FINANCE AND ADMINISTRATION COMMITTEE
Eighteenth Session
Suva, Fiji (Hybrid)
27 November to 3 December 2024

Development of a WCPFC IT Security Framework

FAC18-2024-09
18 October 2024

Submitted by the Secretariat

Purpose

1. The purpose of this paper is to provide information to FAC18 on the Secretariat's ongoing efforts to secure WCPFC information and technology infrastructure.

Background

2. In recent years, the WCPFC 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 proposes the development of a more structured IT Security Framework that is suitable and appropriately scaled for the needs of the WCPFC. This paper provides an overview of the proposed framework, the basis for its development, and the intended approach for implementation.

Need for an IT Security Framework

3. The increasing complexity of cyber threats, coupled with WCPFC's reliance on digital systems for data and information management, necessitates the creation of a comprehensive IT Security Framework. Such a framework would allow the Commission to systematically identify, mitigate, and manage security risks in an organized and transparent manner. It will also allow the Commission to strategically invest in its IT security to a level the Commission determines is appropriate. The current approach to cybersecurity, including regular penetration (PEN) tests and security reviews, while effective, would benefit from being integrated into a larger, overarching framework to ensure continuity, consistency, and scalability of security measures.

4. The Secretariat is exploring the use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework as guidance for the WCPFC IT Security Framework. This choice is based on NIST's reputation as a globally recognized, adaptable, and scalable set of best practices for managing and reducing cybersecurity risk.

5. The adoption of a cybersecurity framework by the WCPFC that is based on NIST would provide a structured and consistent approach to cybersecurity, enhancing the Secretariat's ability to address both internal and external risks, while ensuring alignment with international best practices. Recognizing that the WCPFC has unique needs, modifications will be made to the

NIST Framework to ensure that it is appropriately tailored to suit the size, operations, and specific challenges faced by the organization.

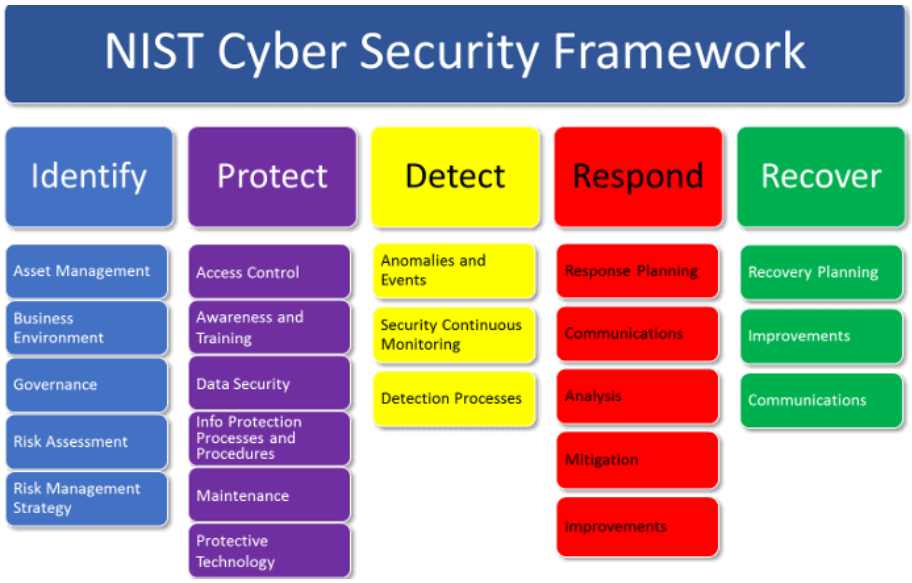

Illustration of the NIST Cybersecurity Framework, including its five core functions. Source: https://www.nist.gov/

Next Steps

6. The development of the WCPFC IT Security Framework will utilize existing resources, ensuring that the process is both cost-effective and efficient. The Secretariat has already gained valuable insights through its ongoing cybersecurity initiatives, such as the recent PEN tests carried out in 2023 and 2024, and security reviews. These insights will inform the customization of the NIST Framework to suit the specific requirements of WCPFC.

7. The Secretariat will undertake the development of a Security Risk Register beginning in early 2025 to help identify and assess potential risks to WCPFC's IT infrastructure and information systems. This exercise will form the basis of the new IT Security Framework, ensuring that identified risks are documented, classified, and managed effectively.

8. The development of an IT Security Framework, based on the NIST Cybersecurity Framework, 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 IT systems remain secure and resilient in the face of evolving cyber threats.

9. The Secretariat provides this information for awareness and welcomes questions and feedback from FAC18. Updates will be provided to TCC21 and FAC19 in 2025.