TECHNICAL AND COMPLIANCE COMMITTEE
TWENTY-SECOND REGULAR SESSION
23-29 September 2026
Pohnpei, Federated States of Micronesia (Hybrid)

Update on WCPFC Information and Network Security Framework

WCPFC-TCC22-2026-21
25 August 2026

Submitted by the Secretariat

Purpose and Introduction

1. The purpose of this paper is to provide an update on the Secretariat's efforts to implement an Information and Network Security Governance Framework for the WCPFC that ensures the organization's digital assets are secure and that any potential cyberthreats or security breaches are mitigated and managed in accordance with best practice.

2. To mitigate vulnerabilities and exposure to cyber threats, the WCPFC Secretariat has continued its efforts since TCC21 through various initiatives to maintain its strong security posture. Efforts such as ongoing alignment towards the DSI *SMB1001*[1] cybersecurity framework and regular penetration (PEN) testing on software solutions continue to provide the Secretariat with the relevant information to strategically assess infrastructure improvements.

Implementation Progress

3. In 2026, the Secretariat initiated a third-party system review of the Secretariat's data network and overarching IT ecosystem. The review will entail a holistic assessment of the Secretariat's IT infrastructure, information management systems (IMS), data governance, and operational policies and procedures, with the purpose of identifying risk factors stemming from areas needing improvement. The review will also provide information on how well the Secretariat's organizational needs and IT investments are aligned to meet current and emerging needs.

4. The data network review began by establishing five key assessment areas:

   i. **Hardware and Infrastructure:** hardware, infrastructure, hosting, cloud servers, networks, and disaster recovery.

[1] For further detail on SMB1001| https://dsi.org/smb1001.

ii. **Technology Supportability:** operating systems, vendor support, patching, legacy risks, and upgrade pathways.

iii. **Data Governance and Access Controls:** data governance, including data classification, retention, and user access.

iv. **Database Application Architecture:** database structures, integration, and coding languages.

v. **User Interface and Service Delivery:** usability, performance, and service delivery of user portals.

5. Assessments of these five areas involve various Secretariat team members, IT development firms, and Secretariat IT consultants. Information was documented through surveys/questionnaires, interviews, and non-intrusive, read-only, meta-data system access granted to reviewers. Weekly meetings were conducted with all available contributors to maintain communication and provide updates on the data network review's progress.

6. Ongoing security risk awareness remains an important aspect of the Secretariat's security governance framework, as demonstrated by recent efforts such as the implementation of system-driven flagging of suspicious emails and the establishment of training campaigns for new staff through the KnowBe4[2] platform. As cybersecurity threats continue to evolve, these processes will be expanded upon to cover additional topics such as safer use of agentic AI, and its monitoring thereof.

Next Steps

7. At the time of preparing this paper, the Secretariat is progressing the following activities:

i. Progress data network review to assess *SMB1001* security governance framework alignment through related IT infrastructure components.

ii. Conduct routing penetration testing by October 2026 to assess software systems undergoing streamlining and migration.

8. At the policy level, the Secretariat aims to leverage findings from the data network review to produce digital asset management guidelines where needed. This was initially established by both the Secretariat and reviewers as an area of improvement.

9. The Secretariat welcomes questions and feedback from TCC22.

[2] https://www.knowbe4.com/