International Civil Aviation Organization

Twelfth Meeting of the Common aeRonautical Virtual Private Network Operations Group (CRV OG/12)

Denarau Island, Fiji, 23-26 January 2024

Agenda Item 12: Using the rest of CRV Pioneer State Contribution to the ICAO Managed Service Agreement (MSA)

CYBER SECURITY REVIEW UPDATE

(Presented Airways New Zealand)

SUMMARY

This paper presents an update on the proposed Cyber Security Review.

1. INTRODUCTION

1.1 Several Cyber security review options were presented at CRV OG11 held in Bangkok 01-03 February 2023.

1.2 It was decided to pursue the following options which was endorsed by the meeting for ACSICG/10 consideration and CNS SG/27 adoption:

Option 2 - Penetration test of the PCCWG implementation only. This option would involve a penetration tester access the PCCWG CRV network from PCCWG's office, POP or CRV users site. The test would involve discovering but not limited to the connectivity available from that site with the CRV network, including any possible exploits of the PCCWG NID, visibility of the last mile service providers network, visibility of the internet, visibility of the wider PCCWG network.

Option 5 - Engage a Security consultant to review the Common Package, RFP documentation including the response, Implementation Plan and the Operations Manual and provide a Security recommendation based on this review. The recommendations would not necessarily expose any States or PCCWGs security implementations. Any agreed recommendations we implement would need to be implemented on trust.

2. DISCUSSION

2.1 A Terms of Reference was created as per the discussion at CRV OG11 by the Ad Hoc Expert Group and present to ACSICG10 meeting where the ToR was adopted by ACSICG.

2.2 ToR is attached to this paper as **Appendix A**.

2.3 Two Cyber Security organisations that specialize in carrying out Cyber Security Reviews and Penetration testing have been engaged to provide quotations.

These are Aura Cyber Security Consultant - IT Risk Assessment - New Zealand and ZX Security Full spectrum security services - ZX Security

2.4 The quotes have come back as follows:

a) Aura Security Design Review – NZD13,200
Review all CRV documents in the Common Package
Interview PCCWG Engineers
Interview CRV USERS

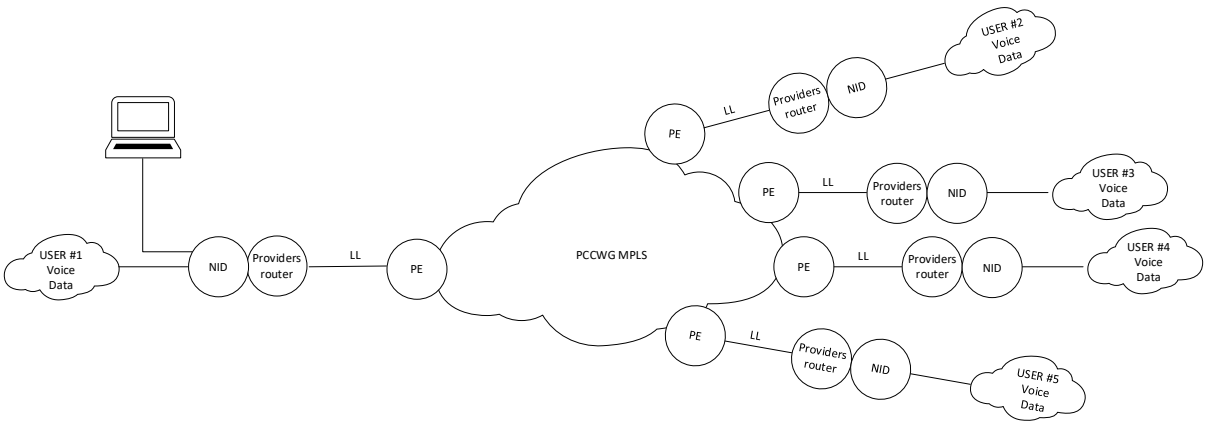
b) Aura Penetration Test – NZD22000
Actual test to be determined.

ZX Security Design Review – NZD57,960
Review all CRV documents in the Common Package
Interview PCCWG Engineers
Interview CRV USERS

ZX Security Penetration Test – NZD10650 – NZD14650

2.5 The potential penetration test could be the connecting of a test laptop/PC/device to the extra port on a CRV NID and running the scan and tests from there. This would need to be run in the Best Effort class so as not to interfere with operational traffic. The test would also need to be run at a time of low traffic.

This would validate the GRE tunnel construct and surface any potential endpoint issues but not test the potential of a compromise external to the GRE tunnel.



2.6 The meeting is requested to review both quotations, suggest the need of further quotations, if felt necessary, deliberate and share agreement/disagreement for the proposed amount, and discuss the way forward to execute this task. Based on the outcomes of the discussion, the draft

conclusion may be formulated by the meeting for the endorsement by ACSICG/11 and adoption by CNS SG/28 Meeting.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;
b) review the quotations received;
c) discuss the need of further quotations, if required, and provide support to get more quotations if needed;
d) deliberate the way forward for execution of the task; and
e) discuss any relevant matter as appropriate.

– – – – – – – – – – – – –

Terms of Reference

1. Background

The Asia Pacific Common aeRonautical Virtual Provide Network (APAC CRV) provides air traffic navigation networking to the Asia Pacific Region
The APAC CRV Operations Group (APAC CRV OG) have requested a design review of the CRV.

To assess the architecture design on how well this has been secured. It will draw on industry best practices, documentation from the telecommunications provider the CRV, PCCW Global, and various CRV members using in the solution, and the experience of the consultant and wider team.

2. In Scope

The scope of this engagement will be limited to:

- A Security Design Review of the CRV
- Network Review

3. Out of Scope

The following are not in scope for the Services under this ToR:

- Any interaction with the live operational environment
- Testing which might cause a denial of service
- Implementation countermeasures and fixes. Advice will be provided on how this should be done by the consultant
- Any remediation testing is out of scope of this agreement and will be provided separately if requested in writing by the APAC CRV OG at the APAC CRV OG's cost.

Detail of Work

1. Security Design Review

The consultant will carry out a security review of the CRV design.

- A review of the design concepts and the architectural design proposal. The aim is to both understand the approach for subsequent aspects of this review and to provide early feedback that may be used to guide the design down better pathways. This can start with the signing of the ToR and once the consultant has received all the design documentation, the review can be done remotely.

In reviewing the design, the consultant will:

- Use APAC CRV security objectives from the RFP and Operations Manual to be the basis of validation but will bring industry best practices to advise if these objectives are sufficient.
- Use policies and standards by relevant government, industry or internal bodies. These are likely to include but not limited to CIS benchmarks, ISO27001, ICAO Annex 17, NIST and ASD.
- Characterise the system architecture, component technologies, and interfaces to identify trust boundaries, data flows, and current security enforcing controls,
- Identify any additional controls that could be implemented to mitigate identified risks

Security Design Review	
Service Type	Security Design Review
Assets / Targets	APAC CRV
Effort (days)	TBD
Access	Remote, with calls via video conferencing when required.
Approach	• Consume the documentation provided by the APAC CRV OG • Identify areas where further clarification may be necessary and, after receiving permission from the APAC CRV OG and PCCWG to hold video calls with authorised technical stakeholders • Walk through a list of preliminary findings with authorised technical stakeholders • Advise preliminary outcomes to APAC CRV OG Co-Chairs • Release a draft report for feedback • Release a final report
Specific requirements	• Up to date documentation • A list of authorised APAC CRV OG and PCCWG individuals who can respond to technical questions during the engagement Note: These requirements must be met at least 1 week before work is due to commence.

2. Network Review of the APAC CRV

Security Design Review	
Targets	PCCWG's APAC CRV routers
Perspectives	Unauthenticated physical network access Authenticated physical network access
Effort (days)	TBD
Access	On site using Consultant provided Laptop Computers with options to provide testing VM within instance at consultant's discretion
Approach	• The Consultant will be positioned on-site within a PCCWG POP or an APAC CRV OG members server/equipment room • The Consultant will be granted connectivity to the PCCWG CRV router or network element at the authorised site(s)

	• The Consultant will leverage information discovered during attacks against the CRV to compromise the CRV. • The Consultant is not specifically testing the APAC CRV members LAN however by design, access to this network is required to identify and access threat surface it presents to the CRV Vulnerabilities exploited or discovered that lead to a compromise of the CRV will be reported, additional vulnerabilities will be reported to the APAC CRV Co-Chairs regarding the CRV at the consultant's discretion. The assessment is conducted according to the PTES Penetration Testing Methodology[1]. Activities include but are not limited to the following: • Passive network reconnaissance • Active interception and redirection of traffic • Enumeration of exposed services and versions • Automated vulnerability scanning of network systems • Targeted exploitation of identified weaknesses • Evaluation of the technical impact of each identified issue • Horizontal and vertical privilege escalation • Provide recommendations to mitigate any issues found in the review

3. Restricting communications

- APAC CRV OG has requested that communications regarding the engagements in this Terms of Reference be treated as "Traffic Light Protocol: Red". That is to say, outcomes from each engagement must be limited to named individuals.
- APAC CRV OG must make the Consultant aware of any changes to personnel which might impact this requirement.
- The Consultants internal quality assurance processes necessitates peer review by another consultant; these consultants will be named.

Deliverables

The deliverables for this project will include:

1. Final Report

A final report that will be delivered in PDF format and available the week following testing. It will contain the following components:

- An Executive Summary providing a summary of findings and general recommendations resulting from the review. The summary presents the assessment of APAC CRV's state of security and will detail APAC CRV's adherence to industry best practices and identify the current level of risk. The Executive Summary is intended to describe business-level risks resulting from technical findings such as regulatory, reputational and operational impacts. This section also includes a summary of severity rated as "Critical", "High", "Medium" or "Low" at a level that can be easily understood by functional management. Severity is based on a number of variables including the ease with which the vulnerability may be exploited and the potential impact of its exploitation in context of Client's business environment.
- A Detailed Findings section, which will provide in-depth details of identified vulnerabilities. This will include the steps to reproduce the issue, potential impacts of exploitation and severity rationale, and recommended remediation actions.
- A Compromise Narrative section may be included should the Consultant achieve significant compromise of APAC CRV's systems during the provision of the Services. The Compromise Narrative will provide a walk-through of the process used to achieve such compromise, including information on the tools and techniques used.

From receipt of the final report, the APAC CRV's has one working month to review and request changes. After this time the report is considered final and no further changes will be made.

2. Final Presentation

The Consultant will deliver the findings of the report to the relevant project stakeholders. The purpose of this presentation is to clearly articulate our findings, ensuring they are understood and to agree on the next steps.