International Civil Aviation Organization

Ninth Meeting of the Common aeronautical Virtual Private Network Operations Group (CRV OG/9)

Video Teleconference, 25 – 27 January 2022

Agenda Item 11: Share best practices on cyber-safety/security and resilience among ACSICG/CRV OG/SWIM TF

CRV DIVERSITY AND SECURITY IMPLEMENTATION

(Presented by name of Federal Aviation Administration/USA)

SUMMARY

This paper reviews methods of used by the FAA in the CRV network to provide security and diversity for AMHS and voice services.

1. INTRODUCTION

1.1 This paper gives an overview of how the FAA has implemented diversity and security for CRV network access.

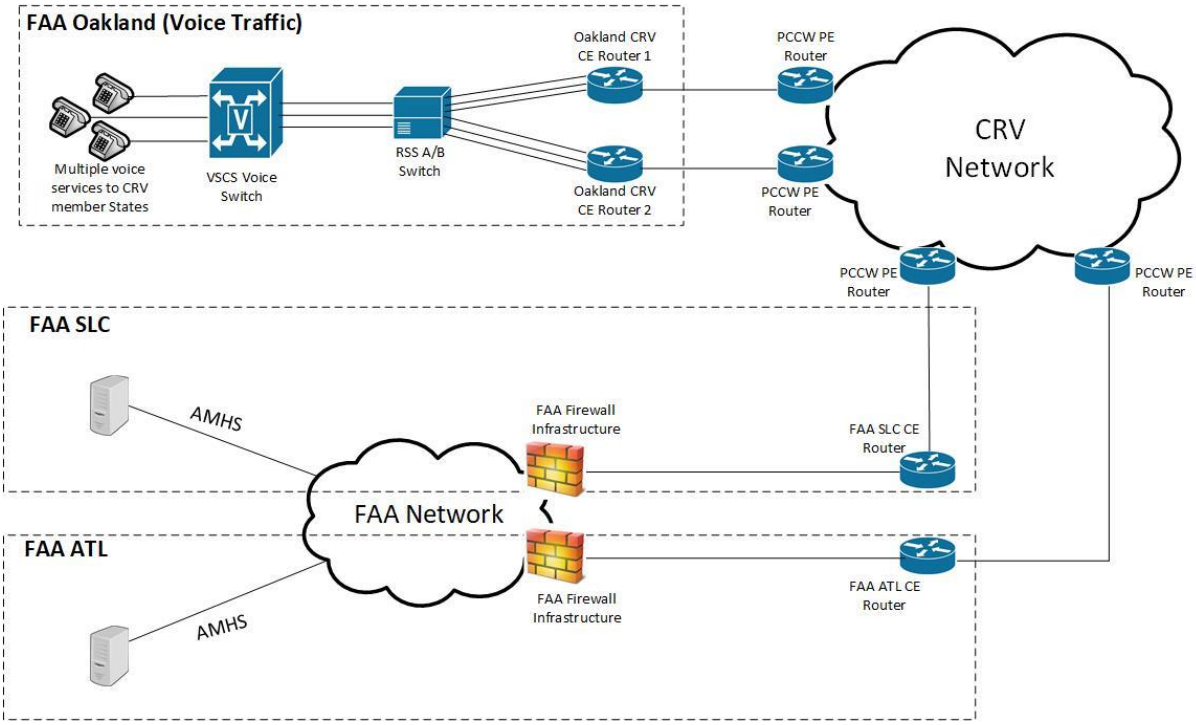
2. DISCUSSION

2.1 The United States FAA (Federal Aviation Administration) has a total of 4 connections into the CRV network: two for data traffic (AMHS) and two for voice traffic.

2.1.1 Diversity for the AMHS traffic is accomplished by incorporating CRV network connections to two geographically different FAA facilities one in Salt Lake City, Utah (SLC) and one in Atlanta, Georgia (ATL). BGP routing advertisements favor SLC as the primary path and ATL as the backup path. Either access can be used in conjunction with the FAA Network to reach the appropriate AMHS application.

2.1.2 Diversity for voice traffic has a different implementation: there are two CRV CE routers located at the Oakland, California FAA facility. The routers have identical analog voice interfaces but have telco connections from different vendors that provide diverse connectivity to the CRV network. One router acts as a primary and the other as a backup. In the event of failure of the primary router or its CRV access path, PCCW has the routers configured to automatically switch the voice traffic to the backup router/path. They also will notify the Oakland facility to change the A/B switch providing the analog connections to the VSCS voice switch.

USA (FAA) CRV Connectivity



2.2 Since Airservices Australia is dependent on the CRV for all data connections, the FAA and Airservices have implemented a backup Internet VPN. In the event of failure of Airservices' CRV access, the Internet VPN can be used for carrying AMHS traffic between the FAA and Airservices. Internet access is provided through the FAA's Oklahoma City facility.

2.3 Although data security is not a requirement of the CRV network, some degree of privacy is accomplished using GRE (Generic Routing Encapsulation) tunnels over MPLS between corresponding CRV users. Each tunnel only allows routing between the member states that the particular tunnel services. For instance, OAK-BNE (Oakland – Brisbane) tunnel only permits IP routing between these two entities. In this way, users can limit traffic only to partners who have agreed to establish tunnels and, in a security incident, could deny traffic from one or more tunnels.

2.3.1 Additional network level security is provided within the FAA's framework by the FAA's firewall infrastructure that terminates external sessions and performs data inspection.

3. ACTION BY THE MEETING

3.1 The meeting is invited to note the information contained in this paper.