PUBLIC CONSULTATION

PROPOSED CYBERSECURITY BILL 2026

Introductory Statement and Matters for Stakeholder Comment

The Government of Papua New Guinea invites public authorities, operators of essential services and critical infrastructure, financial institutions, telecommunications and digital service providers, cybersecurity professionals, law enforcement agencies, civil society organisations, academic institutions, development partners and members of the public to comment on the proposed Cybersecurity Bill 2026.

The proposed Bill is intended to provide a comprehensive national framework for cybersecurity governance, protection of critical information infrastructure, cyber incident prevention and response, cybercrime investigation, online safety, and the regulation of cybersecurity services. It supports the objectives of the National Cyber Security Strategy 2024-2030 and responds to the policy positions set out in the drafting instructions for the proposed legislation.

This introductory statement identifies the principal matters on which feedback is sought. It should be read with the Draft of the Cybersecurity Bill 2026 and the relevant drafting instructions. Stakeholders are encouraged to address the practical effect of the proposed provisions, including their suitability for Papua New Guinea's legal, constitutional, institutional, economic, social and technical circumstances.

Purpose and policy setting

Papua New Guinea's National Cyber Security Strategy 2024-2030 sets a vision of a safe, resilient and secure cyberspace that enables innovation and economic prosperity, protects essential services and strengthens national sovereignty. The Strategy calls for coordinated legal, technical, organisational, capacity-building and cooperation measures, supported by a risk-based approach and clear responsibilities across government, industry, law enforcement and civil society.

The drafting instructions translate that policy direction into an evolutionary legislative framework. They propose that national capability should first be incubated within NICTA so that the new regulatory functions can draw on existing telecommunications expertise, technical resources, operational systems and industry relationships. The longer-term policy position is that the cybersecurity function should move to a separate national authority when the necessary operational capability, governance, funding and national-security arrangements are in place.

The proposed Bill also recognizes that not every system can be protected in the same manner. It adopts a risk-based approach under which systems and services that are essential to national

security, economic stability, public health, safety or continuity of government may be designated as critical information infrastructure and made subject to enhanced security, audit, incident-reporting and cooperation requirements.

The framework must support effective prevention, detection, response, investigation and prosecution while respecting constitutional rights, privacy, due process, judicial oversight and the distinct responsibilities of regulators, law enforcement agencies and national-security bodies. The consultation therefore seeks views not only on the powers proposed, but also on the safeguards, institutional boundaries and implementation arrangements required for their lawful and sustainable exercise.

Proposed legislative framework

The Draft provides for NICTA to Bill as the National Cybersecurity Authority and administer the proposed Bill until legislation establishes a separate Authority. It provides for a dedicated cybersecurity division, separate accounts and budget allocation for the new functions, Ministerial policy directions, annual reporting to Parliament and the eventual transfer of functions, assets, records, agreements, proceedings and staff arrangements to the separate Authority.

The proposed framework provides for a National Cybersecurity Strategy, a national coordination committee, a Cybersecurity Operations Centre and PNGCERT. It establishes a regime for designating and protecting critical information infrastructure, including security plans, minimum standards, risk assessment, audit, incident reporting and the continuing accountability of local operators where critical systems rely on cloud or third-party service providers.

Specific provisions address the protection of financial systems in coordination with the Bank of Papua New Guinea, including cybersecurity controls, incident response, electronic asset-freezing procedures and cooperation with financial intelligence and supervisory functions. Separate provisions address child online safety and social media regulation, including age restrictions, age-assurance measures, harmful-content reporting, takedown arrangements and platform accountability.

Cybercrime investigation functions are assigned to a specialised Unit within the Royal Papua New Guinea Constabulary rather than to the regulatory Authority. The proposed investigation and digital-evidence framework addresses search and seizure, preservation and production of data, interception subject to judicial authorisation, chain of custody, admissibility, forensic standards and cross-border cooperation.

The proposed Bill further imposes registration, local representation, data-preservation, reporting, cooperation and takedown duties on relevant platforms and ICT service providers. It provides mandatory incident reporting, information-sharing arrangements and time-limited emergency powers subject to Ministerial action and Parliamentary oversight. A licensing regime is proposed for providers of cybersecurity auditing, penetration testing, digital forensics and managed security services.

Implementation will require staged commencement, regulations, standards, codes, forms, inter-agency arrangements, public awareness and sustained technical capacity. The Draft also contemplates consequential amendments and continuing coordination with existing laws, including the Cybercrime Code Bill 2016, the Evidence Bill 1975, the NICTA Act, financial-sector legislation and the proposed Data Governance and Data Protection Bill 2026.

Matters for stakeholder feedback

Stakeholders are invited to comment on the following matters and to identify provisions that are unclear, disproportionate, impracticable, inconsistent with existing law or likely to create unintended consequences.

1. Scope and application

Does the proposed Bill clearly identify the persons, systems, services, conduct and entities to which it applies? Feedback is sought on its territorial and extraterritorial reach; application to public bodies, private operators, foreign platforms and offshore service providers; the treatment of cloud and third-party environments; and whether any exclusions, exemptions or thresholds are necessary and sufficiently confined.

Stakeholders should also consider whether the definitions of cybersecurity incident, platform, ICT service provider, cybersecurity service, critical information infrastructure and related terms are sufficiently precise for enforcement and future technological change.

2. Institutional governance and accountability

Are the proposed functions of the Minister, NICTA as the interim Authority, the Authority's Board and Chief Executive Officer, the national coordination committee, PNGCERT, the Cybersecurity Operations Centre, the Child Online Safety Commissioner and the Royal Papua New Guinea Constabulary clearly separated and capable of effective coordination?

Comment is sought on regulatory independence, Ministerial direction, Parliamentary reporting, funding, separate accounts and staffing, information sharing, conflicts of function, protection of confidential information and the mechanisms required to coordinate cybersecurity regulation with national security, policing, digital government, data protection, telecommunications, competition, financial regulation and censorship functions.

3. Critical information infrastructure

Does the proposed designation process appropriately identify systems, networks, facilities and services whose disruption would materially affect national security, the economy, public health, safety, essential services or continuity of government? Should initial designations be confined to government and core financial infrastructure, or extend at commencement to major telecommunications, energy, transport, health and other private-sector operators?

Are the proposed duties relating to security plans, minimum controls, audits, risk assessments, incident reporting, exercises, access to information and compliance directions proportionate and workable? Views are invited on supply-chain and cloud risks, accountability for outsourced systems, confidentiality of designation and security information, sector-regulator coordination, review rights and the time required for operators to reach compliance.

4. Protection of financial systems

Do the proposed protections for banks, insurers, savings and loan societies, micro-finance institutions, payment providers, mobile-money services and other regulated financial institutions align with the supervisory responsibilities of the Bank of Papua New Guinea and existing financial-crime frameworks?

Feedback is sought on mandatory controls, reporting to both the Authority and the Bank, incident-response planning, electronic asset-freezing orders, recovery of cybercrime proceeds, information sharing and the risk of overlapping or inconsistent directions from different regulators.

5. Child online safety and platform obligations

Are the proposed protections for children clear, effective and proportionate, including the restriction on social media accounts for children under 16, the obligations placed on platforms, age-assurance requirements, limits on profiling and behavioural advertising, harmful-content reporting and removal notices?

Stakeholders should address privacy-preserving and accessible methods of age assurance; protection and deletion of age-verification data; appropriate exceptions for educational, health and other beneficial services; procedural fairness for takedown decisions; platform registration and local representation; feasibility for services operated outside Papua New Guinea; and coordination with child-protection, censorship, criminal law and data-protection requirements.

6. Cybercrime investigation powers and digital evidence

Do the proposed arrangements appropriately vest cybercrime investigation functions in the Cybercrime Investigation Unit of the Royal Papua New Guinea Constabulary while keeping the Authority's regulatory and incident-response functions distinct? Is the proposed provincial presence achievable, and what resourcing, training, accreditation and forensic capability will be required?

Comment is sought on warrants, search and seizure of devices and data, preservation and production orders, interception, urgent action, access to encrypted information, extraterritorial investigations, chain of custody, admissibility and expert evidence. Are the thresholds, judicial controls, privilege protections, reporting obligations and remedies sufficient to protect constitutional rights and ensure that digital evidence is reliable and usable in court?

7. Incident reporting and emergency powers

Are the proposed incident-reporting thresholds and timeframes workable, including the 24-hour notification and subsequent full-report requirements for critical infrastructure and relevant entities? Feedback is sought on reportable events, reporting channels, confidentiality, legal privilege, use and sharing of reported information, duplication with personal-data breach notification and sector-specific reporting, and protection for organisations that report in good faith.

Are the grounds for declaring a cybersecurity emergency and the scope of emergency directions sufficiently clear, necessary and proportionate? Stakeholders should consider the approval process, maximum duration, Parliamentary oversight, judicial review, compensation or cost allocation, protection of essential services and safeguards governing any direction to isolate, suspend, access or take control of systems.

8. Licensing of cybersecurity services

Should licensing apply to all cybersecurity auditing, penetration testing, digital forensics and managed security services, or initially be limited to the most sensitive services identified in the drafting instructions, particularly penetration testing and managed security operations? Are the proposed eligibility, competence, character, security, record-keeping, renewal, suspension and appeal requirements proportionate to the risks?

Stakeholders are invited to address transitional recognition of existing providers, treatment of overseas specialists, individual and corporate licensing, professional standards, conflicts of interest, confidentiality, procurement implications, licence duration, fees and the risk that regulation may unintentionally restrict access to scarce expertise.

9. Implementation and legislative coherence

What commencement periods, transitional arrangements, regulations, standards, codes, guidance and capacity-development measures are required for credible implementation? Comment is sought on the proposed timing for establishment of functions, designation of critical infrastructure, platform compliance, provincial investigation capability, service-provider licensing, national exercises, public awareness and independent review of the Act.

Does the proposed Bill interact coherently with the Constitution, the Cybercrime Code Bill 2016, the Evidence Bill 1975, the NICTA Act, financial-sector and anti-money-laundering laws, child-protection and censorship laws, electronic-transactions legislation and the proposed Data Governance and Data Protection Bill 2026? Stakeholders should identify duplication, inconsistent definitions, conflicting powers, gaps, consequential amendments or sequencing issues that should be resolved before enactment.

Central governance question

A principal matter for consultation is the institutional mechanism through which the proposed legislation should initially be administered and how the national cybersecurity function should evolve as capability matures.

The drafting instructions propose an incubation model. NICTA would initially perform the role of National Cybersecurity Authority, allowing the new function to use existing regulatory systems, telecommunications expertise, technical resources and industry relationships. The Draft gives effect to that immediate position by providing that NICTA administers the Bill until separate legislation establishes a standalone National Cybersecurity Authority.

The longer-term policy position is that the national cybersecurity function should transition out of NICTA once the necessary operational milestones, governance, leadership, funding, systems and national-security coordination arrangements are in place. The drafting instructions contemplate an eventual standalone body integrated with the national-security framework, while the Draft leaves the timing and detailed constitution of that body to a future Bill of Parliament.

CONSULTATION QUESTION

Does the proposed phased governance model, under which NICTA initially acts as the National Cybersecurity Authority before functions transfer to a separately established Authority, provide an appropriate, independent, and sustainable mechanism for national cybersecurity governance in Papua New Guinea?

In responding, stakeholders are asked to consider whether NICTA should perform the functions at commencement or whether a standalone Authority should be established immediately; which functions should be incubated within NICTA; and which investigative, intelligence, policy or operational functions should remain with other institutions.

Views are also sought on the legal and operational safeguards required during the interim period, including separate budgeting, accounts, records, staffing, decision-making and reporting; the independence of regulatory and enforcement decisions; accountability to the Minister, Parliament and the public; and the treatment of complaints or investigations involving government agencies or NICTA-regulated entities.

Stakeholders should comment on the transition trigger. Should transition occur after a fixed period, such as the 36-48 month incubation period contemplated in the drafting policy, after independently assessed operational milestones are achieved, following a National Executive Council decision, or through a combination of those mechanisms? What minimum conditions should be met before functions, PNGCERT, assets, records, staff, agreements, rights and liabilities transfer?

Comment is further invited on the relationship of the future Authority with the National Security Council and national coordination arrangements; the continued role of DICT in policy; the independence of the Royal Papua New Guinea Constabulary's Cybercrime Investigation Unit; sector-regulator participation; and the expertise, appointment process and accountability expected of the future Authority's governing body and leadership.

Form of submissions

Submissions should identify the provision or subject addressed, state the stakeholder's position and, where possible, explain the likely legal, operational, financial, technical or social effect of the proposal. Alternative wording, implementation options, cost information, sector evidence and relevant international experience are welcome. Stakeholders should clearly identify any information they consider confidential and provide reasons for that request.

The consultation is intended to test both the substance of the proposed legal framework and the governance arrangements required to administer it. Feedback will inform further refinement so that the legislation strengthens national cyber resilience, protects critical services and citizens, supports effective investigation and incident response, and remains practical for government, industry and communities across Papua New Guinea.

Policy and drafting basis

This notice has been prepared principally with reference to the drafting instructions and policy framework for the proposed Cybersecurity Bill 2026. The Draft has been used to identify the proposed legal structure and mechanisms, and the Papua New Guinea National Cyber Security Strategy 2024-2030 has been used as supporting policy context.

Submissions and Enquiries

A joint Technical Working Group has been established by the Department of Information and Communications Technology (DICT) and the National Information and Communications Technology Authority (NICTA) to assess, review and develop the policies, strategies, legislation and regulatory instruments required to support the broader ICT sector reform programme.

The current legislative review and drafting process is being coordinated through the Technical Working Group. Government agencies, industry participants, civil society organisations, professional bodies, academic institutions and members of the public are invited to provide written comments, submissions and recommendations on the proposed legislative framework.

Submissions should clearly identify the relevant provision, issue or policy area being addressed and, where possible, include the reasons for the proposed position and any recommended alternative wording or implementation approach.

All submissions, enquiries and requests for clarification should be directed through the following channels:

ICT Legislative Review Submission Portal

Website: https://ict.gov.pg/ict-legislation-consultation

Or Email Submissions and Enquiries
Email: ictsector_reset@nicta.gov.pg

NICTA Contact
Ms Lillian Smith
Manager, Research and Emerging Technology
Email: lsmith@nicta.gov.pg

Department of ICT Contact
Mr Thomson Simon
Manager, Policy Development
Email: thomson.simon@ict.gov.pg

Mr Pokana Nouari
Manager, Policy Planning and Implementation
Email: pokana.nouari@ict.gov.pg

Submissions should include the name of the individual or organisation making the submission, relevant contact details and an indication of whether the submission may be published or referenced as part of the consultation process.

Unless confidentiality is specifically requested and accepted, submissions may be treated as public consultation material and may be summarised, published, or referred to in the final consultation report.

Closing Date for Submissions: *19th August 2026*
Reference: Draft Cybersecurity Bill 2026 Consultation