International Civil Aviation Organization

THE FIFTEENTH MEETING OF THE COMMON AERONAUTICAL VIRTUAL PRIVATE NETWORK OPERATIONS GROUP (CRV OG/15)

Mumbai, India, 15-19 June 2026

Agenda Item 12: Cyber-safety/security and resilience

ADDITIONAL GUIDELINES FOR ICAO DOC 9855 IN THE CONTEXT OF CRV INTERNET-BASED CONNECTIVITY

(Presented by Singapore / Civil Aviation Authority of Singapore)

SUMMARY

This paper presents the use of public Internet-based connectivity for inter-State aeronautical communication, including Internet-based Common aeRonautical Virtual Private Network (CRV) connectivity using Internet Protocol Security (IPSec) over Authority-provided Internet links. While such configurations provide flexibility where dedicated aeronautical communication infrastructure is not available, they introduce cybersecurity and resilience considerations. This paper provides additional guidance based on the principles of Confidentiality, Integrity and Availability (CIA), supported by Public Key Infrastructure (PKI), to strengthen the security and trust of Internet-based aeronautical communications.

1. INTRODUCTION

1.1 ICAO Doc 9855 provides guidance on the use of the public Internet for aeronautical applications, recognising both its benefits and associated risks.

1.2 In the Asia and Pacific (APAC) region, Internet-based connectivity is increasingly used to support inter-State coordination, including through CRV implementations where dedicated access is unavailable.

1.3 One such implementation is CRV Package D, which enables connectivity to the CRV network using IPSec tunnels over Authority-provided Internet links, without reliance on dedicated terrestrial or satellite access.

1.4 This Working Paper complements ICAO Doc 9855 by providing additional cybersecurity considerations for Internet-based connectivity, with emphasis on maintaining secure, resilient and interoperable aeronautical communications.

BACKGROUND

1.5 ICAO Doc 9855 highlights that the public Internet may be used for aeronautical applications under certain conditions, particularly where dedicated networks are unavailable or as a contingency solution.

1.6 States can connect to the CRV network via Internet-based IPSec tunnels using locally provisioned Internet access.

1.7 While this approach improves accessibility and flexibility, it introduces additional dependencies on public Internet infrastructure, including exposure to varying performance, security risks, and external service providers.

1.8 There is a need to strengthen existing guidance with more detailed cybersecurity considerations to ensure that Internet-based connectivity is implemented in a secure and resilient manner.

2. DISCUSSION

2.1 General

2.1.1 Where Internet-based connectivity is used to support inter-State aeronautical communication, cybersecurity objectives should include:

a) protection against unauthorised disclosure;

b) prevention of message manipulation and spoofing; and

c) resilience against service disruption.

2.2 Confidentiality

2.2.1 Internet-based CRV connectivity utilises IPSec tunnels to secure communications over the public Internet.

2.2.2 While IPSec provides encryption at the network level, additional measures may be required to ensure end-to-end confidentiality, including:

a) mutual authentication mechanisms;

b) strong access control policies; and

2.2.3 In distributed APAC environments, these controls are essential to protect operational data transmitted across shared networks.

2.3 Integrity

2.3.1 IPSec tunnels provide baseline protection for data in transit, but they do not inherently guarantee end-to-end message integrity across interconnected aeronautical systems.

2.3.2 To address this, States may consider:

a) PKI-based authentication mechanisms;

b) digital signatures for critical messages; and

c) cryptographic hashing to detect message alteration.

2.3.3 These measures reduce the risks of message alteration and unauthorised message injection in multi-system environments.

2.4 Availability

2.4.1 CRV connectivity relies on States' Internet infrastructure, introducing dependency on third-party networks and potential exposure to:

a) network congestion;

b) upstream outages; and

c) cyber-enabled disruptions such as distributed denial of service (DDoS) attacks.

2.4.2 To enhance availability, States may consider:

a) redundant Internet providers;

b) diverse paths;

c) monitoring and detection capabilities; and

d) contingency and degraded mode procedures.

2.4.3 Such measures are consistent with Doc 9855 guidance and are particularly important in regions with limited network diversity.

2.5 Cybersecurity Assurance and Coordination

2.5.1 Additional assurance measures may include:

a) validation of secure gateway configurations;

b) periodic vulnerability assessments; and

c) coordinated incident response procedures.

2.5.2 Given the reliance on public Internet infrastructure, cross-border coordination is essential to ensure a timely response to incidents affecting inter-State communications.

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 proposal for requirements for public Internet-based connectivity for inter-State aeronautical communication; and

c) discuss any relevant matter as appropriate.

– – – – – – – – – – – – –