FACTSHEET – ASSESSING AND TREATING IN-SERVICE AIRCRAFT CYBER SECURITY RISKS

AIM

This factsheet guides early adopters through the process for assessing and treating risks to manned aircraft due to cyber hazards, where such an assessment did not occur during the aircraft's Initial Type Certification.

INTRODUCTION

Within the aviation safety domain, cyber security is commonly understood as the protection of information systems against intentional unauthorised electronic interactions. Like many aviation safety authorities globally, both military and civil, DASA has concluded that the Defence Aviation Safety Regulations (DASR) should also regulate cyber security to the extent that it affects aircraft airworthiness. The proposed DASA approach to protection from cyber hazards, together with supporting rationale, is described in the document *Cyber Hazards to Aviation Safety: A DASA Blueprint*, Issue 1.0.

DASA has developed draft regulations on cyber security, *DASR.Cyber* that will be released in a pre-Notice of Proposed Amendment (pre-NPA) format to allow the regulated community to become familiar with the proposed DASA approach to regulation of cyber security. A formal NPA process will be initiated when the level of maturity in understanding and implementation of Cyber Security frameworks within the broader Defence community is such that the DASR.Cyber requirements will be readily understood and able to be adopted by the regulated community. In the interim, the proposed DASA approach may be adopted on a 'voluntary' basis to permit those organisations having the understanding and capacity to do so to implement controls for known cyber security hazards.

To support early adopters of the proposed DASA approach, DASA has released a chapter on protections from cyber hazards in the Airworthiness Design Requirements Manual (ADRM). This chapter contains recommended, rather than essential design requirements. These requirements may become essential upon the eventual release of the DASR.Cyber regulations.

PROCESS FOR ASSESSING AND TREATING CYBER RISKS TO IN-SERVICE AIRCRAFT

The following flowchart outlines the process for the assessment, and subsequent treatment, of Cyber Security Risks to in-service aircraft as it applies to Military Type Certificate Holders, Military Air Operators, and Continuing Airworthiness Managers. The process is intended to apply the standards outlined in the ADRM Section 2 Chapter 12 – *Cyber Security.* Engagement with DASA is encouraged if standards other than those recommended in the ADRM are applied.

		MTCH	Operator	CAM
1	The proposed DASA approach includes the conduct of Cyber Risk assessments for in-service aircraft to identify and subsequently treat identified Cyber hazards. To support those choosing to adopt the proposed approach early, DASA has released an ADRM chapter prescribing requirements for protections from Cyber Hazards. The early adoption of the approach outlined in the ADRM chapter and this factsheet is not mandatory, but does represent credible and defensible good practice for protection from cyber hazards.	Conduct Cyber Risk Assessment?	MAO confirms that the adoption of Cyber regulations in advance of formal release is not warranted, and retains any potential cyber security risks.	
2	If a Cyber Risk Assessment utilizing the preferred DASA approach outlined in ADRM Section 2 Chapter 12 is undertaken, the ADRM requirements must be appropriately recorded in the platform TCB through application for a Major Change to Type Design. MTC Holders may be informed by security risk assessments performed by other N/MAAs in the conduct of the Cyber Risk Assessment process. If security risk assessments by other N/MAAs are relied upon, a Configuration, Role and Environment (CRE) assessment should be undertaken to confirm the applicability of the security risk assessments to the ADF context.	Major Change to Type required Other N/MAA risk assessments used? CRE Assessment		
3	Assessment of Cyber risks is outlined in paragraphs 7-15 of ADRM Section 2 Chapter 12 – Cyber Security. The approach is based upon application of the cyber security process in ED-202A/DO-326A Airworthiness Security Process Specification. Further guidance on conducting the risk assessment can be found in ED-203A/DO-356A Airworthiness Security Methods and Considerations.	Conduct Risk Assessment		
4	After performing the security risk assessment, MTC holders should, in close consultation with the relevant MAO, treat the identified risks in accordance with Defence's seven-step risk management process. Risk treatments may be informed by the treatments considered by other NAAs/MAAs, but recognising the potential for CRE differences and that these risks assessments would not consider Australia's legislated risk management requirements in the WHS Act. If risk-minimising design controls are reasonably practicable, such design controls should be implemented. If the implemented design controls would not eliminate the identified risks, then the MAO should undertake in-service risk management of the residual risks, including the implementation of reasonably practicable operational controls.	Other N/MAA risk assessments used? CRE Assessment Treat Identified Risks	Treat Identified Risks Risks eliminated or otherwise minimised SFARP?	
5	Once identified risks are eliminated or otherwise minimised SFARP, risk treatment should be documented in a Special condition MCRI for insertion into the aircraft TCB and a declaration of compliance with the relevant design requirements used in informing the Cyber Risk assessment process made.	Document Risk treatments in Special Condition MCRI Submit Form 31a with substantiation pack		
6	Upon approval of the change to Type, MTC holders should support the relevant CAM in developing a cyber-relevant continuing airworthiness management framework, by providing any relevant cyber-related instructions for continuing airworthiness developed during the change. In developing the continuing airworthiness management framework, a risk assessment focusing on Continuing Airworthiness aspects should be completed using ED-20A/DO-356A. Specific considerations for continuing airworthiness can be found in ED-204/DO-355.			Develop Cyber-relevant continuing airworthiness management framework

FURTHER INFORMATION

ADRM Section 2 Chapter 12 *Cyber Security*
Cyber Hazards to Aviation Safety: A DASA Blueprint, Issue 1.0 (DPN only)
Pre-NPA Draft Regulations - *DASR.Cyber*
DASA Website - *Cyber Security*

DASA Point of Contact: Design Technologies & Standards (dasa.dtsenquiries@defence.gov.au)