**Date:** 28 November 2025

**ICANN Public Comment Proceeding: "Registration Data Request Service (RDRS) Policy Alignment Analysis"**

**Comprehensive Response from Papua New Guinea on the RDRS Policy Alignment Analysis**

## 1. Introduction

Papua New Guinea (PNG) fully endorses the draft GAC Comments on the RDRS Policy Alignment Analysis (27 November 2025) and supports the ICANN Board's roadmap to align policy, implementation, and operational needs for access to gTLD nonpublic registration data.

This submission is grounded in PNG's current national realities:

- The .pg ccTLD is currently administered by Papua New Guinea University of Technology (Unitech) under a long-standing but informal arrangement;
- The Government is actively standardizing the .gov.pg subdomain to ensure integrity and prevent impersonation;
- PNG is in the research phase of exploring a national Protective DNS (PDNS) system, in collaboration with the Australian Government; and
- The Department of ICT is leading the development of a formal, sovereign .pg ccTLD governance framework.

These initiatives highlight a critical gap: PNG's ability to secure its national digital ecosystem depends heavily on access to accurate gTLD registration data, since the majority of cyber threats—phishing, fraud, disinformation—originate from domains registered under gTLDs like .com and .net.

## 2. National Context: .pg Stewardship and Digital Sovereignty

### 2.1 Current .pg Administration by Unitech

The .pg ccTLD has historically been delegated to Papua New Guinea University of Technology (Unitech), a respected academic institution with technical expertise but no formal mandate or institutional capacity for national domain governance, policy development, or cross-border abuse coordination.

While Unitech has responsibly maintained minimal .pg operations, this arrangement is not sustainable as PNG's digital economy and cybersecurity needs grow. The Government recognizes the need to transition .pg to a formal, accountable, and nationally governed structure—a process now underway.

### 2.2 Securing .gov.pg

To protect public trust, PNG is implementing strict controls to limit .gov.pg registration exclusively to verified government entities. However, malicious actors routinely register lookalike domains under gTLDs (e.g., health-dept[.]com) to impersonate government services.

Without timely access to gTLD registrant data via a reliable system like RDRS, PNG cannot effectively detect, attribute, or disrupt these threats.

### 2.3 Exploring Protective DNS (PDNS)

In partnership with the Australian Government, PNG is researching the feasibility of a national Protective DNS (PDNS) service to block access to known malicious domains in real time. However, PDNS is a blocking tool—not an attribution tool. To fully leverage PDNS for threat disruption (e.g., takedowns, law enforcement action), PNG must be able to identify the individuals or entities behind malicious domains.

This makes a robust, timely, and standardized registration data access mechanism essential—even before PDNS is deployed.

## 3. Position on the Six RDRS Enhancements

PNG fully supports the six enhancements proposed by the ICANN Board and offers the following national perspective:

i) **Mandatory Registrar Participation:** Voluntary RDRS participation has resulted in inconsistent responses, particularly from registrars unfamiliar with PNG authorities. All gTLD registrars must be contractually obligated to respond, ensuring equity for developing countries.

ii) **Disclosure of Privacy/Proxy Customer Data:** Threat actors exploit registrar-affiliated privacy/proxy services to evade accountability. Registrars must be required to disclose underlying customer data via RDRS for authenticated urgent requests.

iii) **Technical Integration (APIs):** As PNG builds future cyber capabilities—including potential PDNS and automated abuse reporting—API access to RDRS is critical for scalability and efficiency.

iv) **SLAs for Urgent Requests:** Delays directly compromise investigations into government impersonation, child exploitation, and financial fraud. Binding SLAs (e.g., 24–72 hours) must be enforceable through contractual mechanisms.

v) **Phased Federated Authentication:** PNG supports law enforcement-first authentication, but urges ICANN to ensure the system is globally inclusive, low-cost, and compatible with developing-country institutional realities.

vi) **Voluntary ccTLD Participation:** While PNG explores future .pg participation, we recognize that ccTLDs operate under distinct legal and technical regimes. ICANN should provide flexible, sovereignty-respecting pathways—not mandates—for interoperability.

## 4. On Policy Pathways and Urgency

PNG acknowledges the GNSO's historical work but stresses that years of deliberation have not produced enforceable access mechanisms, while cyber threats escalate.

We fully support the GAC's position: if the GNSO cannot deliver consensus policy swiftly, ICANN must pursue alternative mechanisms—including contractual obligations—to implement the six enhancements.

Our national digital sovereignty—and the safety of our citizens—cannot wait.

## 5. Recommendations

i) Mandate RDRS participation for all gTLD registrars via contractual terms by end of 2026.

ii) Require registrars to disclose underlying privacy/proxy customer data for urgent, authenticated requests.

iii) Prioritize API development with support for automation in low-resource environments.

iv) Enforce SLAs for urgent requests, tied to compliance reporting.

v) Finalize inclusive law enforcement authentication with regional stakeholder input.

vi) Support ccTLDs like .pg with technical guidance for voluntary, sovereignty-aligned participation as PNG transitions to formal .pg governance.

**DEPARTMENT OF INFORMATION & COMMUNICATIONS TECHNOLOGY**
PO Box 784 Vision City, WAIGANI, National Capital District ,TISA RUMA, Section 427, Hohola (Islander Drive), Waigani,
Email: russell.woruba@ict.gov.pg

## 6. Conclusion

Papua New Guinea is at a pivotal moment in its digital journey—transitioning from informal .pg stewardship to a sovereign, accountable governance model, while strengthening public sector cybersecurity and exploring next-generation defenses like PDNS.

But these efforts are only as effective as our ability to act across the global DNS. A mandatory, technically integrated, and enforceable RDRS is essential infrastructure for digital sovereignty, public safety, and international cooperation in the Global South.

We urge ICANN, the GNSO, and the Board to act decisively, inclusively, and without delay.

Submitted on behalf of the Government of Papua New Guinea through the Department of Information and Communications Technology

**Jessy Sekere**
Acting Deputy Secretary
Digital Government Coordination & Delivery
jessy.sekere@ict.gov.pg