TECHNICAL AND COMPLIANCE COMMITTEE
Eighteenth Regular Session
Electronic Meeting 21 – 27 September 2022

UPDATE ON ANNUAL TASK THAT THE SECRETARIAT REVIEW THE INTEGRITY OF VMS DATA

WCPFC-TCC18-2022-23
19 September 2022

Paper by the Secretariat

Purpose

1. The purpose of this paper is to table for TCC18's consideration an improved mechanism for verifying the integrity of the VMS data.

Background

2. The VMS SSPs Section 6 paragraph 10 stipulates an annual tasking to the Secretariat to review the integrity of VMS data as follows:

> *"The integrity of the Secretariat's VMS data will be verified annually by qualified personnel exterior to the Commission Secretariat staff."*

3. The Secretariat's approach to this requirement in the past has been to contract Deloitte Guam to complete what is often referred to internally as an "IT Audit". In practice, the IT Audit is a Review of the Secretariat's management of VMS (and related) data, through a set of Agreed Upon Procedures (AUP). The procedures are intended to consider the package of IT systems and associated Secretariat data management and IT system management procedures that utilize or store WCPFC VMS data. This review is based on scrutiny of a set of documents and log files from our internal corporate network, computer configurations and building access.

4. Prior to the COVID-19 pandemic, part of the "IT Audit" AUPs was that Deloitte Guam would send an IT auditor to WCPFC Secretariat headquarters to complete the review and conduct interviews with relevant staff. Since the COVID-19 pandemic, the FSM's travel border restrictions have prevented the travel by the Deloitte Guam staff member, and this continues to challenge the completion of an annual review.

5. Furthermore, the Secretariat was recently advised by Deloitte that they will be closing the Guam office and not offering this service in future.

6. The most recent Review was based on virtual interviews and the submission of log files and documents by the Secretariat in June 2021 "2021 Review of Integrity of Secretariat VMS data, and Review of Integrity of IMS and RFV" and the report is presented to TCC18 (WCPFC-TCC18-2022-RP09).

Recent developments and additional considerations related to IT Security

7. There are some additional considerations that the Secretariat has been considering internally and conscious that the scope of the Deloitte AUP is limited to the VMS data integrity. These include:

- In the last 5 years, WCPFC has moved to a more distributed platform with CCMs able to interact with secure content via our website infrastructure and our service providers such as Trackwell. This is hosted outside of the Secretariats internal server network located in Pohnpei. These developments have been driven by a need for the Secretariat to support greater expectations from the Commission and wider stakeholders from WCPFCs work and data. At present the Commission has broad range of online reporting solutions that we provide as services to CCMs but also information/reports/figures that are made available publicly.
- Over the past 24 months as a matter of necessity due to the COVID-19 pandemic, the Secretariat has been successful in continuing to build upon and leverage the IT systems and infrastructure that we have built over several years, and fortunately this meant that we were successfully able to transition to supporting online meetings.
- As a response to the COVID-19 pandemic circumstances the Secretariat has also been able to utilize our online IT infrastructure to ensure that all staff, both professional and support, were able work almost as effectively remotely as they do from the office. The introduction of regular cybersecurity awareness training using the *Knowbe4 training platform* for staff has been an important step in mitigating some of the potential IT security risks, and particularly with more staff working outside of the office including over long periods.
- Also, in the past 12 to 18 months we have seen a significant increase in cybersecurity breaches globally either as a social engineering attack or exploiting a software vulnerability.
- The Commission at WCPFC18 approved the Secretariats 2022/23 plans to commence IT system upgrades, that respond to limitations of the Microsoft SharePoint software platform that WCPFC has used to support the Compliance Monitoring Scheme and Annual Reporting, as well as the Record of Fishing Vessels and Transhipment E-reporting systems among many others.
- The scope of the annual IT security review is limited to reviewing a relatively traditional set of procedures that were agreed when the reviews began with a focus on internal IT infrastructure.

8. In addition, the Secretariat recommends, due to the expanded online resource development and trend towards additional electronic data exchanges through API developments, and cloud hosted environments, that it would be a sensible and appropriate next step for the Secretariat to present for TCC's consideration and the Commission's approval, a recommendation to broaden the scope of the IT security audit and security assessments to cover full range of IT systems and services that are delivered by WCPFC.

9. In late 2021, the Secretariat decided to supplement the regular IT audit / review undertaken by Deloitte, by commissioning some independent expert to provide the Secretariat with an additional more holistic review of the Secretariat's approach to information security. This was undertaken by DEFEND NZ with the stated objective "*to provide an effective*

assessment of our cybersecurity posture and to provide an appropriate set of control to monitor given the size of WCPFC and the nature of the organization".

Outcomes of the DEFEND Review

10. The review recommended the Secretariat formalize its approach to managing cybersecurity risk by developing a register of vulnerable systems and processes, identifying key cyber risks, and required risk mitigation activities (implement sufficient controls to bring risks within WCPFC's risk tolerance/appetite).

11. Also identified through the review was the lack of true penetration testing being conducted on WCPFC systems. The Secretariat have increased the breadth and frequency of scanning systems for known vulnerabilities and applying security patches as a routine practice. The review recommends supplementing the vulnerability scan with periodic penetration testing to be conducted by an external cybersecurity organization.

12. The review identified several gaps in the policy and procedures of the Secretariat, gaps the Secretariat have attempted to fill for some time now.

13. To facilitate further consideration of cybersecurity matters and next steps within the Secretariat in 2022 an internal cybersecurity committee was established, consisting of the Finance and Administration Manager, the Compliance Manager and the IT Manager. The role of the Secretariat's cybersecurity committee will be to prioritize and coordinate the schedule of activities to improve the security posture of the Secretariat and the information systems.

Proposed Approach

14. TCC is invited to consider moving away from the annual audit of agreed upon procedures currently conducted by Deloitte Guam to a more dynamic and continual assessment of the WCPFC information systems. This would be done through working with an IT security firm to develop a risk register that is continually updated. The risk register and the recommended solutions to those risks and associated budget could form the basis of a report to TCC in place of the annual audit. This new proposed approach is estimated to require an increase of $3,500 USD, over-and-above the existing VMS Security Audit budgeted amount (currently $8,400 USD) ~ total annual budget of $11,900 USD.

Recommendation

15. TCC is invited to support the Secretariat's recommendation to expand the annual VMS Security Audit budget, to include a more dynamic and continual assessment of the WCPFC information systems, with an estimated budget of $11,900 USD.

16. TCC is invited to also consider recommending to the Commission that an additional budget allocation of $15,000 USD be set aside for annual penetration testing of the WCPFC information systems.