PAPUA NEW GUINEA

NICTA

SIM REGISTRATION REGULATION (AMENDMENT AND CONSOLIDATION) 2026 CONSULTATION

RESPONSE TO COMMENTS REPORT

03-18-26

1. Introduction

The National Information and Communications Technology Authority (NICTA), pursuant to its mandate under the National Information and Communications Technology Act 2009, undertook a public consultation on the proposed **SIM Registration Regulation (Amendment and Consolidation)** to review and update the existing SIM Registration Regulation 2016.

The consultation was conducted from **23 December 2025 to 31 January 2026** and was subsequently **extended from 1 February to 28 February 2026** to allow additional time for stakeholder submissions. The review aims to strengthen the regulatory framework governing SIM registration and enhance subscriber identity verification within Papua New Guinea's telecommunications sector.

Stakeholders, including mobile network operators, government agencies, and other interested parties, were invited to provide feedback on the proposed amendments, which focus on improving SIM registration procedures, strengthening privacy and data protection safeguards, enhancing regulatory oversight, and reducing fraud and misuse of telecommunications services.

This **Response to Stakeholder Comments Report** summarizes the feedback received and outlines NICTA's responses to the issues raised, which have informed the finalization of the amended SIM Registration Regulation.

Contents

2. Stakeholder Submissions Received

NICTA received submissions from the following stakeholders:

- Digicel PNG
- Vodafone PNG
- Telikom PNG
- Independent Consumer and Competition Commission (ICCC)
- Papua New Guinea National Research Institute (PNGNRI)
- National Intelligence Office (NIO)
- Department of Foreign Affairs (DFA)
- Bank South Pacific (BSP) to be submitted

These submissions provided perspectives on regulatory design, operational challenges, consumer protection considerations, and broader governance issues relating to SIM registration practices.

3. Responses to Consultation Questions

Part A: Compulsory Questions

Question 1. Do you support the proposed update and consolidation of the SIM Registration Regulation?

Stakeholder Comments

Stakeholders generally expressed support for the proposed review and consolidation of the SIM Registration Regulation.

Digicel PNG supported the review, noting that the existing regulation should be updated to reflect current operational and technological developments within the telecommunications sector. The company also noted that improved identity verification mechanisms could enhance customer identification processes, although it raised concerns regarding certain amendments proposed in the draft regulation.

Vodafone PNG also supported the proposed review but emphasized the importance of carefully managing implementation timelines and addressing potential cost implications for mobile network operators.

The Independent Consumer and Competition Commission (ICCC) supported the update and consolidation of the regulation, noting that effective SIM registration frameworks are an important component of national digital infrastructure. The Commission highlighted that stronger registration systems could improve regulatory compliance, strengthen national security, and support the development of Papua New Guinea's digital economy.

The Papua New Guinea National Research Institute (PNGNRI) supported the proposed update and emphasized that clear and consistent regulatory rules are essential to maintaining trust in mobile services. PNGNRI also noted that SIM cards increasingly support essential services including mobile banking, e-government services, and emergency communications.

The National Intelligence Office (NIO) supported the consolidation of the regulation, noting that the reform could address weaknesses in the existing framework, including manual identity verification processes and weaknesses in subscriber database integrity.

The Department of Foreign Affairs (DFA) also supported the reform and highlighted the importance of maintaining strong governance arrangements in regulatory frameworks affecting telecommunications services.

NICTA Response

NICTA notes the broad support expressed by stakeholders for the review and consolidation of the SIM Registration Regulation.

NICTA agrees that the updated framework should reflect current technological developments and strengthen mechanisms to ensure accurate subscriber registration and improved regulatory oversight.

NICTA also acknowledges stakeholder comments regarding implementation challenges and operational costs. These considerations will be taken into account during the implementation phase to ensure the revised regulatory framework is practical, effective, and proportionate.

Question 2. Should Digital ID be mandatory for all new SIM Registrations?

Stakeholder Comments

Stakeholders expressed differing views on whether Digital ID systems should be made mandatory for SIM registration.

Digicel PNG did not support making the Digital ID system mandatory at this stage, arguing that the system should first be fully developed, implemented, and widely adopted before being introduced as a mandatory identification mechanism.

Vodafone PNG acknowledged that Digital ID systems could strengthen Know Your Customer (KYC) processes and assist in addressing fraud risks. However, Vodafone highlighted several practical challenges in Papua New Guinea, including low internet penetration, limited digital literacy, and gaps in civil registration coverage. Vodafone also noted that mandatory Digital ID requirements could impose additional operational and financial costs on telecommunications operators.

ICCC supported the integration of Digital ID systems into SIM registration, noting that digital identity platforms could strengthen identity verification processes and enhance data protection safeguards.

PNGNRI indicated conditional support for mandatory Digital ID requirements, provided that the system remains simple, accessible, and clearly communicated to the public, including through local languages.

The **National Intelligence Office** supported mandatory Digital ID requirements, noting that stronger identity verification mechanisms could reduce fraudulent or duplicate SIM registrations and assist law enforcement investigations.

NICTA Response

NICTA acknowledges the views expressed by stakeholders regarding the potential use of Digital ID systems for SIM registration.

Given that the national Digital ID framework is still under development, NICTA considers it premature to mandate its use as a compulsory requirement for SIM registration at this stage.

Accordingly, the revised regulation will not require mandatory Digital ID verification during the initial implementation phase. NICTA will continue to monitor developments in national identity infrastructure and may review this position in the future as relevant systems become operational and widely adopted.

Question 3. Should existing SIMs be re-verified using Digital ID?

Stakeholder Comments

Stakeholders generally supported the concept of re-verifying existing SIM registrations but emphasized that the process should be carefully managed to avoid service disruptions and ensure accessibility for all users.

Digicel PNG expressed general support for re-verification but noted that such measures should only be implemented once the necessary systems and operational processes are fully developed and integrated into operators' registration systems. Digicel also suggested that re-verification should be conducted progressively and may be triggered when customers update their subscriber information or request additional services.

Vodafone PNG supported the re-verification of existing SIM cards but recommended that the process be implemented gradually. Vodafone proposed a minimum transition period of up to **36 months** to allow operators sufficient time to update systems, conduct

nationwide verification campaigns, and ensure that subscribers are not unfairly disconnected.

The **Independent Consumer and Competition Commission** supported mandatory re-verification of existing SIM registrations, noting that regular verification helps ensure that mobile numbers remain linked to legitimate subscribers and reduces the risk of misuse for unlawful activities. ICCC also highlighted the importance of strong public awareness campaigns to ensure users understand the process.

The **Papua New Guinea National Research Institute** supported re-verification but emphasized that the process should be phased and clearly communicated to the public. PNGNRI cautioned that abrupt deactivation of SIM cards could disrupt livelihoods, financial services, and emergency communication, particularly for vulnerable populations.

The **National Intelligence Office** supported a nationwide re-verification exercise to address legacy SIM registrations that may contain inaccurate or incomplete information. The agency noted that a structured re-verification program could improve the reliability of subscriber data used in investigations.

The **Department of Foreign Affairs** did not provide specific comments on re-verification requirements but emphasized the importance of maintaining effective and accessible regulatory processes.

NICTA Response

NICTA notes the general support expressed by stakeholders for the re-verification of existing SIM registrations.

The NICTA recognizes that maintaining accurate subscriber information is critical for strengthening regulatory oversight and addressing the misuse of telecommunications services. However, NICTA also acknowledges stakeholder concerns regarding potential service disruption and operational challenges.

Accordingly, any future re-verification exercise will be implemented in a **phased and carefully managed manner**, supported by appropriate public awareness initiatives and reasonable transition periods to allow subscribers and operators to comply with the requirements.

Question 4. Should Biometric verification be required?

Stakeholder Comments

Stakeholders expressed mixed views on whether biometric verification should be required as part of the SIM registration process.

Digicel PNG did not support mandatory biometric verification, noting that while biometrics may strengthen identity verification, mandatory collection could raise privacy concerns and increase operational costs for telecommunications operators. Digicel also noted that deploying biometric devices to all customer-facing agents could create significant logistical and financial challenges.

Vodafone PNG also cautioned against mandatory biometric verification. The company noted that some individuals may experience difficulty providing biometric data due to physical conditions, occupational factors such as worn fingerprints, or other limitations. Vodafone emphasized the need for alternative verification methods to ensure that users are not excluded from telecommunications services.

The **Independent Consumer and Competition Commission** acknowledged that biometric verification could strengthen identity verification mechanisms but emphasized that its use must be balanced with appropriate privacy safeguards and measures to prevent digital exclusion.

The **Papua New Guinea National Research Institute** recommended that biometric verification be applied selectively rather than universally. PNGNRI suggested that biometrics could be used for higher-risk transactions such as SIM replacement or account changes.

The **National Intelligence Office** supported the use of biometric verification as a means of strengthening identity assurance but emphasized that biometric data should be managed through appropriate governance frameworks and safeguards.

The **Department of Foreign Affairs** did not provide specific comments on biometric verification but emphasized the importance of strong personal data protection safeguards.

NICTA Response

NICTA acknowledges the views expressed by stakeholders regarding the potential use of biometric verification for SIM registration.

While biometric technologies may strengthen identity verification mechanisms, NICTA recognizes the concerns raised regarding privacy protection, operational feasibility, and potential barriers to access.

Accordingly, the revised regulation will **not mandate biometric verification for SIM registration** at this stage. Telecommunications operators may continue to use existing identification and verification processes that comply with regulatory requirements.

NICTA will continue to monitor developments in identity verification technologies and may review the potential role of biometric verification in future regulatory reviews.

Question 5. What Privacy Safeguards should be included?

Stakeholder Comments

Stakeholders emphasized the importance of strong privacy safeguards to protect subscriber information collected during SIM registration processes.

Digicel PNG recommended that clear safeguards be established to ensure that personal data collected during SIM registration is used only for legitimate regulatory purposes. Digicel also suggested the establishment of independent oversight mechanisms and enforceable audit controls to prevent misuse of personal data.

Vodafone PNG emphasized the importance of ensuring that personal data collected during subscriber registration is handled in accordance with recognized data protection principles. Vodafone noted that access to subscriber information should be restricted to authorized personnel and that appropriate data protection controls should be implemented.

ICCC recommended implementing strong security protections for subscriber information, including secure data handling processes and clear safeguards against unauthorized access.

PNGNRI highlighted the importance of limiting data collection to information necessary for SIM registration and ensuring that subscribers have the ability to review and correct inaccurate personal information.

NIO emphasized the importance of strong safeguards to protect sensitive subscriber information while ensuring that lawful access processes remain available for legitimate investigations.

The **Department of Foreign Affairs** highlighted the need for clear governance arrangements to ensure that personal information collected through SIM registration is appropriately protected.

NICTA Response

NICTA acknowledges the importance of maintaining strong privacy protections for subscriber information collected during SIM registration.

NICTA agrees that appropriate safeguards must be in place to ensure that subscriber data is securely stored, accessed only by authorized parties, and used solely for legitimate regulatory and operational purposes.

The revised regulation maintains existing data protection obligations and reinforces the requirement for telecommunications operators to implement appropriate security measures to protect subscriber information.

Question 6. Are the Proposed Rural or Offline Verification Methods Sufficient?

Stakeholder Comments

Stakeholders emphasized the importance of ensuring that SIM registration processes remain accessible to users in rural and remote communities.

Digicel PNG noted that reliance on technology-driven verification processes may create challenges for rural populations who may have limited access to connectivity, identification documentation, or registration facilities. Digicel highlighted that existing provisions within the current SIM Registration Regulation allow individuals without formal identification documents to be registered through verification by a reputable person. The company recommended that such provisions be maintained in the revised regulation to ensure continued access to telecommunications services in rural areas.

Vodafone PNG indicated that the consultation paper did not provide sufficient details regarding the proposed rural or offline verification mechanisms. Vodafone therefore recommended that additional information be provided on how these systems would operate in practice before operators can fully assess their feasibility.

ICCC indicated that the proposed provisions appear sufficient and did not provide further comments on rural verification mechanisms.

PNGNRI supported the introduction of rural and offline verification mechanisms but emphasized that implementation should be supported by mobile registration teams and community outreach initiatives to ensure accessibility in remote communities.

The **National Intelligence Office** supported the direction of the proposed rural verification approach but recommended that implementation plans include clear targets for rural coverage and deployment schedules.

The **Department of Foreign Affairs** emphasized that implementation of the SIM registration framework should ensure that vulnerable groups and individuals in remote areas are not excluded from accessing telecommunications services.

NICTA Response

NICTA acknowledges the concerns raised by stakeholders regarding the need to maintain accessibility for users in rural and remote communities.

NICTA agrees that SIM registration procedures must remain inclusive and practical for all users across Papua New Guinea. Accordingly, the revised regulation will maintain flexible verification provisions to support individuals who may not possess formal identification documents, while ensuring that appropriate safeguards remain in place to protect the integrity of subscriber registration processes.

NICTA also recognizes the importance of effective implementation strategies and will work with industry stakeholders to ensure that SIM registration mechanisms remain accessible to users in rural and underserved areas.

Question 7. What Additional Measures Should Support Rural or Marginalized Groups?

Stakeholder Comments

Stakeholders emphasized the importance of ensuring that regulatory reforms do not unintentionally exclude vulnerable populations from accessing telecommunications services.

Digicel PNG noted that barriers such as limited access to connectivity, lack of digital literacy, and absence of formal identity documentation may create challenges for marginalized groups. The company emphasized that regulatory frameworks should remain inclusive and ensure that vulnerable communities are not disadvantaged.

Vodafone PNG also emphasized the importance of maintaining accessible verification processes that take into account the infrastructure limitations faced by rural communities.

ICCC recommended additional measures to improve access in rural areas, including the use of mobile registration units and community-based registration initiatives.

PNGNRI suggested bringing registration services closer to communities through local outreach programs and community registration drives. PNGNRI also recommended that implementation be managed carefully to avoid service disruptions for rural users.

The **National Intelligence Office** recommended implementing targeted outreach initiatives and public awareness campaigns to ensure that communities across the country understand SIM registration requirements.

The **Department of Foreign Affairs** emphasized that implementation strategies should consider the needs of vulnerable populations and individuals living in remote areas.

NICTA Response

NICTA acknowledges the importance of ensuring that SIM registration requirements remain accessible and inclusive for all users.

NICTA agrees that appropriate implementation measures should be adopted to support rural and marginalized communities. These may include community outreach initiatives, public awareness campaigns, and practical registration mechanisms designed to accommodate users in remote areas.

NICTA will continue to work with stakeholders to ensure that SIM registration processes remain accessible while maintaining appropriate safeguards to ensure the integrity of subscriber information.

Question 8. Should the Regulation Mandate Minimum Cybersecurity Standards?

Stakeholder Comments

Stakeholders broadly supported the inclusion of cybersecurity safeguards to protect subscriber data collected during SIM registration.

Digicel PNG supported the need for clear cybersecurity standards but suggested that such requirements should be addressed through broader cybersecurity frameworks rather than being prescribed directly within the SIM Registration Regulation.

Vodafone PNG supported the implementation of strong cybersecurity controls and recommended independent security assessments to ensure that systems handling subscriber data remain secure and resilient.

ICCC supported the inclusion of minimum cybersecurity standards to safeguard subscriber information and maintain trust in telecommunications systems.

PNGNRI emphasized the importance of data protection measures such as encryption, controlled access to subscriber databases, and secure authentication mechanisms.

The **National Intelligence Office** strongly supported mandatory cybersecurity safeguards, including robust authentication systems, secure system interfaces, and monitoring mechanisms to detect potential security incidents.

The **Department of Foreign Affairs** emphasized the importance of strong governance arrangements to ensure secure management of telecommunications data.

NICTA Response

NICTA acknowledges the importance of strong cybersecurity safeguards to protect subscriber information.

NICTA agrees that telecommunications operators must implement appropriate security measures to safeguard subscriber data and ensure the integrity of registration systems. Existing regulatory obligations already require operators to implement appropriate information security controls when handling subscriber information.

NICTA will continue to monitor developments in cybersecurity practices and may review additional regulatory measures where necessary to ensure the continued protection of subscriber information.

Question 9. What Should be the Minimum Data Retention and Breach Reporting Requirements?

Stakeholder Comments

Stakeholders expressed differing views regarding appropriate data retention periods and breach reporting requirements.

Digicel PNG indicated that the existing requirement to retain subscriber records for six months after SIM deactivation remains appropriate. The company also suggested that broader breach reporting requirements should be addressed through comprehensive privacy or data protection legislation rather than through SIM registration regulations alone.

Vodafone PNG recommended a longer retention period of up to seven years, noting that extended retention may assist regulatory compliance, investigations, and operational record keeping.

ICCC recommended retaining subscriber identification data for the duration that a SIM card remains active and for a period of five years after deactivation. ICCC also recommended prompt reporting of any cybersecurity incidents affecting subscriber information.

PNGNRI emphasized that data retention requirements should remain proportionate and limited to what is necessary for regulatory and legal purposes.

NIO recommended maintaining appropriate retention periods to support lawful investigations while ensuring that data protection safeguards remain in place.

The **Department of Foreign Affairs** emphasized the importance of clear protocols for information sharing and data protection.

NICTA Response

NICTA acknowledges the range of views expressed by stakeholders regarding appropriate data retention requirements.

NICTA considers the current data retention provisions within the existing regulatory framework to be appropriate and proportionate. These requirements support regulatory oversight and assist legitimate investigations while maintaining safeguards for subscriber privacy.

NICTA will continue to monitor developments in data protection frameworks and may review these requirements as necessary in future regulatory reviews.

Question 10. Should SIM Registration Agents be Licensed and Certified?

Stakeholder Comments

Stakeholders expressed differing views on whether SIM registration agents should be licensed or formally certified.

Digicel PNG did not support licensing or certification requirements for agents, arguing that mobile network operators are already responsible for ensuring that their agents comply with regulatory obligations.

Vodafone PNG also opposed licensing requirements, noting that operators already maintain oversight of their agents through internal compliance processes.

ICCC supported the licensing or certification of SIM registration agents, stating that such measures could strengthen accountability and oversight while reducing the risk of fraudulent registrations.

PNGNRI also supported certification requirements for agents, emphasizing that this could improve consumer protection and provide clearer accountability mechanisms.

The **NIO** supported licensing and certification requirements, recommending additional measures such as training requirements and stronger monitoring of agent activities.

The **Department of Foreign Affairs** did not provide specific comments on agent licensing but emphasized the importance of clear governance arrangements.

NICTA Response

NICTA acknowledges the differing views expressed by stakeholders regarding the licensing of SIM registration agents.

The Authority notes that under the existing regulatory framework, licensed telecommunications operators remain responsible for the actions of their agents and are required to ensure that SIM registration processes comply with regulatory requirements.

Accordingly, the revised regulation will maintain the existing approach under which operators retain responsibility for the conduct and oversight of their agents. Operators will be expected to implement appropriate internal controls, training, and monitoring mechanisms to ensure compliance with SIM registration requirements.

Question 11. How can NICTA prevent or control agent fraud?

Stakeholder Comments

Stakeholders emphasized the need for effective mechanisms to prevent fraudulent SIM registrations conducted through agents.

Digicel PNG noted that the most effective approach would be to maintain the existing principle that telecommunications operators are responsible for the conduct of their agents. The company stated that operators already have strong incentives to implement internal controls, including agent training and monitoring mechanisms.

Vodafone PNG also emphasized the importance of system-based controls rather than extensive regulatory intervention. Vodafone suggested that operators should implement internal fraud detection systems, transaction monitoring, and operational controls to identify suspicious registration activities.

ICCC recommended introducing stronger traceability mechanisms for agents, including assigning unique identification numbers to registration agents and implementing systems that reduce manual data entry during SIM registration processes.

PNGNRI recommended additional measures such as agent certification, GPS tracking of registration devices, random audits, and stronger enforcement measures to discourage fraudulent activities.

The **NIO** recommended enhanced monitoring mechanisms, including device controls, audit trails, and system-based safeguards that detect unusual registration patterns or excessive SIM activations.

The **Department of Foreign Affairs** emphasized the importance of coordination between regulatory authorities, law enforcement agencies, and other relevant institutions to ensure effective enforcement of SIM registration requirements.

NICTA Response

NICTA acknowledges the concerns raised regarding the potential for fraudulent SIM registrations conducted through agents.

The Authority considers it appropriate to maintain the current regulatory principle under which licensed telecommunications operators remain responsible for the conduct of their agents. Operators are therefore expected to implement appropriate compliance mechanisms, including agent training, monitoring systems, and internal audits.

NICTA will continue to exercise regulatory oversight through compliance monitoring and enforcement mechanisms where necessary. NICTA also encourages operators to strengthen internal fraud detection systems to ensure the integrity of SIM registration processes.

Question 12. Are the Roles and Obligations of MNO's clear and achievable?

Stakeholder Comments

Stakeholders provided differing views regarding the clarity and feasibility of the proposed roles and obligations for mobile network operators.

Digicel PNG indicated that some aspects of the proposed framework require further clarification, particularly regarding the division of responsibilities between government institutions and telecommunications operators. The company emphasized that operators should primarily be responsible for verifying subscriber identities rather than performing broader identity registration functions.

Vodafone PNG also noted that certain provisions may require further clarification, particularly regarding implementation responsibilities and cost recovery mechanisms associated with regulatory compliance.

ICCC considered the proposed roles and obligations to be clear and achievable within the current regulatory framework.

PNGNRI indicated that the proposed roles are generally clear but emphasized that operators must maintain strong safeguards to ensure the accuracy and protection of subscriber information.

The National Intelligence Office indicated that the proposed obligations are generally appropriate but recommended additional mechanisms to detect duplicate registrations across multiple networks.

The Department of Foreign Affairs emphasized the importance of maintaining clear governance arrangements between regulatory authorities and telecommunications operators.

NICTA Response

NICTA notes the comments provided by stakeholders regarding the clarity of roles and responsibilities under the proposed regulatory framework.

NICTA considers that the revised regulation clearly establishes the obligations of telecommunications operators with respect to subscriber registration, data accuracy, and regulatory compliance.

NICTA acknowledges the need for continued engagement with operators to address implementation questions and ensure that regulatory requirements remain practical and achievable.

Question 13. What challenges do MNOs foresee in meeting these requirements?

Stakeholder Comments

Stakeholders highlighted several potential challenges associated with implementing the revised regulatory requirements.

Digicel PNG noted that the full scope of technical and operational challenges cannot be fully assessed until detailed technical specifications and implementation guidelines are available.

Vodafone PNG highlighted potential challenges related to system integration, implementation costs, and the operational demands associated with large-scale registration exercises.

ICCC noted that logistical challenges may arise when implementing registration processes in rural and remote areas.

PNGNRI acknowledged that operators may face operational and technical challenges but emphasized that implementation measures should ensure continued accessibility for users across the country.

The **NIO** highlighted additional challenges related to system integration, agent training, and infrastructure limitations in remote areas.

The **Department of Foreign Affairs** emphasized the importance of ensuring that regulatory reforms are implemented in a coordinated manner that aligns with broader governance frameworks.

NICTA Response

NICTA acknowledges that telecommunications operators may face operational and technical challenges in implementing the revised regulatory requirements.

NICTA will continue to engage with industry stakeholders during the implementation phase to ensure that regulatory obligations are clearly communicated and practical implementation timelines are established.

NICTA remains committed to working collaboratively with operators to ensure that the revised regulatory framework is implemented effectively while maintaining service accessibility for users across PNG.

Question 14. Should the Rollout be Phased or Immediate?

Stakeholder Comments

Stakeholders broadly supported a phased implementation approach.

Digicel PNG recommended a phased rollout to allow operators adequate time to prepare operational systems and procedures.

Vodafone PNG also supported phased implementation, noting that immediate compliance timelines could create significant operational and financial pressures for operators.

ICCC supported phased implementation to allow adequate preparation and system readiness across the telecommunications sector.

PNGNRI recommended a gradual implementation approach supported by public awareness initiatives and system testing.

The **National Intelligence Office** supported phased implementation beginning with new SIM registrations followed by a staged process for addressing existing registrations.

The **Department of Foreign Affairs** emphasized that phased implementation would help ensure inclusive and coordinated implementation.

NICTA Response

NICTA acknowledges the broad support expressed by stakeholders for a phased implementation approach.

NICTA agrees that a phased rollout will allow sufficient time for telecommunications operators to prepare systems and operational processes while minimizing disruption to subscribers.

Accordingly, the revised regulatory framework will be implemented in a phased manner, supported by appropriate implementation guidelines and stakeholder engagement.

Question 15. What is a Realistic Implementation Timeline?

Stakeholder Comments

Stakeholders expressed differing views regarding the appropriate timeline for implementing the revised regulatory framework.

Digicel PNG did not propose a specific timeline but emphasized that implementation should occur only once relevant systems and operational frameworks are fully established.

Vodafone PNG proposed a multi-phase implementation timeline spanning several years, including preparation, system integration, and nationwide implementation stages.

ICCC did not provide a specific timeline but supported allowing sufficient time for industry preparation.

PNGNRI recommended a gradual implementation period supported by strong public awareness initiatives.

The **NIO** suggested a staged timeline beginning with regulatory finalization followed by system preparation and nationwide implementation.

The **Department of Foreign Affairs** emphasized the importance of coordinated implementation across relevant institutions.

NICTA Response

NICTA acknowledges the views expressed by stakeholders regarding implementation timelines.

NICTA considers that implementation timelines must balance regulatory objectives with operational feasibility. NICTA will therefore adopt a phased implementation approach supported by appropriate transition periods to allow telecommunications operators sufficient time to comply with the revised requirements.

Further guidance on implementation timelines will be communicated to industry stakeholders following the finalization of the regulation.

PART B – Technical and Operational Questions for Mobile Network Operators

Question B1: What Technical Challenges Do You Foresee with API Integration into Mobile Network Operator Systems?

Stakeholder Comments

Digicel PNG indicated that it is difficult to assess potential technical challenges without access to detailed technical specifications, including system architecture, application interfaces, and integration requirements.

Vodafone PNG identified several potential challenges, including compatibility between existing operator systems and external verification platforms, system performance

considerations, and the need to ensure that operator systems can manage large transaction volumes during nationwide registration exercises.

NICTA Response

NICTA acknowledges that system integration may present technical challenges for telecommunications operators. The Authority recognizes the importance of providing clear technical specifications and implementation guidance to support system integration.

NICTA will continue to engage with operators and relevant stakeholders to ensure that system integration requirements are clearly communicated and that implementation approaches remain practical and achievable.

Question B2: What service-level standards (uptime, redundancy, fallback) should apply to Digital ID APIs?

Stakeholder Comments

Digicel PNG indicated that it could not provide specific recommendations regarding service-level standards without further technical details.

Vodafone PNG recommended that system infrastructure supporting subscriber verification processes maintain high levels of availability, supported by redundant infrastructure and disaster recovery mechanisms. Vodafone also suggested the inclusion of fallback mechanisms to allow temporary verification processes during system outages.

NICTA Response

NICTA acknowledges the importance of maintaining reliable and resilient systems supporting subscriber registration processes.

NICTA agrees that appropriate service-level standards, including system availability, redundancy, and fallback mechanisms, are essential to ensure continuity of SIM registration services. These considerations will be addressed during the technical implementation phase in consultation with industry stakeholders.

Question B3: Should PNG adopt a specific Identity Assurance Level (IAL) for SIM registration?

Stakeholder Comments

Digicel PNG recommended that identity verification requirements remain proportionate and practical given the availability of identification documents within Papua New Guinea. The company suggested that verification requirements should remain flexible to avoid excluding individuals who may not possess formal identification documentation.

Vodafone PNG recommended adopting a moderate identity assurance standard that balances strong verification requirements with practical implementation considerations.

NICTA Response

NICTA acknowledges the views expressed by stakeholders regarding identity assurance requirements.

The Authority agrees that subscriber verification processes must remain both effective and accessible. Accordingly, the regulatory framework will continue to support verification mechanisms that ensure the accuracy of subscriber information while remaining practical for implementation across the country.

Question B4: What biometric modalities are most reliable in PNG environments (fingerprint vs facial)?

Stakeholder Comments

Digicel PNG did not support mandating specific biometric verification technologies and emphasized the need to consider operational challenges and privacy considerations associated with biometric data collection.

Vodafone PNG suggested that fingerprint recognition technologies may provide reliable verification in many environments, while facial recognition could serve as an alternative method where fingerprint verification is not feasible.

NICTA Response

NICTA acknowledges the views expressed regarding biometric verification technologies.

Given the operational and privacy considerations associated with biometric data, NICTA considers that the use of biometric verification should not be mandated under the current regulatory framework.

Telecommunications operators may continue to utilize appropriate subscriber verification methods that comply with regulatory requirements.

Question B5: What cybersecurity controls should be mandatory (MFA, tokenization, endpoint security)?

Stakeholder Comments

Digicel PNG recommended that cybersecurity controls be addressed through broader cybersecurity frameworks rather than being prescribed within SIM registration regulations.

Vodafone PNG recommended several security controls including strong authentication mechanisms, encrypted communications between systems, and secure device management practices.

NICTA Response

NICTA acknowledges the importance of strong cybersecurity safeguards for systems handling subscriber information.

Telecommunications operators are required to implement appropriate security controls to protect subscriber data and maintain the integrity of registration systems. NICTA will continue to monitor cybersecurity practices and may introduce additional regulatory guidance where necessary.

Question B5: Should third-party cybersecurity audits be annual or bi-annual?

Stakeholder Comments

Digicel PNG indicated that decisions regarding cybersecurity audit requirements should be determined as part of broader government cybersecurity frameworks.

Vodafone PNG emphasized that subscriber information should be treated as highly confidential and recommended strict access controls and auditing practices to ensure proper handling of personal information.

NICTA Response

NICTA acknowledges the importance of independent oversight and auditing mechanisms to ensure the security of systems handling subscriber information.

NICTA supports the adoption of appropriate auditing and monitoring practices by telecommunications operators and will continue to review regulatory mechanisms to ensure effective oversight.

Question B7: What is the appropriate data retention period for Sim Registration?

Stakeholder Comments

Digicel PNG supported maintaining the current requirement for operators to retain subscriber records for six months following SIM deactivation.

Vodafone PNG recommended a longer retention period of seven years to support regulatory compliance, operational requirements, and investigations where necessary.

NICTA Response

NICTA acknowledges the differing views regarding data retention periods.

NICTA considers the current retention period within the existing regulatory framework to be appropriate and proportionate. These provisions will therefore be maintained in the revised regulation.

Question B8: What data classification standards should apply to MNO's and Agents?

Stakeholder Comments

Digicel PNG indicated that data classification standards should be determined through broader governance frameworks rather than being specific to SIM registration.

Vodafone PNG recommended that subscriber information be treated as highly confidential data, with strict access controls and monitoring mechanisms in place.

NICTA Response

NICTA agrees that subscriber information must be treated as sensitive personal data and handled in accordance with appropriate security and confidentiality standards.

Telecommunications operators remain responsible for implementing appropriate data protection and access control mechanisms to safeguard subscriber information.

Question B9: How should offline verification systems synchronize securely once reconnected?

Stakeholder Comments

Digicel PNG indicated that synchronization processes should be determined as part of broader system design and implementation frameworks.

Vodafone PNG recommended that any data collected through offline registration processes be synchronized securely with central systems using encrypted communications and appropriate validation controls.

NICTA Response

NICTA acknowledges the importance of ensuring that subscriber information collected through offline processes is securely transmitted and synchronized with central registration systems.

Appropriate security safeguards must be implemented to ensure that subscriber information remains protected throughout the synchronization process.

Question 10: What redundancy measures are required to ensure registration continuity?

Stakeholder Comments

Digicel PNG emphasized the importance of ensuring system reliability through robust infrastructure, strong service-level agreements, and fallback mechanisms to support verification processes during system outages.

Vodafone PNG recommended implementing high-availability infrastructure, load balancing, and failover systems to maintain service continuity.

NICTA Response

NICTA agrees that robust infrastructure and redundancy mechanisms are essential to ensure uninterrupted SIM registration services.

Telecommunications operators are expected to implement appropriate system reliability and contingency measures to ensure continuity of registration processes.

4. Conclusion

NICTA appreciates the constructive feedback provided by stakeholders during the consultation process.

The submissions received have provided valuable insights into the operational, regulatory, and technical considerations associated with updating the SIM Registration Regulation. The Authority has carefully considered all comments received and has incorporated relevant stakeholder feedback where appropriate in the final regulatory framework.

The revised SIM Registration Regulation aims to strengthen the integrity of subscriber information, improve regulatory oversight, and support the secure and reliable provision of telecommunications services across Papua New Guinea.

5. Next Steps

Following the completion of the consultation process and consideration of stakeholder submissions, NICTA will proceed with finalizing the **SIM Registration Regulation (Amendment and Consolidation)**.

The finalized regulation will be submitted for approval in accordance with the requirements of the **National Information and Communications Technology Act 2009**.

NICTA will continue to engage with Mobile Network Operators and relevant key stakeholders during the implementation phase to ensure smooth and effective compliance with the revised regulatory framework.