



ICAO

*International Civil Aviation Organization*

**The 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)

**UPDATES ON CRV PIONEER STATES' REMAINING CONTRIBUTION TO  
THE ICAO MANAGED SERVICE AGREEMENT (MSA)**

(Presented by the Secretariat)

**SUMMARY**

This paper presents an update on the recent development of using the balance fund of the MSA.

**1. INTRODUCTION**

1.1 In the CNS SG/21 meeting held from 17 to 21 July 2017, on behalf of Fiji, Hong Kong China, New Zealand, USA, and the ICAO Secretariat, USA presented WP/17 to propose a recommendation to the Meeting to manage the remaining funds not used for the CRV selection process. The Meeting endorsed Draft Conclusion CNS SG/21-DC6: Amendment of the Management Service Agreement for CRV project (RAS14801) for APANPIRG/28 adoption.

1.2 The APANPIRG/28 meeting held from 11 to 14 September 2017 adopted the Conclusion APANPIRG/28/19: Amendment of the Management Service Agreement for CRV project (RAS14801). The CRV OG and concerned States/Administrations have taken various follow-up actions for the Conclusion APANPIRG/28/19. However, the Conclusion remains one of the outstanding Conclusions up to APANPIRG/33 held in November 2022.

1.3 The CRV OG/9 meeting held from 25-27 January 2022 prepared and adopted the Revised Annex 1 to Management Service Agreement (MSA) to utilize in the remaining fund in 5 years starting from the actual date of adoption of the revised document by APANPIRG, which was adopted as Conclusion APANPIRG/33/6 (CNS SG/26/01).

1.4 The Tenth Meeting of the Aeronautical Communication Services (ACS) Implementation Coordination Group (ACSICG/10) was held at the ICAO APAC Regional Office, Bangkok, Thailand, from 24 to 26 May 2023. The Meeting was attended by 62 participants from 19 States/Administrations, 2 International Organizations, namely IATA and ICAO, and 1 industry partner, namely Frequentis. The ACSICG/10 meeting report, working papers, information papers, and other resources can be accessed by following link: <https://www.icao.int/APAC/Meetings/Pages/2023-CRV-OG-Ad-hoc-Governance-Group-and-the-ACSICG10.aspx>

1.5 The Eleventh Meeting of the Common aeRonautical Virtual Private Network Operations Group of APANPIRG (CRV OG/11) was held from 1 to 3 February 2023 in ICAO Asia and Pacific Regional Office, Bangkok, Thailand. The Meeting was attended by 65 participants from 19 Member States/Administrations. The meeting report, working papers, information papers, and other resources can be accessed by the following link:

<https://www.icao.int/APAC/Meetings/Pages/2023-CRV-OG11-.aspx>

1.6 This paper summarizes the recent development of utilizing the remaining funds of the CRV project and invites the Meeting to take follow-up actions.

## **2. DISCUSSION**

### *Revised Amendment of the Management Service Agreement for CRV project (RAS14801)*

2.1 The eighteen CRV Pioneer States/Administrations (Australia, China, Hong Kong China, Macao China, Democratic People's Republic of Korea, Fiji, France, India, Japan, Malaysia, Myanmar, New Zealand, Philippines, Republic of Korea, Singapore, Sri Lanka, Thailand, and USA) had established Management Service Agreement (MSA) with ICAO Technical Cooperation Bureau (TCB) to select a common service provider for telecommunication service in the region. As a result, a common service provider was selected.

2.2 After the selection of the common service provider in 2016, a fund balance of USD 104,596 remained as of 31 March 2017. To better utilize the rest of their initial contribution to continue to support CRV implementation, the APANPIRG/28 meeting adopted the Conclusion APANPIRG/28/19 - Amendment of the Management Service Agreement for CRV project (RAS14801).

2.3 As of 31 December 2022, the remaining funds for use were approximately USD 88,000 (total of all remaining contributions from sixteen Pioneer States/Administrations) after refunding the remaining fund balance share to one pioneer State/Administration on request and excluding the contribution of a Pioneer State for which a direct CRV connection is not considered feasible in 2017 by the selected vendor.

2.4 The approved amended Project Document by the Conclusion APANPIRG/28/19 was not sent for the signing of pioneer member states. However, most pioneer states expressed their interest in continuing the fund for CRV in various CRV OG meetings held afterward. Moreover, some clauses of the approved amended Project Document required modifications in 2021.

2.5 The revised amended Project Document, also known as the revised Annex 1 to the Management Service Agreement (MSA), was prepared and approved by the CRV OG/9 meeting. To get the formal consent from the Pioneer States/Administration to utilize the remaining fund for the CRV as proposed by the CRV OG/9, the Revised Amendment of the Management Service Agreement for CRV project (RAS14801) was further endorsed by ACSICG/9, CNS SG/26 and APANPIRG/33 as Conclusion APANPIRG/33/6 (CNS SG/26/01), which superseded the outstanding Conclusion APANPIRG/28/19: Amendment of the Management Service Agreement for CRV project (RAS14801). As per Revised Annex 1 to Management Service Agreement (MSA), the fund will be utilized in 5 years starting from the actual date of adoption of the revised document by APANPIRG.

2.6 As such, ICAO Secretariat issued State Letter Ref.: T 8/2.15 –AP-CNS 00xx/23 dated 9 January 2023 and Ref.: T 8/2.15 – AP-CNS 0026/23 dated 17 January 2023 on the subject: - Revised Amendment of the Management Service Agreement for the CRV project (RAS14801) to Countersign

the Revised amended Project Document or inform the intention to receive the share of the remaining fund balance to 16 pioneer States. Additional clarifications were issued on 17 January 2023. In response, 16 Member States countersigned or shared confirmation to countersign the revised amended Project Document to provide consent to utilize the remaining funds for the CRV.

2.7 The CRV OG/11 Meeting held from 1 to 3 February 2023 agreed that after finalizing the Terms of Reference for the approved task and estimated cost if the remaining amount is too low to utilize for agreed tasks, CRV OG may deliberate and decide on additional cost-sharing arrangements. Additionally, if it is agreed that the remaining amount is too low for approved work and there is no consensus for the remaining cost-sharing arrangement, the remaining share to all 16 pioneer States/Administrations will be refunded.

*Using the remaining funds for a Safety Assessment of the CRV network and its ToR*

2.8 Discussion at previous CRV OG Meetings suggested that the remaining funds from the CRV Project could be used to facilitate a Safety Assessment of the CRV network. It was assumed that the Safety Assessment means a Cyber Security Review. In CRV OG/11, New Zealand presented Safety Assessment options for the CRV using the remaining money. The 6 possible Security Review options were provided to be considered by the CRV OG/11 meeting.

2.9 The CRV OG/11 meeting deliberated on various proposed options and agreed to adopt Option 2 - Penetration test of the PCCWG implementation only and 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, which was further adopted by ACSICG/10 as Conclusion ACSICG/10/02 (CRV OG/11/03) – Selection of Security Review Options 2 and 5 and Develop a ToR, for utilization of remaining money from CRV Project.

2.10 As a way forward, CRV OG/11 agreed that a draft ToR will be prepared by CRV OG Ad-hoc Expert Group and submitted to the ACSICG/10 Meeting for review and approval. After the ACSICG/10 Meeting approves ToR, quotations will be requested from various cyber security expert agencies and appraised cost with a tentative plan and timelines for its accomplishment will be presented to the CRV OG/12 Meeting for agreement on the scope of work and the final decision for utilization of fund for agreed ToR. After the approval of CRV OG/12, an agency will be selected, and the chosen agency will execute the task.

2.11 Later on, the draft ToR for Security Review using Options 2 and/or 5 was prepared by the CRV OG Ad-hoc Expert Group, which was shared with the CRV OG/11 delegates for their review and feedback on 25 April 2023. The draft ToR provided in Appendix A to this paper was reviewed by ACSICG/10 Meeting and endorsed as Conclusion ACSICG/10/03 – Adoption of ToR for CRV Security Review using Options 2 and/or 5.

2.12 Based on the adopted ToR, CRV OG Ad-hoc Expert Group has invited quotations from different vendors to prepare cost estimates for the work. Further information about the cost estimate and way forward is being shared by CRV OG Co-Chair (Asia) by WP/08 in this Meeting.

### **3. ACTION BY THE MEETING**

3.1 The Meeting is invited to:

- a) note the information contained in this paper;

- b) discuss and review the presented quotation and way forward for preparing the plan for utilization of remaining money for CRV; and
- c) 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	<ul style="list-style-type: none"><li>• Consume the documentation provided by the APAC CRV OG</li><li>• 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</li><li>• Walk through a list of preliminary findings with authorised technical stakeholders</li><li>• Advise preliminary outcomes to APAC CRV OG Co-Chairs</li><li>• Release a draft report for feedback</li><li>• Release a final report</li></ul>
Specific requirements	<ul style="list-style-type: none"><li>• Up to date documentation</li><li>• A list of authorised APAC CRV OG and PCCWG individuals who can respond to technical questions during the engagement</li></ul> <p>Note: These requirements must be met at least 1 week before work is due to commence.</p>

### 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

CRV OG/12  
Appendix A to WP/07

<b>Approach</b>	<ul style="list-style-type: none"><li>• The Consultant will be positioned on-site within a PCCWG POP or an APAC CRV OG members server/equipment room</li><li>• The Consultant will be granted connectivity to the PCCWG CRV router or network element at the authorised site(s)</li><li>• The Consultant will leverage information discovered during attacks against the CRV to compromise the CRV.</li><li>• 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</li></ul> <p>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.</p> <p>The assessment is conducted according to the PTES Penetration Testing Methodology<sup>1</sup>. Activities include but are not limited to the following:</p> <ul style="list-style-type: none"><li>• Passive network reconnaissance</li><li>• Active interception and redirection of traffic</li><li>• Enumeration of exposed services and versions</li><li>• Automated vulnerability scanning of network systems</li><li>• Targeted exploitation of identified weaknesses</li><li>• Evaluation of the technical impact of each identified issue</li><li>• Horizontal and vertical privilege escalation</li><li>• Provide recommendations to mitigate any issues found in the review</li></ul>
-----------------	---

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.