TECHNICAL AND COMPLIANCE COMMITTEE
Nineteenth Regular Session
20 –26 September 2023
Pohnpei, Federated States of Micronesia

IT Security Update 2023

WCPFC-TCC19-2023-23
14 September 2023

Prepared by the Secretariat

Purpose

1. This paper presents an update for the information of TCC19 on the Secretariat's IT Security status following a Commission decision in 2022 for the Secretariat to expand its annual VMS security review to cover WCPFC information systems administered by the Secretariat.

Background

2. The Commission's VMS SSPs Section 6.10 requires the Secretariat to undertake an annual review of the integrity of the VMS data, using external (to the Secretariat), qualified personnel. At TCC18 (2022), the Secretariat proposed a revised approach to carrying out its mandated VMS security review to expand its scope to include a more dynamic and continual assessment of the WCPFC information systems. This expanded scope followed a Secretariat-initiated security assessment undertaken in 2021 in partial response to the increase in online-based activities resulting from the global pandemic.

3. TCC18 supported the Secretariat's recommendation for an expanded security review, with a budget of USD$11,900, which was subsequently adopted by the Commission at WCPFC19. In addition, the Commission agreed to the Secretariat including annual penetration testing of WCPFC information systems, at an additional budget allocation of USD$15,000. The indicative budget for 2024 and 2025 approved at WCPFC19 had anticipated there would be continuation of the expanded security review approach work, including penetration testing, through 2024-2025.

2023 Update

4. On March 16, 2023, consultancy services for the provision of ongoing Cybersecurity analysis and support were tendered and the successful bidder, Defend NZ was awarded the contract mid-April.

5. Defend assigned a dedicated Cybersecurity Adviser (CSA) to manage the ongoing process of improving the security posture of the Secretariat. The CSA has conducted monthly assessments since mid-April and provided advice to the Secretariat's IT Department on areas that require attention. An internal IT Security Committee within the Secretariat provides support to the consultancy and ensures the work is carried out consistent with Commission requirements.

6. Following initial advice from the CSA, the Secretariat directed its early focus toward additional strengthening of in-house server and workstation security ahead of developing a security risk register, the latter of which was determined to be a key output of the Secretariat's 2021 security assessment. The risk register development will be an iterative process coordinated by the Secretariat's IT Security Committee in the third and fourth quarters of 2023.

7. To achieve "best practice" in the technical program of work, the Secretariat undertook a migration to the *Microsoft 365* Defend platform to systematically assess security controls in place. In conjunction with the Microsoft security assessments, several configuration changes and policy updates have been implemented to strengthen the Secretariat's IT security infrastructure.

8. Upcoming related work will involve development of a single-sign-on (SSO) across all IT systems in the Secretariat. This means that with an SSO, users will be able to access multiple Secretariat systems with the same login credentials, a feature which improves enterprise security by reducing the need for multiple passwords across multiple systems.

9. To support implementation of an SSO, the Secretariat is continuing to migrate its information systems from the SharePoint to the Drupal platform, a process that has been completed for the RFV and which has resulted in improved security of RFV data. Platform migration of the system that supports the Annual Report Part 2 and development of the Compliance Monitoring Report is in process, and updates will be provided to TCC20.

10. The Secretariat continues to strengthen its cybersecurity awareness through monthly and quarterly tests and training on common attempts at security breaches that users may encounter in the course of their work.

11. A proposal is currently under development for a third party to develop a scope of work on an external penetration test across the Secretariat's public facing secure websites, expected to be completed by the end of 2023. This will utilize the budgeted funds for 2023 and prepare for implementation in 2024. A report on this work will be provided to TCC20.

12. Further updates and views from the Secretariat to support this work will be provided to FAC17.

Recommendation

13. TCC19 is invited to:

a. note the Secretariat's progress in strengthening its in-house security of IT systems and resources;

b. Note the Secretariat's plans to continue the ongoing, expanded security review work, which includes completing work on the development of an IT Systems Risk Register and conduct of routine penetration testing, and efforts to continue to improve the Secretariat's IT security score.

c. Recommend the Commission support the continuation of the Secretariat's ongoing, expanded security review work.