Judge in Chambers shall be informed as soon as reasonably practicable.**

(3) Nothing in this section authorises further use or disclosure merely because it is said to be in the “public interest”. Any further use must have a specific legal basis and satisfy applicable constitutional and data-protection requirements.

(4) The NCA shall implement access controls, security measures and auditable logs showing who accessed, copied, disclosed, altered or exported data obtained under this Part.

(5) Data shall be retained only for so long as reasonably necessary for the authorised investigation, prosecution, appeal, asset-recovery proceeding or other lawful purpose. Retention shall be periodically reviewed and data no longer required shall be securely deleted or irreversibly anonymised, subject to any legal obligation to preserve a record or evidence.

(6) Subject to subsection (7), a person who had lawful custody or control of a computer system or data seized or copied by the NCA may, by written request, obtain access to or a copy of data reasonably required for legitimate personal or business purposes.

(7) Access may be postponed or refused only to the extent that a specified legal ground exists, including a real risk of prejudicing an investigation or proceeding, facilitating an offence, disclosing protected information or compromising another person’s rights. The reasons shall be recorded in writing and the person may apply to the Judge in Chambers for review.

(8) Processing under this section shall remain subject to the Data Protection Act and to any lawful restriction or exception applicable to criminal investigations.

Rationale

The circulated clause states a purpose limitation but then creates broad exceptions, including a stand-alone “public interest” ground. The rewrite removes that open-ended route, creates a defined emergency exception, imposes retention, minimisation and audit controls and gives a person a reviewable route to regain necessary data without prejudicing an investigation.

CLAUSE 53 — CONTROLLED OPERATION AND SURVEILLANCE

STATUS	REWRITE	Authorised undercover work without a blank cheque for criminal conduct or prolonged surveillance
---------------	----------------	---

Government text

53. Controlled operation and surveillance
 (1) An investigative officer may, with the approval of the Director-General, use the following investigative techniques for the purpose of gathering intelligence or evidence –
 (a) controlled operation; and
 (b) surveillance.
 (2) In this section –
 “controlled operation” means an operation which allows for the performance of an act by one person that would qualify as a financial crime, a cybercrime or other complex, serious and organised crime for the purpose of identifying any person involved in the commission of the crime;
 “surveillance” means the continual act of monitoring, observing or listening to a person, his movements, conversations or other activities and communications, from a public place, with the likely result of obtaining private information about that person or another person.

Proposed amendment

~~53. Controlled operation and surveillance~~

~~(1) An investigative officer may, with the approval of the Director-General, use the following investigative techniques for the purpose of gathering intelligence or evidence –~~

~~(a) controlled operation; and~~

~~(b) surveillance.~~

~~(2) In this section –~~

~~“controlled operation” means an operation which allows for the performance of an act by one person that would qualify as a financial crime, a cybercrime or other complex, serious and organised crime for the purpose of identifying any person involved in the commission of the crime;~~

~~“surveillance” means the continual act of monitoring, observing or listening to a person, his movements, conversations or other activities and communications, from a public place, with the likely result of obtaining private information about that person or another person.~~

53. Controlled operation and directed surveillance

(1) An NCA investigative officer may use a controlled operation or directed surveillance only pursuant to a written authorisation stating the offence under investigation, the objective of the operation, the persons or activity targeted, the technique authorised and the period of authorisation.

(2) The Director-General may authorise a controlled operation only where satisfied that it is necessary and proportionate for the investigation of a specified financial crime, cybercrime or other complex, serious and organised crime and that the objective cannot reasonably be achieved by less intrusive means.

(3) Where a controlled operation contemplates conduct which, but for lawful authorisation, would constitute a criminal offence, the prior written consent of the Director of Public Prosecutions shall be obtained. No authorisation may permit conduct intended to cause death or serious bodily injury, a sexual offence, the fabrication or planting of evidence, perjury, the obstruction or perversion of justice, or conduct expressly prohibited from authorisation by another enactment.

(4) A controlled operation shall not be used to induce a person to commit an offence which that person would not otherwise have intended to commit. Nothing in this subsection prevents officers from providing an opportunity to a person already willing to engage in unlawful conduct, subject to the ordinary law.

(5) Directed surveillance from a public place may be authorised by the Director-General for a period not exceeding 7 days. Surveillance extending beyond 7 days in any 30-day period, involving systematic location tracking, or using technology capable of revealing intimate or highly sensitive private information shall require an Order of the Judge in Chambers applying the principles in section 54.

(6) Every authorisation shall be reviewed before renewal, and a complete operational log shall be maintained for subsequent audit by the Internal Affairs Division and inspection by the Independent Advisory Panel, without permitting either body to direct the investigation.

(7) In this section –

“controlled operation” means a lawfully authorised operation in which conduct is permitted for the purpose of identifying, preventing or obtaining evidence of participation in a specified offence;

“directed surveillance” means planned or systematic monitoring, observing or listening from a public place where the operation is likely to obtain private information about a person.

Rationale

The circulated definition permits a controlled operation involving conduct that would itself qualify as a crime, while leaving approval solely to the Director-General. The rewrite adds written scope, necessity, proportionality, DPP involvement where otherwise criminal conduct is contemplated, anti-entrapment limits, prohibited conduct and judicial control for prolonged or technologically enhanced surveillance.

CLAUSE 54 — INTRUSIVE SURVEILLANCE, COVERT INTELLIGENCE AND EQUIPMENT INTERCEPTION

STATUS	REWRITE	Judicial warrant with strict scope, duration, CHIS and equipment-interference safeguards
---------------	----------------	---

Government text

54. Intrusive surveillance, covert intelligence and equipment interception

(1) Notwithstanding any other enactment, where an NCA investigative officer has reasonable grounds to suspect that a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime has been, is being, or is likely to be, committed by any person, the investigative officer may, with the approval of the Director-General, apply to the Judge in Chambers for an Order to use the following investigative techniques for the purpose of gathering intelligence or evidence –

(a) intrusive surveillance;

(b) the conduct and use of covert intelligence human source; or

(c) equipment interception.

(2) Where, on an application made under subsection (1), the Judge in Chambers is satisfied that a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime has been, is being, or is likely to be, committed, and the techniques proposed to be used are proportionate, the Judge may grant the Order for such period as he may determine.

(3) In this section –

“conduct and use of covert intelligence human source” means inducing, asking or assisting a person to engage in the conduct of covert human intelligence source as undercover agent to obtain information by means of the conduct of such a source;

“covert human intelligence source” means a person who –

(a) provides intelligence gathered by interpersonal contact to assist in investigations;

(b) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating surveillance or intrusive surveillance;

(c) covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(d) covertly discloses information obtained by the use of a relationship, or as a consequence of the existence of such a relationship;

“equipment interception” means either remotely or physically interfering with computers or computer-like devices such as, inter alia, tablets, smart phones, cables, wires and static storage devices, for the purpose of obtaining communications, equipment data or other information;

“intrusive surveillance” –

(a) means an act of monitoring, observing or listening to a person, his movements, conversations or other activities and communications, from within a place other than a public place; and

(b) includes –

(i) surveillance from any residential premises or in any private vehicle or private property; and

(ii) the use of any kind of surveillance device, drone or other electronic device to enter a place other than a public place.

Proposed amendment

~~54. Intrusive surveillance, covert intelligence and equipment interception~~

~~(1) Notwithstanding any other enactment, where an NCA investigative officer has reasonable grounds to suspect that a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime has been, is being, or is likely to be, committed by any person, the investigative officer may, with the approval of the Director-General, apply to the Judge in Chambers for an Order to use the following investigative techniques for the purpose of gathering intelligence or evidence –~~

~~(a) intrusive surveillance;~~

~~(b) the conduct and use of covert intelligence human source; or~~

~~(c) equipment interception.~~

~~(2) Where, on an application made under subsection (1), the Judge in Chambers is satisfied that a financial crime, a cybercrime or other complex, serious and organised crime, or any other crime has been, is being, or is likely to be, committed, and the techniques proposed to be used are proportionate, the Judge may grant the Order for such period as he may determine.~~

~~(3) In this section –~~

~~“conduct and use of covert intelligence human source” means inducing, asking or assisting a person to engage in the conduct of covert human intelligence source as undercover agent to obtain information by means of the conduct of such a source;~~

~~“covert human intelligence source” means a person who –~~

~~(a) provides intelligence gathered by interpersonal contact to assist in investigations;~~

~~(b) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating surveillance or intrusive surveillance;~~

~~(c) covertly uses such a relationship to obtain information or to provide access to any information to another person; or~~

~~(d) covertly discloses information obtained by the use of a relationship, or as a consequence of the existence of such a relationship;~~

~~“equipment interception” means either remotely or physically interfering with computers or computer-like devices such as, inter alia, tablets, smart phones, cables, wires and static storage devices, for the purpose of obtaining communications, equipment data or other information;~~

~~“intrusive surveillance” –~~

~~(a) means an act of monitoring, observing or listening to a person, his movements, conversations or other activities and communications, from within a place other than a public place; and~~

~~(b) includes –~~

~~(i) surveillance from any residential premises or in any private vehicle or private property; and~~

~~(ii) the use of any kind of surveillance device, drone or other electronic device to enter a place other than a public place.~~

54. Intrusive surveillance, covert human intelligence and equipment interference

(1) An NCA investigative officer may, with the written approval of the Director-General, apply by affidavit to the Judge in Chambers for an Order authorising –

(a) intrusive surveillance;

(b) the conduct and use of a covert human intelligence source; or

(c) targeted equipment interference,

for the purpose of gathering intelligence or evidence in a specified investigation into a financial crime, a cybercrime or other complex, serious and organised crime.

(2) The Judge shall not grant an Order unless satisfied that –

(a) there are reasonable grounds to suspect that the specified offence has been or is being committed, or is about to be committed in circumstances presenting a real and imminent risk;

(b) the technique is likely to obtain information of substantial value to the investigation or to prevent the commission or continuation of the specified offence;

(c) the technique is necessary and proportionate;

(d) the objective cannot reasonably be achieved by a less intrusive measure; and

(e) the proposed safeguards adequately protect persons not under investigation and any legally privileged or otherwise legally protected confidential material.

(3) An Order shall specify the offence, target or subject, premises, device or system so far as known, the technique authorised, the information sought, any conduct expressly authorised, the safeguards required, and the commencement and expiry of the authority. No Order shall remain in force for more than 30 days.

(4) A renewal shall require a fresh application and fresh findings of necessity and proportionality and shall not exceed 30 days.

(5) Targeted equipment interference shall not authorise bulk or indiscriminate access, interference with unrelated systems except to the minimum technically unavoidable extent, or the creation of a systemic weakness, vulnerability or generalised access mechanism.

(6) Where a covert human intelligence source is authorised, the NCA shall appoint a designated handler and controller, undertake and periodically review a risk assessment, keep a secure record of tasking and contact, and take reasonable measures for the safety and welfare of the source. A source shall not be authorised to cause death or serious bodily injury, commit a sexual offence, fabricate evidence, commit perjury, obstruct or pervert justice, or induce a person to commit an offence that the person would not otherwise have intended to commit.

(7) Where the operation is reasonably likely to obtain legally privileged material or other confidential material specially protected by law, the application shall expressly disclose that risk. The Judge shall impose a sealing, filtering or independent-review procedure and material determined to be legally privileged shall not be used for investigative or evidential purposes.

(8) Information incidentally obtained about persons outside the authorised scope shall not be retained or disseminated beyond what is strictly necessary for the authorised purpose or another purpose permitted by a court.

(9) The NCA shall keep complete audit records of every application, Order, renewal, execution, access, dissemination and termination under this section. The Independent Advisory Panel may inspect compliance records but shall not direct or interfere with individual operations.

(10) In this section –

“covert human intelligence source” means a person who covertly establishes or maintains a relationship for the purpose of obtaining or disclosing information to assist a lawful investigation;

“equipment interference” means targeted remote or physical interference with a specified computer, device, cable, wire, storage medium or related equipment for the purpose of obtaining communications, equipment data or other specified information;

“intrusive surveillance” means monitoring, observing or listening carried out from within private premises, a private vehicle or private property, or by use of a device that intrudes into such a place.

Rationale

This clause combines the Bill’s most intrusive techniques and extends them to “any other crime”. The rewrite confines the power to the NCA’s defined jurisdiction, requires a detailed judicial warrant, limits duration, requires less-intrusive alternatives to be considered, protects privilege and third parties, regulates covert human sources and prevents equipment interference from becoming a general or systemic access power.

CLAUSE 55 — EVIDENCE GATHERED DURING INVESTIGATIVE TECHNIQUES

STATUS	REWRITE	Preserve judicial control over admissibility and fairness
--------	---------	---

Government text

55. Evidence gathered during investigative techniques
Any evidence gathered using the investigative techniques under sections 53 and 54 shall be admissible in a Court of law.

Proposed amendment

~~55. Evidence gathered during investigative techniques~~

~~Any evidence gathered using the investigative techniques under sections 53 and 54 shall be admissible in a Court of law:~~

55. Evidence gathered during investigative techniques

(1) Evidence obtained under sections 53 and 54 shall not be admissible merely by reason of having been obtained under those sections. Its admissibility shall be determined by the Court in accordance with the Constitution, this Act, the law of evidence and the requirements of a fair trial.

(2) Where the lawfulness of the acquisition of evidence is reasonably challenged, the prosecution shall make available to the Court sufficient material to enable the Court to determine whether the relevant authorisation, Order and statutory safeguards were complied with, subject to any lawful protective order necessary to safeguard sensitive information.

(3) The Court may exclude evidence, or make such other order as justice requires, where evidence was obtained in material breach of this Act, where integrity or chain of custody has not been established, or where admission would render the proceedings unfair.

(4) Nothing in this section renders legally privileged material admissible contrary to law.

Rationale

A statutory statement that all evidence “shall be admissible” risks displacing the Court’s ordinary responsibility to decide relevance, legality, evidential integrity and fairness. The rewrite preserves useful evidence while leaving the final admissibility decision with the Court and creates a workable mechanism for challenges to covertly obtained material.

CLAUSE 56 — POWERS OF ARREST

STATUS	REWRITE	Constitutional threshold, necessity and judicial process for non-attendance
--------	---------	---

Government text

56. Powers of arrest

(1) An NCA investigative officer who has reasonable grounds to suspect that a person has committed, is committing, or is likely to commit, a financial crime, a cybercrime or other complex, serious and organised crime, may arrest that person.

(2) A person who, without reasonable excuse, fails to attend before the NCA in accordance with the terms of a notice under section 41(1) may be arrested by an NCA investigative officer.

Proposed amendment

56. Powers of arrest

~~(1) An NCA investigative officer who has reasonable grounds to suspect that a person has committed, is committing, or is likely to commit, a financial crime, a cybercrime or other complex, serious and organised crime, may arrest that person:~~
~~(2) A person who, without reasonable excuse, fails to attend before the NCA in accordance with the terms of a notice under section 41(1) may be arrested by an NCA investigative officer.~~

56. Powers of arrest

(1) An NCA investigative officer may arrest a person without warrant only where the officer has reasonable grounds to suspect that the person has committed, is committing, or is about to commit a financial crime, cybercrime or other complex, serious and organised crime and the arrest is necessary for one or more of the purposes set out in subsection (2).

(2) The purposes are –

- (a) preventing the commission or continuation of the offence or serious injury or loss;
- (b) preventing destruction, concealment or interference with material evidence;
- (c) preventing intimidation or interference with a witness;
- (d) preventing the person from absconding;
- (e) ascertaining the person's identity where it cannot reasonably be established otherwise; or
- (f) bringing the person promptly before a court where required by law.

(3) At the time of arrest or as soon as reasonably practicable, the officer shall identify himself as an NCA investigative officer, inform the person in a language the person understands of the fact and reasons for the arrest, give any caution required by law and inform the person of the right to consult a legal representative.

(4) Any force used in effecting an arrest shall be no more than is reasonably necessary and proportionate in the circumstances and shall comply with section 40.

(5) Where a person fails, without reasonable excuse, to comply with a notice under section 41(1), the NCA may apply to a Magistrate or Judge for a warrant to secure the person's attendance. Non-attendance alone shall not authorise warrantless arrest by an NCA investigative officer.

(6) Every arrest shall be recorded without delay, including the time, place, grounds, arresting officer, use of force if any, property taken from the person and the time and place at which the person is transferred into police custody or released.

Rationale

Section 5 of the Constitution permits deprivation of liberty on reasonable suspicion of having committed or being about to commit an offence and requires reasons for arrest, access to a legal representative and production before a court without undue delay. The circulated phrase “likely to commit” is broader and clause 56(2) allows direct arrest for failure to attend an NCA notice. The rewrite ties arrest to constitutional language, adds a necessity test and requires a judicial warrant for non-attendance.

CLAUSE 57 — DETENTION IN POLICE CELL

STATUS	REWRITE	Separate NCA investigation from police/court control of custody and release
---------------	----------------	--

Government text

57. Detention in police cell

A person arrested by an NCA investigative officer shall, unless released on parole by the Director-General or released on bail, be detained in a police cell.

Proposed amendment

~~57. Detention in police cell~~

~~A person arrested by an NCA investigative officer shall, unless released on parole by the Director-General or released on bail, be detained in a police cell.~~

57. Custody following arrest

- (1) A person arrested by an NCA investigative officer shall, unless lawfully released, be taken without undue delay to a police station or other place of lawful custody and shall thereafter be detained, released or brought before a court in accordance with the Constitution and the law governing arrest, custody and bail.
- (2) The Director-General or any NCA officer shall not have power, merely by virtue of this Act, to grant, refuse or condition bail or parole, or to direct the continuation of police detention. Decisions concerning police custody and release shall be taken by the authority empowered by law and remain subject to judicial control.
- (3) A person in custody shall be afforded reasonable facilities to consult a legal representative of his choice and shall be informed of and afforded such other rights as are guaranteed by the Constitution or any other enactment, including access to necessary medical attention and communication with a relative or other appropriate person, subject to lawful and proportionate restrictions.
- (4) Any questioning by the NCA while a person is in police custody shall be recorded in the custody record and conducted in accordance with applicable safeguards governing caution, legal representation, voluntariness and treatment of detained persons.

Rationale

The circulated provision gives the Director-General an undefined power to release an arrested person “on parole” while placing detention in a police cell. The rewrite separates investigation from custody, leaves bail and continued detention to the authorities legally responsible for those decisions, and expressly anchors custody in section 5 of the Constitution and ordinary criminal-procedure safeguards.

CLAUSE 58 — REFERRAL TO DIRECTOR OF PUBLIC PROSECUTIONS

STATUS	AMEND	Complete evidential file and express DPP independence
---------------	--------------	--

Government text

58. Referral to Director of Public Prosecutions

- (1) After conclusion of an investigation, the Director-General shall submit to the Director of Public Prosecutions a report which shall include –
 - (a) all information and statements, and a description of the material evidence, obtained in the course of the investigation; and
 - (b) the recommendations of the NCA.
- (2) After considering the report submitted under subsection (1), the Director of Public Prosecutions may –
 - (a) advise prosecution;
 - (b) require the Director-General to conduct such further investigation as he may determine; or
 - (c) advise no further action.
- (3) Notwithstanding the conclusion of an investigation, the Director-General may seek advice from the Director of Public Prosecutions during the course of the investigation.

Proposed amendment

~~58. Referral to Director of Public Prosecutions~~

~~(1) After conclusion of an investigation, the Director-General shall submit to the Director of Public Prosecutions a report which shall include—~~

- ~~(a) all information and statements, and a description of the material evidence, obtained in the course of the investigation; and~~
- ~~(b) the recommendations of the NCA.~~

~~(2) After considering the report submitted under subsection (1), the Director of Public Prosecutions may—~~

- ~~(a) advise prosecution;~~
- ~~(b) require the Director-General to conduct such further investigation as he may determine; or~~
- ~~(c) advise no further action.~~

~~(3) Notwithstanding the conclusion of an investigation, the Director-General may seek advice from the Director of Public Prosecutions during the course of the investigation.~~

58. Referral to Director of Public Prosecutions

(1) After conclusion of an investigation, the Director-General shall submit to the Director of Public Prosecutions a complete investigation file which shall include –

- (a) all material statements, information and evidence obtained in the course of the investigation, whether inculpatory or exculpatory;
- (b) an indexed description of physical, documentary and digital evidence and its chain of custody;
- (c) copies or particulars of material warrants, Orders and compulsory notices used in the investigation;
- (d) any material fact known to the NCA that may affect the legality, reliability or admissibility of evidence; and
- (e) any recommendation of the NCA, clearly identified as non-binding.

(2) After considering the file, the Director of Public Prosecutions may, in the independent exercise of constitutional and statutory functions –

- (a) advise or institute prosecution;
- (b) require or request such further investigation as is lawfully necessary;
- (c) advise that no further action be taken; or
- (d) take any other step permitted by law.

(3) The NCA shall respond promptly to any lawful request for further information or investigation from the Director of Public Prosecutions, while ensuring that all further investigative steps remain within the powers and safeguards of this Act.

(4) The Director-General may seek legal advice from the Director of Public Prosecutions during an investigation. Nothing in this Act shall require the Director of Public Prosecutions to disclose privileged prosecutorial deliberations or shall be construed as subjecting the Director of Public Prosecutions to the direction or control of the NCA.

Rationale

The circulated clause appropriately places the prosecution decision with the DPP. The amendment strengthens that safeguard by requiring the NCA to transmit the complete evidential picture, including exculpatory material and material irregularities, and by making clear that an NCA recommendation is not binding on the constitutionally independent prosecutorial decision.

CLAUSE 59 — PROSECUTION

STATUS	AMEND	Preserve DPP control while allowing specialist counsel under clear safeguards
---------------	--------------	--

Government text

59. Prosecution

(1) No prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, or any other offence committed under this Act, shall be instituted except by, or with the consent of, the Director of Public Prosecutions.

(2) Subject to subsection (3), no person, other than the Director of Public Prosecutions or any of his officers, shall conduct

prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, or for any other offence committed under this Act.

(3) A barrister of the NCA may, with the approval of the Director of Public Prosecutions, conduct prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, or for any other offence committed under this Act.

Proposed amendment

59. Prosecution

~~(1) No prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, or any other offence committed under this Act, shall be instituted except by, or with the consent of, the Director of Public Prosecutions:~~

~~(2) Subject to subsection (3), no person, other than the Director of Public Prosecutions or any of his officers, shall conduct prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, or for any other offence committed under this Act.~~

~~(3) A barrister of the NCA may, with the approval of the Director of Public Prosecutions, conduct prosecution for a financial crime, a cybercrime or other complex, serious and organised crime, or for any other offence committed under this Act.~~

59. Prosecution

(1) No prosecution for a financial crime, cybercrime, other complex, serious and organised crime, or an offence under this Act shall be instituted, continued, discontinued or materially altered except by, or under the authority of, the Director of Public Prosecutions in accordance with the Constitution and any other applicable law.

(2) A prosecution may be conducted by the Director of Public Prosecutions, an officer acting under the Director's authority, or such barrister as the Director of Public Prosecutions may specifically instruct or authorise in writing for the case.

(3) A barrister employed by the NCA may conduct a prosecution only where –

(a) specifically designated in writing by the Director of Public Prosecutions;

(b) acting under the direction and control of the Director of Public Prosecutions for the purposes of that prosecution; and

(c) the barrister has not personally participated in investigative decisions in the case and no actual or apparent conflict of interest arises.

(4) Decisions whether to charge, amend or discontinue a charge, accept a plea, offer no evidence, appeal, or take any other material prosecutorial step remain decisions of the Director of Public Prosecutions or a person acting under the Director's lawful authority.

(5) Nothing in this section authorises the NCA to represent publicly that it has made the independent prosecutorial decision in a case.

Rationale

The circulated clause already reserves institution and consent to the DPP, but subsection (3) allows an NCA barrister to prosecute with approval. The amendment preserves the possibility of using specialist NCA counsel while placing that counsel expressly under DPP authority and separating investigation from prosecution where a conflict could arise.

Reference Notes — Clauses 47–59

Constitution of Mauritius: section 5 (personal liberty and safeguards on arrest/detention), section 9 (privacy of home and other property), and section 10 (protection of the law/fair-hearing guarantees).

Data Protection Act 2017: criminal-investigation exceptions remain subject to a necessity-and-proportionality standard in a democratic society, together with applicable security and accountability duties.

Convention on Cybercrime (Budapest Convention): Articles 15–21 provide the international framework for conditions and safeguards, expedited preservation, production orders, real-time traffic data and content interception. Mauritius deposited its instrument of accession on 15 November 2013; the Convention entered into force for Mauritius on 1 March 2014.