DEPARTMENT OF INFORMATION & COMMUNICATIONS TECHNOLOGY

PUBLIC CONSULTATION PAPER

Verifiable Credentials and Trust Services Bill 2026

Invitation to Make Submissions

Submissions close: *19th August 2026*

Submit to: thomson.simon@ict.gov.pg or pokana.nouari@ict.gov.pg

HOW TO READ THIS PAPER

This Consultation Paper accompanies the Verifiable Credential and Trust Services Bill 2026 (the Bill) and the Explanatory Notes prepared by the Papua New Guinea Department of Information and Communications Technology. It is intended to help individuals, organisations, and institutions provide focused, useful feedback on the specific policy choices embedded in the Bill.

The Paper follows the structure of the Bill Part by Part. Each section opens with a summary of what that Part does and why it matters, followed by targeted questions on the issues where public feedback will genuinely inform the final legislation.

You do not need to answer every question. You are encouraged to respond only to the questions that are relevant to your experience, sector, or expertise. A focused submission on two or three questions is more useful than a general response that covers everything briefly.

Who should respond?

This consultation is open to all interested persons and organisations. The following groups are particularly encouraged to engage:

- Individual residents and civil society organisations especially on holder rights (Part VI), privacy (Part VII), and the non-exclusion guarantee (Part I, clause 3(3));
- Private sector entities especially on mandatory acceptance timelines (Part II, clause 23), accreditation requirements (Part V), the fee and sustainability framework (Part II, clause 26), and the commercial services provisions;
- Financial institutions and payment service providers on eKYC and AML/CTF interface issues (Part II, clauses 23 and 30) and the Digital Identity Sustainability Fund;
- Government agencies and public bodies on mandatory acceptance timelines and operational readiness (Part II, clause 23), interoperability with existing systems, and consequential amendments (Schedule 1);
- Legal practitioners and academics on constitutional safeguards (Part I), the liability allocation framework (Part VIII, clause 73), appeals (Part VIII, clause 75), and the interaction with the Data Governance and Data Protection Act 2026;
- Technology and cybersecurity experts on the technical architecture, credential schemas (Part II, clause 19), approved digital wallet standards (Part II, clause 14), data residency requirements (Part II, clause 25), and cryptographic key management; and
- Bilateral and development partners and multilateral organisations on the Framework's alignment with international standards, cross-border interoperability (Part II, clause 24), and its fit with regional Digital Public Infrastructure initiatives.

How to make a submission

Format: Submissions may be made in writing by email or through the online submission portal at [URL TO BE CONFIRMED]

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

There is no required format. You may respond to specific questions, make general comments, or both.

Deadline: 19th August 2026. Late submissions may be accepted at the Department's discretion.

Reference: Draft Cybersecurity Bill 2026 Consultation

Contact (for queries about the consultation process)**:**

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

Publication: Submissions will be published on the Department's website (www.ict.gov.pg) unless you request confidentiality. Please clearly mark any parts of your submission you wish to be treated as confidential and explain why.

Reference documents: The Bill and Explanatory Notes are available at www.ict.gov.pg. It is recommended that you read the Explanatory Notes for the relevant Part before responding to the questions in this Paper.

PART I — PRELIMINARY (Clauses 1–6)

Background

Part I sets out the objects of the Bill, the constitutional and rights safeguards, the key definitions, and the Bill's relationship with other laws. The most consequential policy choices in this Part are the objects clause (which will guide interpretation of the entire Act), the constitutional non-exclusion guarantee (no person denied essential services for lack of SevisPass), and the boundaries between this Act and existing legislation such as the Citizenship Act 1975, the Passports Act 1982, and the Civil and Identity Registration Act 2024.

Objects and scope (clause 2)

Question 1: Do the objects in clause 2 accurately reflect what PNG needs from a national digital identity and verifiable credentials system?

(a) Are there objectives that are missing — for example, relating to financial inclusion, digital commerce, or international competitiveness?

(b) Are any of the stated objects unclear or potentially in tension with each other?

(c) How should conflicts between the objects be resolved if they arise in practice?

Particularly relevant to: All stakeholders

Non-exclusion guarantee (clause 3(3))

Clause 3(3) provides that no person shall be denied access to an "essential government service" solely because they do not hold SevisPass.
"Essential government service" is defined to mean a public service prescribed by regulation or declared by the Minister after consultation, covering basic public administration, civil status, health, education, social protection, emergency services or justice.
The definition is open-ended: the list of essential services will ultimately be settled by regulation and Ministerial declaration.

Question 2: Is the non-exclusion guarantee in clause 3(3) strong enough to protect people who cannot or do not wish to enrol in SevisPass?

(a) Should the guarantee be strengthened — for example, by specifying a minimum list of essential services on the face of the Act rather than leaving it entirely to regulation and Ministerial declaration?

(b) Should the guarantee extend beyond government services to privately-provided services of a public nature, such as banking, telecommunications, or utilities?

(c) How should the guarantee be enforced in practice, and who should a person complain to if they are refused a service?

Particularly relevant to: Civil society, disability advocates, human rights organisations, legal practitioners, development partners

Definitions (clause 4)

Question 3: Are the key definitions in clause 4 clear, appropriately scoped, and technology-neutral?

(a) Is the definition of "verifiable credential" sufficiently clear to include the range of credentials PNG intends to issue under the Act, while excluding credentials outside its scope?

(b) Is the definition of "essential government service" appropriately scoped, or is it too broad or too narrow?

(c) Are there any defined terms that are unclear, missing, or that could be interpreted in unintended ways?

Particularly relevant to: Legal practitioners, technology experts, government agencies

Relationship with other laws (clause 6)

Question 4: Does clause 6 adequately manage the interface between this Bill and existing legislation?

(a) Are there specific Acts not listed in clause 6(2) that could create uncertainty or conflict with the Bill's operation?

(b) Clause 6(3) preserves existing requirements for physical document production unless those laws are amended. Is this the right default position, or should the Bill take a more active approach to enabling digital substitution?

(c) Are there sectors or transaction types where the interaction between this Act and existing law is unclear and needs further guidance?

Particularly relevant to: Government agencies, legal practitioners, financial institutions, private sector

PART II — NATIONAL DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS SYSTEM (Clauses 7–26)

Background

Part II is the operational core of the Bill. It establishes SevisPass and SevisWallet; creates the verifiable credentials ecosystem; provides for the legal recognition, presentation, and verification of digital credentials; and sets out the sovereignty, data residency, and sustainability framework. The policy choices in this Part will have the most direct impact on individuals, businesses, and government agencies.

SevisPass design: one credential for life and biometric anchoring (clauses 7–12)

> SevisPass is a randomly generated 12-digit non-intelligent identifier, issued once for life, to which a holder's primary biometric is anchored for deduplication. It explicitly does not constitute proof of citizenship or nationality.
> Re-issuance, replacement, restoration, and updates do not create a new identity record except for fraud control, deduplication, or system rectification purposes.
> SevisPass can be issued to a child with demographic-only enrolment until the prescribed age for biometric collection is reached.

Question 5: Is "one SevisPass for life" the right design principle for PNG's national digital identity system?

(a) What safeguards should exist for individuals whose SevisPass record contains errors that cannot easily be corrected, particularly in remote or low-connectivity areas?

(b) How should the system handle persons who were registered under pilot programmes before this Act commences? Is the transitional validation provision in clause 79 sufficient?

Question 6: Are the protections against mission creep sufficient — specifically, the provisions preventing SevisPass from being used as proof of citizenship, nationality, or immigration status (clause 8(2))?

(a) Are there specific use cases you are aware of where this boundary might be blurred in practice?

(b) What additional safeguards, if any, should be included to prevent SevisPass from being used in ways that go beyond its intended purpose?

Question 7: Are the provisions for issuing SevisPass to children (clause 11(2)) appropriate?

(a) At what age should biometric collection begin, and should this be specified in the Act rather than left to regulation?

(b) What safeguards should apply to children's biometric and credential data that go beyond the general protections in Part VII?

(c) How should consent for a child's SevisPass enrolment work, and what happens if a child's guardian refuses to consent on the child's behalf?

Particularly relevant to: Civil society, child rights organisations, disability advocates, legal practitioners, development partners

Digital wallets: SevisWallet and approved private wallets (clauses 13–14)

SevisWallet is designated as PNG's official national digital wallet. Additional private wallets may be approved by the Regulator subject to standards compliance, interoperability with SevisWallet and SevisDEx, support for selective disclosure, and security requirements.
The Bill explicitly states that approved private wallets must not undermine SevisWallet's status as the official State-designated national wallet.

Question 8: Is the dual-wallet model (SevisWallet as official national wallet, with additional approved private wallets) the right approach for PNG?

(a) What criteria should the Regulator use when assessing private wallet applications, particularly for security, resilience, and holder rights protection?

(b) How should the Regulator ensure that private wallets genuinely compete on quality and do not disadvantage holders who use them compared to SevisWallet?

(c) Should there be a cap on the number of approved private wallets, or should the market remain open to any entity meeting the standards?

Particularly relevant to: Technology sector, financial institutions, civil society, development partners

Prescribed credential categories and legal recognition (clauses 16–22)

The Bill lists 13 categories of prescribed credentials (e.g. driver's licences, passports, birth certificates, Grade 12 certificates, TIN certificates, police clearances, superannuation credentials). Additional categories may be prescribed by regulation.
A verifiable credential issued under the Act has legal recognition equivalent to the underlying physical document. Verifiers cannot unreasonably refuse to accept a digital credential in lieu of the physical document, subject to three exceptions.
Verifiers are subject to data minimisation obligations: they can only request the minimum attributes necessary for the stated lawful purpose.

Question 9: Is the list of prescribed credential categories in clause 16 appropriate?

(a) Are there credential categories that are missing and should be included?

(b) Are there categories listed that create practical difficulties — for example, because the enabling law for that credential has not been updated to support digital issuance?

(c) Should the Act specify a process or timeline for adding new credential categories, rather than leaving this entirely to regulation?

Question 10: Will the legal recognition provisions in clause 20 be effective in driving acceptance of verifiable credentials across PNG's public and private sectors?

(a) What are the main practical barriers to acceptance of digital credentials that the legal recognition provisions may not fully address?

(b) Are the three exceptions to the anti-refusal obligation (clause 20(3)) appropriately defined, or are they too broad and likely to be used to avoid acceptance?

(c) Should the Act include a dispute resolution mechanism for individuals who are refused a digital credential where no valid exception applies?

Question 11: Are the data minimisation and purpose limitation obligations on verifiers (clause 21) workable in practice?

(a) How should the Regulator monitor and enforce compliance with these obligations, particularly for smaller or lower-capacity verifiers?

(b) Should there be sector-specific guidance on what constitutes "minimum attributes" for common verification use cases (e.g. age verification, employment verification, financial due diligence)?

Question 12: Are the natural justice protections for suspension and revocation of credentials (clause 22) adequate?

(a) The Bill permits emergency temporary suspension without prior notice for fraud prevention, public safety, cybersecurity, or system integrity reasons. Is this exception too broad? What additional safeguards should apply in emergency suspension cases?

(b) How quickly should reasons for emergency suspension be provided to the affected holder?

(c) Should holders have an automatic right to seek an urgent stay of suspension pending review?

Particularly relevant to: All stakeholders — civil society and legal practitioners on Q7–9; private sector and government agencies on Q6 and Q8

Mandatory acceptance timelines (clause 23)

The Bill requires:
• Public bodies: accept SevisPass within 12 months of commencement of the relevant provision.
• Financial institutions, superannuation funds, payment service providers: accept SevisPass for eKYC within 18 months.
• Telecommunications, education, transport, professional bodies, utilities: accept SevisPass within 24–36 months.
Sectoral regulators may issue implementing instructions but cannot narrow the substantive acceptance obligation.

Question 13: Are the mandatory acceptance timelines in clause 23 realistic given the current state of digital infrastructure and systems readiness in PNG?

(a) For public bodies: is 12 months achievable? What are the main barriers to compliance, and what government support would be needed?

(b) For financial institutions and payment service providers: is 18 months achievable given AML/CTF system integration requirements? Should different timelines apply to different sizes or types of financial institutions?

(c) For telecommunications, education, and other sectors: is the 24–36 month range appropriate, and how should the Regulator sequence compliance obligations within that range?

(d) Should there be a formal mechanism for entities to apply for an extension where compliance by the prescribed date is genuinely not feasible?

Question 14: Should the mandatory acceptance obligation for financial institutions include specific guidance on the interface between SevisPass-based eKYC and existing AML/CTF customer due diligence obligations?

(a) The Bill (clause 30) makes clear that SevisPass is not a substitute for financial institution customer risk ratings, transaction monitoring, or sanctions screening. Is this boundary sufficiently clear in the Bill?

(b) What guidance should the Regulator issue on how SevisPass verification interacts with Know Your Customer (KYC) requirements under the Anti-Money Laundering and Counter Terrorist Financing Act 2015?

Particularly relevant to: Government agencies, financial institutions, superannuation funds, telecommunications operators, educational institutions, development partners

Cross-border recognition and foreign participation restrictions (clauses 24, 24A)

The Minister may approve cross-border recognition arrangements for SevisPass with other jurisdictions, subject to the Regulator's advice and preservation of PNG's sovereign control.
Clause 24A prohibits foreign State-linked entities from being designated as the Implementation Authority. Ownership changes resulting in a foreign person or entity holding 15% or more beneficial interest require prior Ministerial approval.

Question 15: With which jurisdictions should PNG prioritise cross-border recognition arrangements, and on what terms?

(a) What safeguards beyond those in clause 24(2) should apply to cross-border data flows when PNG credentials are verified in partner jurisdictions?

(b) Should the Act specify that cross-border arrangements require Parliamentary approval or tabling, rather than being made entirely by Ministerial decision?

(c) How should the Regulator assess whether a partner jurisdiction provides equivalent privacy, security, and rights protections before approving a cross-border arrangement?

Question 16: Is the 15% foreign beneficial interest threshold in clause 24A the right trigger for Ministerial approval of changes in control of the Implementation Authority?

(a) Should the threshold be lower, given the sensitive sovereign nature of digital identity infrastructure?

(b) How should "foreign State-linked entity" be defined and monitored in practice, particularly for entities with complex ownership structures?

Particularly relevant to: Development partners, bilateral partners, legal practitioners, financial institutions, technology sector

State sovereignty and data residency (clause 25)

Clause 25 establishes that the State retains sovereign ownership and ultimate control over SevisPass, SevisWallet, SevisDEx, the Trust Registry, public cryptographic trust anchors, and designated credential schemas.
All personal data, biometric data, credential data, and audit logs must be stored on infrastructure physically located in PNG. Biometric raw data and root cryptographic key material may never be stored or processed offshore. Limited offshore processing of other data is permitted only with Ministerial gazette approval, encryption, jurisdictional protection, and contractual prohibition on foreign government disclosure.
The Implementation Authority must maintain a cryptographic key escrow arrangement, with key material independently verified by the Regulator at 12-month intervals.

Question 17: Are the data residency requirements in clause 25 workable given the current state of ICT infrastructure in PNG?

(a) Is the prohibition on offshore storage of biometric raw data and root cryptographic key material appropriate, or does it create operational challenges that should be addressed?

(b) The conditions for permitting offshore processing of non-biometric data require Ministerial gazette approval, encryption, and contractual prohibition on foreign government disclosure. Are these conditions adequate, or should additional safeguards apply?

(c) What should the Regulator's standards require for physically secure in-country data storage facilities, particularly for cryptographic key material and biometric data?

Question 18: Are the step-in rights and procedures in clauses 24B and 37 proportionate and practically workable?

(a) Is a 12-month cap on the duration of a step-in period appropriate?

(b) Should there be independent oversight of the exercise of step-in rights — for example, requiring National Court approval within a specified period?

(c) Is the compensation framework for the Implementation Authority during a step-in period (no compensation for lost revenue; reimbursement of documented direct costs only) fair and appropriate?

Particularly relevant to: Technology experts, cybersecurity specialists, development partners, government agencies, legal practitioners

Sustainability framework and the Digital Identity Sustainability Fund (clause 26)

> The Digital Identity Sustainability Fund receives fees, levies, commercial revenues, appropriations, and grants. It is managed by the Regulator in trust for the State.
> Basic SevisPass functions are free for all residents. Fees may be charged to institutional and commercial participants.
> The Implementation Authority may offer commercial services on a fee-for-service basis, including enhanced identity assurance, identity-as-a-service, bulk verification services, and consent-governed data-sharing.

Question 19: Is the Digital Identity Sustainability Fund model the right approach to financing the long-term operation of the National Digital Trust Ecosystem?

(a) Should the Fund be managed by the Regulator, or by an independent body? What oversight mechanisms are needed to ensure the Fund is used appropriately?

(b) How should the fee structure be designed to ensure institutional and commercial participants bear a fair share of costs without stifling adoption and innovation?

(c) Are the restrictions on use of the Fund (clause 26(5C)) appropriate, or are there other legitimate uses that should be permitted?

Question 20: Should the Implementation Authority be permitted to offer commercial services (clause 26(6)), and if so, under what conditions?

(a) Does allowing the Implementation Authority to offer commercial services create a conflict of interest with its role as the neutral utility operator of the ecosystem?

(b) How should the Regulator ensure that commercial service revenues do not cross-subsidise the Implementation Authority's core public infrastructure functions, or vice versa?

(c) Should there be an independent review mechanism for the pricing of commercial services to prevent abuse of the Implementation Authority's dominant position?

Particularly relevant to: Private sector, financial institutions, development partners, government agencies, civil society

PART III — REGULATOR (Clauses 27–32)

Background

Part III designates the entity responsible for regulating ICT and the digital economy as the Regulator — currently NICTA. The Regulator's functions span accreditation, standards-setting, supervision, enforcement, and maintenance of the Trust Registry. A Technical Standards and Advisory Committee is required. The Regulator must submit an annual report to Parliament.

Independence, identity, and capacity of the Regulator (clause 27)

> Unless another entity is designated under the National Information and Communications Technology Act 2009, NICTA is the Regulator.
> The Regulator is described in the Explanatory Notes as an "independent statutory regulator", but the Bill designates the existing ICT regulator rather than creating a new regulatory body.

Question 21: Is NICTA the right entity to be the Regulator for digital identity and verifiable credentials, or should a new or different body be established?

(a) Does NICTA have, or can it credibly build, the technical, legal, and operational capacity needed to discharge the Regulator's functions under this Act?

(b) Is there a real or perceived conflict of interest between NICTA's existing ICT regulatory functions and its proposed role as the digital identity Regulator?

(c) If a separate regulatory body is established in the future, what criteria should govern the transition?

Question 22: Are the Regulator's functions and powers in clauses 28 and 29 appropriate and sufficient?

(a) Are there functions that the Regulator should have that are not listed in clause 28?

(b) The Regulator may apply to the National Court for an injunction (clause 29). Should it also have emergency powers — for example, to issue interim stop orders without Court approval in urgent cybersecurity situations?

(c) How should the Regulator coordinate with BPNG, the data protection regulator, and sectoral regulators to avoid regulatory gaps or overlaps?

Particularly relevant to: Government agencies, legal practitioners, private sector, development partners

Technical Standards and Advisory Committee (clause 31)

Question 23: How should the Technical Standards and Advisory Committee be composed, and what should its mandate be?

(a) What specific technical expertise should be required for Committee membership?

(b) Should the Committee's decisions or recommendations be binding on the Regulator, or advisory only?

(c) Should civil society and credential holders be represented on the Committee, in addition to government, private sector, and technical experts?

(d) Should the Committee's proceedings and recommendations be published as a matter of course?

Particularly relevant to: Technology experts, civil society, private sector, development partners

PART IV — IMPLEMENTATION AUTHORITY (Clauses 33–38)

Background

Part IV establishes the framework for designating an Implementation Authority — a separate entity from the Regulator that will design, deploy, operate, and maintain the core operational components of the National Digital Trust Ecosystem. The Implementation Authority is subject to strict sovereignty, governance, and accountability requirements. The State retains step-in rights, and the designation may be revoked. The Minister has 12 months after commencement of Part IV to designate an Implementation Authority.

Design and designation of the Implementation Authority (clauses 33–35)

The Implementation Authority is designated by Ministerial notice in the National Gazette, unless the NEC otherwise directs.
A Special Purpose Vehicle (SPV) established or designated for the limited purpose of implementing the ecosystem may be designated.
The Implementation Authority must have technical, operational, and financial capacity; must be able to maintain continuity, resilience, and cybersecurity; must have a governance structure with a golden share or equivalent mechanism preserving State control; and must operate with the neutrality required of a public utility.

Question 24: Is the Special Purpose Vehicle model the right institutional design for the Implementation Authority?

(a) What should the ownership structure of the SPV be — wholly State-owned, a public-private partnership, or another model? What are the implications of each approach for accountability, sustainability, and innovation?

(b) How should the SPV be incorporated and governed to ensure it operates with genuine commercial discipline while meeting its public interest obligations?

(c) Should the criteria for designation be more prescriptive on the face of the Act, rather than left to regulation and the designation instrument?

Question 25: How should the tension between the Implementation Authority's role as a neutral public utility and its authorisation to offer commercial services (clause 26(6)) be managed?

(a) What ring-fencing arrangements between the core utility functions and commercial services are needed beyond those in clause 36?

(b) Should there be an independent audit of the Implementation Authority's cost allocation between its public infrastructure functions and its commercial activities?

(c) Who should have standing to complain if the Implementation Authority is perceived to be favouring its own commercial services over accredited private sector participants?

Particularly relevant to: Private sector, development partners, government agencies, legal practitioners, financial institutions

Governance requirements and golden share (clause 36)

The Bill requires the Implementation Authority's governance to include: prescribed board representation; annual reporting; risk management protocols aligned with national security and cybersecurity policies; procurement and contracting requirements that preserve State ownership of sovereign infrastructure; ring-fencing of sovereign trust infrastructure in accounts and asset register; a golden share or equivalent mechanism preserving State control; and non-discriminatory access to core services.
All contracts involving sovereign trust infrastructure must contain a termination-for-convenience clause exercisable by the Implementation Authority on written Ministerial direction, without liability to the vendor beyond reasonable notice and direct costs.

Question 26: Are the governance requirements in clause 36 sufficient to ensure the Implementation Authority operates transparently, accountably, and in the public interest?

(a) Should the board of the Implementation Authority include civil society representation, credential holder representation, or independent directors in addition to public-sector and prescribed stakeholder representatives?

(b) Should the Implementation Authority's annual report be tabled in Parliament, not just published?

(c) Is the golden share mechanism the right instrument for preserving State control, or should other instruments — such as regulatory veto rights or a State seat on the board — be used instead or in addition?

Particularly relevant to: Development partners, legal practitioners, private sector, government agencies

PART V — ACCREDITED PARTNERS (Clauses 39–44)

Background

Part V creates the accreditation framework for private sector and other non-public-body participants in the ecosystem. Seven categories of accredited partner are recognised. No entity may operate in a regulated capacity without accreditation. Accredited partners are subject to ongoing obligations covering compliance, privacy, cybersecurity, audit logging, and notification of material incidents.

Question 27: Is the accreditation framework in Part V workable for the types of entities that will want to participate in the National Digital Trust Ecosystem?

(a) Are the seven categories of accredited partner (clause 39) comprehensive, or are there participation roles missing that should be recognised?

(b) What should the accreditation requirements include for each category — for example, what minimum capital, technical capability, or governance standards should apply to accredited issuers, digital wallet providers, and trust service providers?

(c) Should there be a public register of accredited partners and their accreditation status, accessible to credential holders and verifiers?

Question 28: Are the ongoing obligations on accredited partners (clause 43) appropriate and proportionate?

(a) The Bill requires notification to the Regulator of material incidents, breaches, or changes of control "within the prescribed time". What notification timeframes are appropriate for different types of incidents (e.g. data breach vs change of control vs system outage)?

(b) How should the Regulator handle situations where an accredited partner is acquired by or merges with a foreign entity? Should automatic notification to the Regulator trigger a mandatory review?

(c) Are there additional obligations — for example, mandatory cybersecurity audits, penetration testing, or incident response plan approval — that should apply to accredited partners operating in high-risk categories?

Particularly relevant to: Private sector, technology companies, financial institutions, legal practitioners

PART VI — RIGHTS OF CREDENTIAL HOLDERS (Clauses 45–56)

Background

Part VI is the Bill's bill of rights for credential holders. It establishes twelve distinct rights: to enrol, to access records, to correct data, to consent-based sharing, to revoke consent, to notification of access and verification events, to disclosure history, to deletion from a wallet, to portability, to continuity, to redress, and special provisions for vulnerable persons. These rights come into force on the date of certification — before the operational Parts of the Bill — to give holders immediate legal protection.

Question 29: Are the twelve rights in Part VI comprehensive, or are there important rights that are missing?

(a) Should holders have a right to know which verifiers have requested or received access to their credentials, including where the holder has not actively consented (for example, in law enforcement access situations)?

(b) Should holders have a right to object to automated decision-making based on their credential data — for example, where an algorithm uses credential attributes to make a credit or employment decision?

(c) Should the right to deletion from a wallet (clause 52) be extended to a right to request erasure of credential data from an issuer's records, subject to lawful retention obligations?

Question 30: Are the rights in Part VI practically enforceable for holders, particularly those in remote areas, those with low digital literacy, or those in vulnerable circumstances?

(a) What channels should be available for holders to exercise their rights — for example, should offline or in-person channels be mandatory alongside digital channels?

(b) What remedies should be available to a holder whose rights are breached — for example, should compensation be available, not just corrective action?

(c) Should the Regulator be required to publish an annual report specifically on holder rights complaints and outcomes?

Question 31: Are the special provisions for vulnerable persons (clause 56) adequate?

(a) The Bill requires "reasonable accommodations" for persons with disabilities, elderly persons, children, persons in remote areas, and other vulnerable persons. Should the Act be more prescriptive about what accommodations are required?

(b) How should compliance with the vulnerable persons provision be monitored and enforced?

(c) Should there be a dedicated ombudsperson or advocate for credential holders, particularly for vulnerable persons?

Particularly relevant to: Civil society, disability advocates, human rights organisations, development partners, legal practitioners

PART VII — DATA PROTECTION AND PRIVACY (Clauses 57–59)

Background

Part VII contains three provisions on data protection and privacy. All entities must implement privacy by design. All approved digital wallets must support selective disclosure. The Part also governs the relationship between this Act and the Data Governance and Data Protection Act 2026 (DGDPA), which applies concurrently to all personal data processed within the ecosystem. The Regulator and the data protection regulator are required to cooperate and coordinate.

Question 32: Is the relationship between this Bill and the Data Governance and Data Protection Act 2026 sufficiently clear?

(a) Are there areas where the concurrent application of both Acts could create uncertainty, conflicts, or compliance difficulties for entities operating in the ecosystem?

(b) Should this Act or the DGDPA be amended to create a single, clear hierarchy of obligations where both apply?

(c) How should the Regulator and the data protection regulator coordinate in practice — should a formal memorandum of understanding be required, and should its terms be made public?

Question 33: Is the privacy by design obligation (clause 57) specific enough to be meaningfully enforceable?

(a) What specific privacy by design requirements should the Regulator prescribe — for example, data minimisation at system design stage, privacy impact assessments, or encryption standards?

(b) Should the Bill require all ecosystem participants to publish privacy impact assessments before deploying new credential systems or services?

(c) How should the Regulator assess and verify compliance with privacy by design across accredited partners and the Implementation Authority?

Question 34: Is selective disclosure (clause 58) adequately operationalised in the Bill?

(a) Should the Bill specify minimum technical standards for selective disclosure — for example, requiring support for zero-knowledge proofs for specified high-sensitivity attributes?

(b) In what verification contexts should selective disclosure be mandatory rather than optional?

(c) How should the Regulator handle situations where a verifier requests more attributes than are necessary and the wallet provider does not support selective disclosure for that attribute set?

Particularly relevant to: Civil society, legal practitioners, technology experts, development partners, government agencies

PART VIII — ENFORCEMENT, OFFENCES AND APPEALS (Clauses 60–75)

Background

Part VIII creates the enforcement architecture: audits and inspections, compliance directions, information-gathering powers, administrative penalties, and injunctions. It creates seven criminal offences ranging from fraudulent enrolment to unlawful refusal to accept credentials. It allocates liability among participants. It provides for internal Regulator review and appeal to the National Court within 30 days.

Offences and penalties (clauses 65–72)

> Penalty amounts are still to be finalised following advice from the State Solicitor and the Department of Justice and Attorney-General. Indicative ranges are noted in square brackets in the Bill.
> Seven offences are created: fraudulent enrolment or use; unlawful collection or use of biometric data; unauthorised access to SevisDEx, the Trust Registry, or related systems; operating without accreditation; failure to comply with a Regulator direction; failure to notify a notifiable data breach; and contravention of consent requirements.
> Unlawful refusal to accept prescribed credentials is a regulatory contravention (not a criminal offence) dealt with by compliance direction, administrative penalty, or suspension.

Question 35: Are the seven offences in Part VIII the right offences to criminalise, and are they appropriately defined?

(a) Are there serious contraventions currently treated only as regulatory matters that should be criminal offences?

(b) The Bill criminalises "unlawful collection or use of biometric data" (clause 66). Is the boundary between lawful and unlawful collection sufficiently clear, particularly for entities that collect biometric data under their own enabling legislation?

(c) Should there be a specific offence of using credential data to discriminate against a holder — for example, using credential data to deny employment, housing, or services on an unlawful basis?

Question 36: Are the indicative penalty ranges in the Bill appropriate and proportionate?

(a) Do the indicative ranges for individuals (PGK 5,000–100,000 fines; imprisonment) and bodies corporate (PGK 50,000–500,000 fines) reflect the seriousness of the relevant offences in the PNG context?

(b) Should penalties scale with the size of the offending entity — for example, should the maximum fine for a large financial institution be a percentage of annual revenue rather than a fixed amount?

(c) Should the court have discretion to order additional remedies beyond fines and imprisonment — for example, disgorgement of profits from unlawful use of credential data, or mandatory public reporting of a conviction?

Particularly relevant to: Legal practitioners, civil society, government agencies, financial institutions

Liability allocation (clause 73)

Question 37: Is the allocation of liability in clause 73 clear, fair, and workable across all ecosystem participants?

(a) Clause 73(5) protects holders from liability for system errors, issuer errors, verifier misuse, or operator failures. Are there circumstances where a holder should bear some responsibility — beyond fraud, impersonation, or deliberate misrepresentation — for example, failure to report loss of access to their wallet?

(b) Should there be a compensation scheme for holders who suffer loss as a result of issuer errors, system failures, or verifier misuse — particularly where the responsible party is insolvent or has left the ecosystem?

(c) How should liability be allocated where a harm arises from the interaction of failures by multiple ecosystem participants — for example, an issuer error combined with a wallet provider security failure?

Particularly relevant to: Legal practitioners, civil society, private sector, government agencies

Appeals (clause 75)

Question 38: Is the 30-day window for appeals to the National Court in clause 75 appropriate?

(a) For decisions to suspend a credential — which directly affect a holder's access to services — should there be a shorter internal review timeframe before the holder is required to go to the National Court?

(b) Should the Bill establish a specialist Digital Identity Review Tribunal as an intermediate appellate body below the National Court, to provide cheaper and faster dispute resolution?

(c) Should the commencement of an appeal automatically stay a credential suspension, rather than requiring the holder to separately apply for a stay?

Particularly relevant to: Legal practitioners, civil society, development partners

PART IX — MISCELLANEOUS, TRANSITIONAL AND SAVINGS (Clauses 76–87)

Background

Part IX contains the regulation-making power, the NEC oversight requirement for regulations, transitional provisions validating existing pilots and arrangements, savings provisions preserving the operation of the Citizenship Act, Passports Act, AML/CTF Act, and constitutional oversight bodies, a privacy savings provision, and a mandatory post-legislative review within 3 years of full commencement.

Question 39: Is the regulation-making power in clauses 76–78 appropriately scoped, with adequate Parliamentary and public oversight?

(a) A significant volume of operational detail will be prescribed by regulation, including accreditation criteria, fee schedules, data retention periods, and credential schemas. Is this the right approach, or should more matters be settled on the face of the Act?

(b) Should regulations made under this Act be subject to a disallowance process in Parliament, rather than simply NEC approval?

(c) Should there be a requirement to publicly consult before making regulations under this Act on matters that affect holder rights, fees, or accreditation requirements?

Question 40: Is the transitional validation provision in clause 79 sufficient to give legal certainty to activities that have already occurred under existing pilots?

(a) Should the validation provision be time-limited, and what criteria should apply before a pilot arrangement is validated?

(b) Are there specific pilot programmes or provisional issuances that need to be addressed on the face of the Act to give legal certainty, rather than being left to regulations or ministerial notices?

Question 41: Is the mandatory post-legislative review in clause 87 adequate to ensure ongoing accountability and policy responsiveness?

(a) Should the review be conducted by an independent external body rather than being commissioned by the Minister?

(b) The review report must be tabled in Parliament within 6 months of completion. Should Parliament have the power to debate and respond to the report within a specified timeframe?

(c) Are there specific metrics or benchmarks — for example, enrolment rates, service acceptance rates, privacy complaint rates — that should be built into the Act and measured as part of the review?

Particularly relevant to: Legal practitioners, civil society, development partners, government agencies

SCHEDULES

Schedule 1 — Consequential Amendments

Schedule 1 provides for amendments to the National Information and Communication Technology Act 2009, the Digital Government Act 2022, the Civil and Identity Registration Act 2024, and a range of other Acts (including the AML/CTF Act, Road Traffic Act, and migration legislation) to enable the digital issuance, recognition, and presentation of prescribed credentials.

Question 42: Are the consequential amendments in Schedule 1 comprehensive enough to give full legal effect to the Act, or are there additional Acts that need to be amended?

(a) Are there Acts governing specific credential categories (e.g. professional licences, superannuation credentials, education certificates) that are not covered by Schedule 1 and will need to be amended before those credentials can be issued digitally?

(b) How should the consequential amendments be sequenced to avoid gaps in legal authority — for example, should the enabling Act for a credential category be amended before that credential can be prescribed under this Act?

(c) Are there any consequential amendments proposed in Schedule 1 that raise concerns — for example, in terms of their impact on existing regulatory frameworks or individual rights?

Particularly relevant to: Government agencies, legal practitioners, private sector

Schedule 2 — Foundational Principles

Schedule 2 sets out twelve foundational principles that guide the interpretation and administration of the Act and all instruments made under it: legality and constitutional compliance; user-centric design and enforceable holder rights; privacy by design and data minimisation; purpose limitation and lawful consent; security, resilience and cybersecurity by design; interoperability and open standards; selective disclosure and proportionality; inclusion, accessibility and accommodation for vulnerable persons; State sovereignty and control; accountability, transparency and auditability; continuity of service and portability; and phased, practical and sector-sensitive implementation.

Question 43: Are the twelve foundational principles in Schedule 2 the right principles for guiding the administration of PNG's National Digital Trust Ecosystem?

(a) Are there principles missing from Schedule 2 that should be included — for example, an explicit principle of environmental sustainability, or a principle of interoperability with Pacific regional digital infrastructure?

(b) Schedule 2 is expressed as an interpretive guide rather than a source of enforceable obligations. Should some principles — for example, the inclusion and accessibility principle — be given direct legal force in the Act rather than operating only as interpretive guidance?

(c) How should conflicts between principles be resolved — for example, where maximising State sovereignty over infrastructure conflicts with achieving open standards and interoperability?

Particularly relevant to: All stakeholders

GENERAL QUESTIONS

The following questions invite broader feedback not specific to a particular Part of the Bill.

Question 44: Does the Bill as a whole strike the right balance between enabling digital identity and protecting individual rights?

(a) Are there provisions in the Bill that give you particular confidence that rights will be protected?

(b) Are there provisions that you believe could be used in ways that harm individuals — particularly vulnerable groups — even if that is not the intent?

(c) What additional safeguards, review mechanisms, or oversight bodies would give you greater confidence in the Bill's rights protections?

Question 45: How well does the Bill align with international standards and regional Digital Public Infrastructure frameworks?

(a) Is the Bill consistent with the UNCITRAL Model Law on Electronic Transferable Records, the W3C Verifiable Credentials Data Model, and other relevant international standards?

(b) How does the Bill compare with digital identity legislation in comparable Pacific Island nations, and what lessons from those experiences should inform the final Bill?

(c) Is the Bill structured in a way that will enable PNG to participate in APEC and Pacific regional digital identity interoperability frameworks?

Question 46: Are there any aspects of the Bill that are unclear, unnecessarily complex, or difficult to implement in the PNG context that should be simplified or restructured?

Question 47: Is there anything else you wish to bring to the Department's attention that is not addressed by the questions above?

Particularly relevant to: All stakeholders

QUICK REFERENCE: ALL QUESTIONS

For convenience, all questions in this Paper are listed below with their question numbers and the relevant Part of the Bill.

Question	Part	Subject
Q1	Part I	Do the objects in clause 2 accurately reflect what PNG needs?
Q2	Part I	Is the non-exclusion guarantee strong enough?
Q3	Part I	Are the key definitions clear, appropriately scoped, and technology-neutral?
Q4	Part I	Does clause 6 adequately manage the interface with existing legislation?
Q5	Part II	Is "one SevisPass for life" the right design principle?
Q6	Part II	Are protections against mission creep sufficient (clause 8(2))?
Q7	Part II	Are provisions for SevisPass issuance to children appropriate?
Q8	Part II	Is the dual-wallet model the right approach?
Q9	Part II	Is the list of prescribed credential categories appropriate?
Q10	Part II	Will legal recognition provisions be effective in driving acceptance?
Q11	Part II	Are data minimisation obligations on verifiers workable in practice?
Q12	Part II	Are natural justice protections for suspension and revocation adequate?
Q13	Part II	Are mandatory acceptance timelines realistic?
Q14	Part II	Should mandatory acceptance include AML/CTF interface guidance?
Q15	Part II	Which jurisdictions should PNG prioritise for cross-border recognition?
Q16	Part II	Is the 15% foreign beneficial interest threshold appropriate?
Q17	Part II	Are data residency requirements workable?
Q18	Part II	Are step-in rights provisions proportionate and workable?
Q19	Part II	Is the Digital Identity Sustainability Fund model right?
Q20	Part II	Should the Implementation Authority offer commercial services?
Q21	Part III	Is NICTA the right Regulator, or should a new body be established?
Q22	Part III	Are the Regulator's functions and powers appropriate and sufficient?
Q23	Part III	How should the Technical Standards and Advisory Committee be composed?
Q24	Part IV	Is the SPV model the right institutional design for the Implementation Authority?
Q25	Part IV	How should the tension between utility and commercial roles be managed?
Q26	Part IV	Are governance requirements in clause 36 sufficient?
Q27	Part V	Is the accreditation framework workable for ecosystem participants?
Q28	Part V	Are ongoing obligations on accredited partners appropriate and proportionate?
Q29	Part VI	Are the twelve holder rights comprehensive, or are rights missing?
Q30	Part VI	Are rights practically enforceable for all holders?
Q31	Part VI	Are special provisions for vulnerable persons adequate?
Q32	Part VII	Is the relationship between the Bill and the DGDPA sufficiently clear?
Q33	Part VII	Is the privacy by design obligation specific enough to be enforceable?
Q34	Part VII	Is selective disclosure adequately operationalised?
Q35	Part VIII	Are the seven offences the right offences to criminalise?
Q36	Part VIII	Are the indicative penalty ranges appropriate and proportionate?
Q37	Part VIII	Is the liability allocation in clause 73 clear, fair, and workable?
Q38	Part VIII	Is the 30-day appeal window appropriate?

Question	Part	Subject
Q39	Part IX	Is the regulation-making power appropriately scoped, with adequate oversight?
Q40	Part IX	Is the transitional validation provision sufficient?
Q41	Part IX	Is the mandatory post-legislative review adequate?
Q42	Sched 1	Are the consequential amendments comprehensive enough?
Q43	Sched 2	Are the twelve foundational principles the right principles?
Q44	General	Does the Bill strike the right balance between enabling digital ID and protecting rights?
Q45	General	How well does the Bill align with international standards and regional DPI frameworks?
Q46	General	Are there aspects that are unclear, unnecessarily complex, or difficult to implement?
Q47	General	Is there anything else the Department should know?

NOTE: These questions are not exhaustive. If there are issues in the Bill that are important to you but not covered by a question here, please raise them in your submission. The Department will consider all substantive feedback received during the consultation period.

(end of document)