Western and Central Pacific Fisheries Commission

TECHNICAL AND COMPLIANCE COMMITTEE
Twenty-First Regular Session
24 September to 30 September 2025
Pohnpei, Federated States of Micronesia (Hybrid)

UPDATE ON WCPFC'S INFORMATION AND NETWORK SECURITY GOVERNANCE FRAMEWORK

WCPFC-TCC21-2025-26
9 September 2025

Submitted by the Secretariat

Purpose

1. The purpose of this paper is to provide an update on the Information and Network Security Governance Framework and the Secretariat's efforts to improve the organization's security posture.

Introduction

2. Cyber threats continue to grow in frequency and sophistication, including attacks aided by generative AI. The Secretariat has adopted a practical approach to managing information and network security aligned to the organization's scale and risk profile, based on the principle of cost effectiveness with clear steps for continual improvement and regular (annual) updates.

3. In recent years, the Secretariat has undertaken various initiatives to secure its IT infrastructure, recognizing the importance of robust cybersecurity practices to safeguard the Commission's data and information assets. Building upon these efforts, the Secretariat outlined its approach in Finance and Administration Paper 18 to develop a structured Information and Network Security Governance Framework that is suitable and appropriately scaled for the needs of the WCPFC. This approach recognizes the increasing complexity of cyber threats, coupled with WCPFC's reliance on digital systems for data and information management, and proposes a framework-based approach that can identify, mitigate, and manage security risks in an organized and transparent manner. The goal of the proposed framework is to allow the Commission to strategically invest in its IT security to a level the Commission determines is appropriate, while at the same time complementing existing approaches to cybersecurity, including regular penetration (PEN) tests and security reviews, and ensuring an overall framework approach that is effective, sustainable, and scalable to respond to the evolving digital environment.

4. In 2024, the Secretariat explored the use of the US-based National Institute of Standards and Technology (NIST) Cybersecurity Framework as guidance for the WCPFC Information and Network Security Governance Framework.[1] Following careful consideration and closer review, the Secretariat determined that the NIST framework is too resource-intensive to support the Secretariat's needs.

5. Further research in 2025 led the Secretariat to explore an alternative framework from Dynamic Standards International (DSI), the *SMB1001*.[2] The DSI framework is a multi-tiered, regularly updated

[1] See Finance and Administration Paper 18
[2] For further detail on SMB1001| https://dsi.org/smb1001

solution that is expected to support a more agile approach to improvement that is better aligned to the Secretariat's resources.

6. WCPFC's Information and Network Security Governance Framework will be based on the DSI *SMB1001* standard providing cybersecurity certification with five levels:

i. Level 1 establishes essential preventive controls.
ii. Level 2 adds more advanced preventive measures.
iii. Level 3 expands to a holistic risk management approach across people, processes, and technology.
iv. Level 4 strengthens formal governance procedures and policy.
v. Level 5 matures governance and risk practices across the organization.

7. The choice of this framework is intended to utilize existing resources, ensuring that the process is both cost-effective and efficient.

Implementation Status

8. In May 2025, the Secretariat undertook a self-assessment using the DSI *SMB1001* Framework. The outcome of this assessment places the Secretariat above Level 3, with many Level 4 elements already in place. Some components in Level 2 still need full documentation.

9. Alongside work to evaluate the DSI *SMB1001* Framework, activities to continually improve the cybersecurity posture of the Secretariat have continued. In 2025, the Secretariat completed the following activities to improve the organization's cybersecurity posture:

i. An internal Cybersecurity Committee met on a regular basis.
ii. Conducted a training program for all staff on assessing cybersecurity risk.
iii. Developed the WCPFC Cyber Risk Register as a version-controlled living document to help identify and assess potential risks to WCPFC's IT infrastructure and information systems.
iv. Performed routine training for all staff with regular email phishing campaigns.
v. Performed a series of cybersecurity awareness training campaigns.
vi. Routine vulnerability scans on core IT infrastructure.
vii. Upgraded email scanning environment with an AI approach to detecting business email compromise.
viii. Implemented an advanced threat detection capability with formal response actions across our M365 platform.
ix. Monitoring and raising awareness within the Secretariat about recent cybersecurity events in other RFMOs, regional agencies, and within CCMs at national level.

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

i. Annual penetration test on priority, public facing secure websites.
ii. Enhanced staff training to coincide with Cybersecurity Awareness Month through the month of October.

Next Steps

11. Efforts to embed the DSI *SMB1001* Framework in the Secretariat are well underway. This approach represents a logical next step in enhancing the WCPFC's overall cybersecurity posture. By utilizing existing resources and adapting best practices, the Secretariat is committed to ensuring that WCPFC's information systems remain secure and resilient in the face of evolving cyber threats.

12. The Secretariat has set a target for achieving Level 4 on the framework by 2026 and Level 5 on the framework by 2027. Further updates will be provided to FAC19 on any budgetary considerations that may need to be considered for compliance with higher levels of the DSI *SMB1001* framework.

13. The Secretariat provides this information for awareness and welcomes questions and feedback from TCC21.