RA 1202 – Cyber Security for Airworthiness and Air Safety

Rationale

Cyber vulnerabilities in Air Systems represent a significant threat to Type and Continuing Airworthiness and Air Safety. Cyber Security for Airworthiness (CSA) measures are required to identify and mitigate against inadvertent or malicious introduction of such cyber vulnerabilities, to maintain Airworthiness. This RA sets out the CSA operational requirements for management of cyber threats throughout the life of an Air System.

Contents

Regulation 1202(1)

Cyber Security for Airworthiness and Air Safety

1202(1) Aviation Duty Holders (ADH) / Accountable Managers (Military Flying) (AM(MF))[1] and Senior Responsible Owners (SRO) **shall** ensure that cyber security threats to Air Safety and Airworthiness are identified, suitably mitigated, and managed through life, appropriate to the level required by the intended use of the Programmable Elements (PE)[2].

Acceptable Means of Compliance 1202(1)

Cyber Security for Airworthiness and Air Safety

1. To mitigate the cyber security threats to Airworthiness and Air Safety during operation and Maintenance of an Air System, ADHs / AM(MF)s and SROs **should** provide direction to operators. This **should** use recognized cyber security guidance aligned to the principles of the MOD Cyber Compliance Framework[3]. ADHs / AM(MF)s / SROs **should** follow:

    a. Radio Technical Commission for Aeronautics (RTCA) DO-355A / EUROCAE ED-204A[4, 5].

    b. JSP 440[6].

2. The ongoing CSA activity **should** contribute to the development and management of the Air System Safety Case[7].

Guidance Material 1202(1)

Cyber Security for Airworthiness and Air Safety

3. To harmonise the approach taken to address Risks to CSA, detailed in RTCA DO-355A / EUROCAE ED 204A, this RA captures the operational considerations for the management of cyber security threats throughout the life of an Air System.

Note:

RA 5890[8] captures the CSA considerations for Air System Type Design and Changes / Repairs to Type Design.

4. Threat of intentional unauthorized electronic interaction will be systematically addressed throughout the life of an Air System. The introduction of changes through advances in computing technology, coupled with developments in tools and techniques, may increase the Risk associated with existing vulnerabilities or expose new ones. The periodicity and work conducted is commensurate with the potential Safety impact associated with the Air System. This RA gives guidance on actions to

[1] Refer to RA 1024 – Accountable Manager (Military Flying).
[2] Note – scope of activity is not confined to PE, but a whole Air System / operations focus, for the management of cyber security threats and vulnerabilities.
[3] A copy of the MOD Cyber Compliance Framework should be requested from the contracting organization.
[4] Refer to RTCA DO-355A / EUROCAE ED-204A – Information Security Guidance for Continuing Airworthiness (note that DO-355A is titled 'Continued Airworthiness', DO-355A still refers to Continuing Airworthiness throughout the standard despite title of document).
[5] DO-355A is a companion to RTCA DO-326A but written for information security In-Service, as opposed to design. The need for such provision is consistent with Defence Standard (Def Stan) 00-970 Guidance Material (Parts 1, 3, 5 and 7).
[6] Refer to JSP 440 – The Defence Manual of Security.
[7] Refer to RA 1205 – Air System Safety Cases.
[8] Refer to RA 5890 – Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design.

Guidance Material 1202(1)

ADHs / AM(MF)s and SROs responsible for all in-service Air Systems, including Legacy Air Systems[9], on understanding what level of vulnerability they may be subject to from cyber threats. Design Change will always be the preference to address cyber vulnerabilities, however it is accepted that action taken in line with this RA may be more feasible to achieve by justified procedural means.

5. **Cyber Compliance.** Management of cyber security for Air Systems In-Service must be consistent with the MOD Cyber Compliance Framework[3], with a specific focus on Air Safety. The framework can be aligned to relevant aspects of DO-355A[4] for Continuing Airworthiness and JSP 440[10]. The framework is based on the requirements of the US National Institute of Standards and Technology (NIST) Cybersecurity Framework, namely Identify, Protect, Detect, Respond and Recover, which must be followed and maintained through the life of Air Systems. This guidance is applicable to PE, Aircraft components, Aircraft network access points, Aircraft weapon systems, Aircraft intelligence systems, Ground Support Equipment, any associated Ground Support Information Systems, and the associated operators. The National Cyber Security Centre (NCSC)[11] also provides guidance on a Cyber Assessment Framework (CAF) that shares the principles of the NIST Framework.

6. **Identify**. The first step, and foundational for effective application of the MOD Cyber Compliance Framework[3], is understanding cyber security Risk in the operational context of any Air System. Risk Assessments, Risk Management strategies, governance, supply chains and asset management are examples of outcomes within this function. DO-355A[4] and JSP 440[6] provide guidance on these aspects, which are key in identifying cyber threats and vulnerabilities that have the potential to impact Air Safety, along with associated operators' responsibilities.

7. **Protect**. Once cyber threats have been identified, the next step is the development and implementation of appropriate safeguards to ensure safe operation of an Air System, by limiting or containing the impact of a potential cyber Incident on Air Safety. Examples of outcomes include access management, storage, transport, training and awareness, Maintenance, protective technology, and Information Management (IM). DO-355A[4] and JSP 440[6] provide guidance on implementation of these processes.

8. Further information for the Assurance of the supply chain may be found in Def Stan 05-138[12] and Def Stan 05-135[13] (eg, counterfeit materiel may not meet the original manufacturer specifications, undermining protection assumptions, and compromised materiel could deliberately introduce vulnerabilities). The NCSC also provides guidance on Assurance of supply chains.

9. **Detect**. Upon introducing protective safeguards, the detect function will be introduced to enable timely detection of cyber security Incidents that may impact Air Safety, such as continuous monitoring and security log files. By understanding the normal behaviour of relevant Air Systems, anomalies can be identified as potential cyber threats to Air Safety. DO-355A[4] and JSP 440[6] provide guidance on the importance of monitoring and detection systems and processes. Guidance on the management of security events that affects aviation Safety can be found in DO-392[14].

10. **Respond**. Once a cyber incident affecting Air Safety has occurred, the level of response is key in supporting the ability to contain the impact, this includes the need for business continuity plans and associated response plans, Occurrence reporting[15], cyber threat analysis, and Continuous Improvement (CI). The MOD requirement for cyber management controls and Cyber Incident response is detailed in JSP 440[6]. Further guidance can be sought through the MOD Cyber Compliance Framework[3] and the NCSC Cyber Assessment Framework[11]. Guidance on the management of security events that affects aviation safety can be found in DO-392[14].

[9] Refer to MAA02 – MAA Master Glossary
[10] JSP 440 focuses on generic cyber security.
[11] www.ncsc.gov.uk.
[12] Refer to Def Stan 05-138 – Cyber Security for Defence Suppliers.
[13] Refer to Def Stan 05-135 – Avoidance of Counterfeit Materiel.
[14] Refer to DO-392 / EUROCAE ED-206 – Guidance for Security Event Management.
[15] Refer to MOD Cyber Incident Reporting – Security Incident Reporting Form and RA 1410 – Occurrence Reporting and Management.

Guidance Material 1202(1)

11. **Recover**. Directly linked to cyber incident response, recovery is essential in maintaining resilience and restoring operational capability. This function minimizes the impact of a cyber incident through timely recovery via recovery planning and CI. Communication and co-ordination with all stakeholders is required to ensure recovery activities are managed and lessons are identified for future improvements, as per guidance in JSP 440[6]. Further guidance can be sought through DO-392[14], the MOD Cyber Compliance Framework[3] and NCSC Cyber Assessment Framework[11].

Intentionally Blank for Print Pagination