DASR.CYBER (EASA-based version)

Following is an initial draft of the DASR.Cyber regulation and is provided to inform early adopters of the proposed DASA approach to protection from Cyber related hazards. Currently, the draft regulations are written as a "horizontal" regulation with applicability across a number of the DASRs. However, the draft regulations as presented are pre-NPA and may undergo significant changes, including to the Implementation method, as DASA continues to engage with the broader Defence Cyber community in the lead up to release of an NPA.

Cyber.005 Scope

(a) This section specifies information security management system (ISMS) requirements that must be met by an organisation to qualify for the issue or continuation of an approval. This section only applies to organisations where DASR.Cyber is listed as a requirement from the relevant section of the DASR.

GM Cyber.005 Scope

DASR.Cyber requires no separate approval to that held by organisations under other DASR. Compliance with DASR.Cyber requirements will be considered as part of an organisation's extant approval.

Cyber.100 Personnel requirements

(a) The accountable manager of the organisation shall have corporate authority to establish and maintain the organisation's ISMS and shall be responsible for:

1. ensuring that all necessary resources are available to manage information security in accordance with this Regulation;

2. establishing and promoting the information security policy specified at Cyber.200 (a)2;

3. nominating a person, or group of persons, who are ultimately responsible to the accountable manager, with the responsibility for managing the compliance monitoring function as part of the ISMS;

4. nominating a person, or group of persons, who are ultimately responsible to the accountable manager, with the responsibility for managing the development, administration, and maintenance of effective information security management processes as part of the ISMS;

5. ensuring that the person, or group of persons, nominated in accordance with Cyber.100(a)3 and 4 have direct access to the accountable manager so that the accountable manager is kept properly informed of compliance and information security matters; and

6. demonstrating a basic understanding of this Regulation.

AMC Cyber.100(a) Personnel requirements

The accountable manager relevant to this DASR should be the same accountable manager as recorded in the approval for the relevant DASR 21, DASR 145, DASR M, Military Air Operator, Air Navigation Service Provider or Aerodrome Operator.

(b) The person, or group of persons, nominated in accordance with Cyber.100(a)3 and 4 shall demonstrate relevant knowledge, background, and satisfactory experience related to aviation information system security and demonstrate a working knowledge of this Regulation.

AMC Cyber.100(b) Personnel requirements - knowledge

The nominated persons should have the skills discussed in Section 11 of DO-355. Section 12 of DO-355 provides guidance on the training requirement for ongoing sustainment of these required skills.

(c) The organisation shall have a process in place to plan the availability of staff to ensure that the organisation has sufficient and appropriately qualified staff to perform the activities related to this Regulation.

AMC Cyber.100(c) Personnel requirements - process

The process should be documented within the organisation's workforce management processes that support any required quality system accreditation.

(d) The organisation shall have a process in place to check a person's identity and previous experience, including, where legally permissible, any criminal records, as part of the assessment of an individual's suitability to implement a security control and/or for unescorted access to sensitive areas within the organisation.

AMC Cyber.100(d) Personnel requirements – personnel identity

The process of verifying a person's identity and previous experience should be detailed within the organisation's workforce management process. For ADF and APS personnel, compliance with Defence's security requirements as detailed in the Defence Security Principles Framework is sufficient. When other staff are contracted to perform functions under this regulation, the process should explain the proposed verification method.

(e) The organisation shall establish the competencies required for personnel involved in the aviation information systems security roles and shall have a process in place to manage those competencies. In addition to the necessary expertise related to the job function, competence must include an understanding of information security management.

AMC Cyber.100(d) Personnel requirements - competencies

Given the immaturity of Defence's cybersecurity expertise, and the need to develop personnel competencies over time, the Authority does not currently provide specific required personnel competencies. The organisation's proposals will be treated on their merits.

Cyber.200 Information security management system

(a) The organisation shall establish, implement, maintain and continuously improve the ISMS aimed at identifying, protecting from, detecting, responding to and recovering from any information security incident which could potentially affect aviation safety. The ISMS shall:

1. define the lines of responsibility and accountability throughout the organisation, including the direct accountability of the accountable manager;

2. contain an information security policy which describes the overall philosophies and principles of the organisation with regard to information security;

3. identify the organisation activities, facilities and resources, as well as the equipment, systems and services it provides, maintains and operates, which could be exposed to information security risks;

4. identify the interfaces with other organisations with which it shares information security risks;

5. take into account the information security risks inherent to the organisation facilities and activities, to the equipment, systems and services it provides, maintains and operates, and to its interactions with other organisations;

6. take into account the information security risks inherent to the use of equipment, systems and services provided to the organisation;

7. the critical information and communications technology systems, data and processes used for military aviation purposes;

8. perform information security risk assessments, both initially and when changes to the security environment occur, of all identified critical systems, data and processes;

9. based on the outputs of the risks assessments, the ISMS shall:

   (i) develop and implement measures to protect the critical systems, data and processes; and

   (ii) continuously identify vulnerabilities and information security risks to the critical systems, data and processes, take actions to mitigate any unacceptable risks and exploitable vulnerabilities, and verify the continued effectiveness of the protection of critical systems, data and processes;

10. describe how the organisation ensures that personnel have the skills and competencies to perform their tasks;

11. include documentation of all management system key processes and procedures, including a process for making personnel aware of their responsibilities and the procedure for amending this documentation;

12. include a function to monitor compliance of the organisation with the relevant requirements, which shall include a feedback system of findings to the accountable manager to ensure effective implementation of corrective actions as necessary; and

13. implement security measures that have been notified by the Authority.

(b) The ISMS shall correspond to the risks inherent to the nature and complexity of the organisation and its activities.

(c) The performance and effectiveness of the ISMS shall be assessed at planned intervals, and appropriate action shall be taken in a timely manner to address inefficiencies and improve its overall performance.

(d) The organisation may integrate the ISMS with other management systems it has already implemented.

AMC Cyber.200 Information Security Management System

The ISMS should cover the range of relevant operational security matters discussed at RTCA DO-355 Information Security Guidance for Continuing Airworthiness. These matters include airborne software, aircraft components, aircraft network access points, ground support equipment, ground support information systems and digital certificates.

Until adequate standards are created for ISMSs relevant to ANS and aerodromes, ANSPs and Aerodrome Operators are to be guided by DO-355. Note that many of the operational

security matters discussed in this publication are also relevant to ANS and aerodromes, with minor tailoring.

The risk assessment material provided in Section 10 should be considered in the context of the Defence seven-step safety risk management process outlined in DASR.SMS and explained in the DASA Advisory Circular 003/2018 Risk Management in the DASP.

(e) By way of derogation from Cyber.200(a), (b), (c) and (d), the organisation may be exempted by the Authority from implementing an ISMS if it demonstrates to the satisfaction of the Authority that its activities, facilities and resources, as well as the equipment, systems and services it provides, maintains and operates, do not pose any information security risks neither to itself nor to other organisations. This exemption shall be based on a documented safety assessment performed by the organisation, and reviewed and approved by the Authority. This exemption will have a maximum duration of 1 year, and can be reissued for subsequent periods, each for a maximum of 1 year, on the basis of a new documented safety assessment as described above for each exemption and for each subsequent period.

Cyber.300 Information security internal reporting scheme

(a) As part of its ISMS, the organisation shall establish an internal reporting scheme to enable the assessment of information security events and vulnerabilities of equipment, process and services.

(b) Through this scheme, the organisation shall:

1. identify the causes of and contributing factors to any information security incident and address them as part of the information security risk management;

2. ensure the evaluation of all known relevant information relating to information security incidents and deviation from procedures and implement a method to circulate the information as necessary.

(c) Any subcontracted organisation shall be able to report through the organisation's internal information security reporting scheme.

(d) The organisation shall cooperate on investigations with any other organisation that has a significant contribution to the information security of its own activities.

(e) The organisation may integrate this reporting scheme with other reporting schemes it has already implemented.

AMC Cyber.300 Information security internal reporting scheme

Internal incident reporting should consider the matters discussed in Section 8 of DO-355.

Cyber.310 Information security external reporting scheme

(a) As part of its information security management system, the organisation shall implement an information security reporting system.

(b) Without prejudice to Cyber.310(a), the organisation shall ensure that any information security incident which may endanger an aircraft, its occupants or any other person(s) is reported to the Authority.

(c) The reports referred to in Cyber.310(a) and (b) shall be made in a form and manner established by the Authority and shall contain all pertinent information about the condition known to the organisation.

(d) A notification shall be submitted to Authority as soon as the condition has been known to the organisation, with a report complying with Cyber.310(c) being submitted to the Authority within 72 hours.

(e) Where relevant, the organisation shall produce a follow-up report to provide details of actions it has taken or intends to take to recover from the incident and actions it intends to take to prevent similar information security incidents in the future, as soon as these actions have been identified. This report shall be produced in a form and manner established by the Authority.

GM Cyber.310 Information security reporting system

The reporting system should provide sufficient information to allow security breaches to be properly investigated.

AMC Cyber.310 Information security reporting system

External incident reporting should consider the matters discussed in Section 8 of DO-355.

The Authority will provide a template with the format and structure of the report and follow-up report. {The Authority is considering whether reports should be provided through Sentinel or through separate mechanisms, stakeholders are invited to provide feedback and recommendations.}

Cyber.400 Contracted activities

(a) The organisation shall ensure that when contracting any part of its activities to external organisations, the contracted activity conforms to the requirements of this Regulation. The approved organisation shall also ensure that any risks associated with such activities are part of the organisation’s ISMS.

(b) When the organisation contracts any part of its activities to an organisation that is not itself certified in accordance with this Regulation to carry out such activities, it shall

ensure that the contracted organisation works under its oversight. The organisation shall ensure that the Authority is given access to the contracted organisation to determine continued compliance with the applicable requirements under this Regulation.

Cyber.500 Record keeping

(a) Records of the ISMS and contracted activities:

1. The organisation shall ensure that the following records are retained, stored and traceable:

   (i) any exemption received in accordance with Cyber.200(e) together with the records of the safety assessment;

   (ii) records of the management system key processes as defined in Cyber.200;

   (iii) contracts for activities defined in Cyber.400;

   (iv) records of events that reveal unauthorised interference with aeronautical information systems.

2. The records specified under Cyber.500(a)1 shall be retained in accordance with the requirements of the Archives Act 1983 (Cth).

(b) Personnel records:

1. The organisation shall ensure that the records of qualification and experience of personnel involved in information security management and compliance monitoring are retained.

2. The records specified under Cyber.500 (b)1 shall be retained for as long as the person works for the organisation, and in accordance with the requirements of the Archives Act 1983 (Cth) after the person has left the organisation.

(c) The format of the records shall be specified in the organisation's procedures.

(d) Records shall be stored in a manner that ensures protection from damage, alteration and theft, with information being identified, when required, according to its security classification level. The organisation shall ensure that the events described under Cyber.500(a)1(iii) are stored using appropriate means to ensure integrity, authenticity and authorised access.

Cyber.700 Information security management manual (ISMM)

(a) The organisation shall provide the Authority with the ISMM and, where applicable, any referenced associated manuals and procedures that contain:

1. a statement signed by the accountable manager confirming that the organisation will at all times work in accordance with DASR.Cyber and with the ISMM. When the accountable manager is not the chief executive officer (CEO) of the organisation, then such CEO shall countersign the statement;

GM Cyber.700(a) ISMM

For military organisations, reference to the CEO should be read as Commanding Officer, Officer Commanding or Director.

2. the information security policy of the organisation as defined in Cyber.200(a)2;

3. a general description of the staff and of the system in place to plan the availability of staff as required by Cyber.100(c);

4. the title(s), name(s), duties, accountabilities, responsibilities and authorities of the person(s) referred to in Cyber.100(a)3;

5. an organisation chart showing the associated chains of accountability and responsibility between all the person(s) referred to in Cyber.100(a)3;

6. the description of the internal reporting scheme as required by Cyber.300;

7. the procedures that specify how the organisation ensures compliance with DASR.Cyber, and in particular:

   (i) the documentation of the management system key processes as required by Cyber.200;

   (ii) the procedures that define how the organisation controls any contracted activities as required by Cyber.400;

   (iii) the ISMM amendment procedure;

8. the details of currently approved alternative means of compliance.

(b) The ISMM shall be amended as necessary to remain an up-to-date description of the organisation, and a copy of it shall be provided to the Authority.

(c) Amendments to the ISMM shall be managed as defined in the procedure referred to in Cyber.700(a)7(iii).

(d) The organisation may integrate the ISMM with other management expositions or manuals it holds, provided there is a clear cross reference that indicates which portions of

the management exposition or manual correspond to the different DASR.Cyber requirements.

Cyber.800 Changes to the organisation

(a) Changes to the reporting lines between the personnel, nominated in accordance with Cyber.100(a)3 and 4, and the accountable manager shall be subject to prior approval by the Authority.

(b) Other changes may be managed and notified to the Authority as defined in a procedure developed by the organisation and approved by the Authority.

(c) Except for changes managed in accordance with a procedure approved by the Authority as described in Cyber.800(b), the organisation shall apply for and obtain an approval issued by the Authority. The application shall be submitted before any such change takes place.

(d) The organisation shall make available to the Authority any information it requests to evaluate the change.

(e) The change shall be implemented only upon receipt of a formal approval by the Authority.

(f) The organisation shall operate under the conditions prescribed by the Authority during the implementation of such changes.

Cyber.900 Findings

(a) After receipt of the notification of findings from the Authority, the organisation shall:

1. identify the root cause or causes of and contributing factors to the non-compliance;

2. define a corrective action plan; and

3. demonstrate the correction of the non-compliance to the satisfaction of the Authority.

(b) The actions required by Cyber.900 (a) shall be performed within the period agreed with the Authority.