

# NOTICE OF PROPOSED RULE MAKING DGTA 01-09

## AAP7001.053 SECTION 2 CHAPTER 1 REGULATIONS 2 AND 3

### PROPOSED SOFTWARE REGULATIONS

#### INTRODUCTION

##### Applicability

1. This proposal is applicable to all aerospace Project Offices (POs), System Program Offices (SPOs) and Authorised Engineering Organisations (AEOs) involved in the design, development, acquisition and management of CIs for aviation software or aviation systems containing software.

##### Purpose

2. The purpose of this NPRM is to advise and seek feedback from stakeholders on the proposal to issue new regulations in AAP7001.053 *Technical Airworthiness Management Manual* related to software compliance findings and software integrity management by AEOs.

##### Consultation

3. The aim of this NPRM is to promulgate background and details of the proposed changes. Advice on how petitions on this proposal are to be presented to the TAR is also provided.

#### PROPOSAL

##### Background

4. **Software Compliance Findings.** The prevalence of software for monitoring and controlling safety related systems and functions is increasing. This means that many more ADF engineers, not just specialists, are being exposed to software compliance finding activities for safety-related systems as part of daily logistics management and project engineering activities. Often, due to limited resources, these compliance finding activities are not planned for and not commenced until too late in the project lifecycle. The outcome is that shortfalls in the compliance finding may lead to unknown risks or shortfalls in the level of safety of the aviation system. Software compliance findings are challenging engineering assessments which require very specific competency sets only obtained through extensive training and experience. Therefore, planning for and conducting a software compliance finding usually requires specialist input from DGTA and supporting technical specialists.

5. These factors, amongst others have contributed to substantial challenges with the design acceptance of software on numerous recent acquisitions and modifications. In addition to POs and SPOs struggling with the challenges of software compliance findings, there has been a commensurate impact on the TAR's confidence of the outcomes of software compliance findings. This has resulted in the necessity to resolve numerous software compliance finding shortfalls, often late in project lifecycles, which places pressures on project cost and schedule constraints.

6. On the basis of aforementioned limitations and shortfalls, the TAR is now proposing regulations for software compliance findings to ensure that acceptable compliance finding plans are in place for projects making software compliance findings, and that these plans identify an acceptable scope and level of ADF and additional technical specialist involvement as required.

7. **Software Integrity Management.** Software integrity is the degree to which the aviation system hosting the software achieves its required safety features under all operating conditions within a defined operating intent. Management of software integrity, in both the initial development of aviation software, as well as the modification and sustainment of aviation software is fundamental to the extent to which software integrity meets relevant safety benchmarks.

8. DGTA routinely audits ADF and contractor AEOs undertaking the CI management of aviation software or aviation systems containing software. In recent years, DGTA has identified the following consistencies in Corrective Action Requests (CARs) and Observations on software audits with respect to software integrity management. Specifically there are limitations to:

- a. the satisfaction of objectives of TAR recognised software assurance standards or equivalent arrangements acceptable to the TAR;
- b. the extent of application of software safety analysis to aviations systems;
- c. the explicit management of software resident within aviation system configuration items;
- d. the identification and qualification of software tools supporting software development and management;
- e. suitable arrangements for software load control (as defined by RTCA/DO-178B); and
- f. to the configuration management of software versions installed on items returned from repair venues, particularly overseas repair venues.

9. On a number of occasions the ADF has only learned retrospectively of potentially serious software shortfalls of safety-related aviation systems. This has often been the result of limitations in the frameworks and associated procedures for problem reporting, assessment and tracking, often amongst several different contractor and ADF organisations.

10. On the basis of these limitations and shortfalls, DGTA is now proposing regulations on software integrity management to ensure appropriate procedures are in place to assure software integrity of new or modified aviation software, and to provide continuing assurance of the software integrity of accepted software.

### **Benefits of the proposed regulation**

11. This NPRM proposes the addition of new software regulations to be included in AAP7001.053 *Technical Airworthiness Management Manual*. The new regulations are intended to make explicit the TAR's expectations for software compliance findings by ADF POs and SPOs, as well as to ensure that AEOs have in place acceptable procedures for software integrity management.

12. The benefits of the proposed regulation change on Software Compliance Findings are to:
- a. provide POs and SPOs with greater clarity on the TAR's expectations for software compliance findings, particularly for software with potentially severe safety consequences;
  - b. assure that software compliance findings for software with potentially severe safety consequences meet the TAR's expectations;
  - c. provide greater consistency of ADF software compliance findings across all POs and SPOs;
  - d. provide more explicit consideration of the competencies required to undertake challenging software compliance findings on safety-related aviation systems; and
  - e. ensure POs and SPOs have acceptable plans in place prior to undertaking software compliance findings.
13. The benefits of the proposed regulation change on Software Integrity Management are to:
- a. ensure AEOs have appropriate plans in place for software integrity management;
  - b. ensure that acceptable procedures are in place for assuring software integrity of new or modified software, including ensuring that appropriate software safety and assurance benchmarks are met, and that acceptable arrangements exist to support the ADF making software compliance findings in support of design acceptance of aviation software;
  - c. ensure that acceptable procedures are in place to provide continuing assurance of the software integrity of accepted software, including facilitating appropriate AEO, DAR and TAR responses to errors, faults and failures of software which potentially result in large reductions in safety margins (defined consistently with the interpretation of Reg 2.2.3.a.(3).(ii)); and
  - d. reduce the number of Corrective Action Requests (CARs) and Observations raised during DGTA compliance assurance activities related to regulatory compliance aspects of the management of software by AEOs.

**Proposed new AAP7001.053 software regulations**

14. The proposed regulations are included at Enclosure 1.
15. Substantial guidance on compliance with these regulations already exists in AAP7001.054 Section 2 Chapter 7 *Software for Airborne and Related Systems*, and AAP7001.054 Section 2 Chapter 17 *In-service Management of Software for Airborne and Related Systems*. The current guidance should be sufficient to permit POs, SPOs and AEO to achieve compliance with the proposed regulations, as the new regulations do not introduce any new concepts or activities that were not previously expected of engineering organisations involved with aviation system software.
16. However to ensure smooth introduction of these new regulations, the aforementioned guidance will be further expanded in forthcoming amendments, due for release by the end of

2009 and to coincide with the publishing of these regulations. Specifically the following additional guidance is being developed:

- a. Expansion of DGTA's guidance for software compliance findings at Annex C to AAP7001.054 Section 2 Chapter 7.
- b. Release of a DGTA Paper on Software Design Acceptance, including model approaches for undertaking software compliance findings under common scenarios.
- c. Redevelopment of guidance on the Software Assurance Matrix (SAM), formerly Software Assurance Task Matrix (SATM), for inclusion in the AAP7001.054 Sect 2 Chapter 7.
- d. Extension of the AAP7001.054 Section 2 Chapter 7 Software Management Plan (SMP) (Acquisition) template for use as an AEO SMP template for inclusion as an Annex to Section 2 Chapter 17 for use by AEOs for drafting an SMP as per the proposed regulations.

17. **Transition to software regulations.** The following arrangements are intended to apply regarding effect dates for the regulations:

- a. Regulation 2.2.12 Software Compliance Findings will come into immediate effect (upon publishing) for all existing and new acquisitions and modifications.
- b. Regulation 3.5.3 will come into immediate effect (upon publishing) for any new AEOs or changes to the scope of existing AEOs involving software. Existing AEOs will be given a period of 6 months from the date of publishing in which to draft and provide to DGTA the requisite SMP and associated procedures for TAR approval (using the SMP template provided by DGTA).

## **HOW TO SUBMIT COMMENTS ON THIS NPRM**

### **Format**

18. Responses to the NPRM are to be submitted electronically using the NPRM Comments Sheet (Annex A), or as published on the DGTA Intranet and Internet websites. Responses can be e-mailed to [DG TANPRM@defence.gov.au](mailto:DG TANPRM@defence.gov.au).

### **Timing**

19. Comments to NPRM DGTA 01-09 are to be received by close of business 06 Nov 09.

### **Resource Implications**

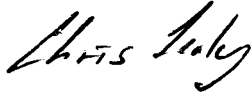
20. Stakeholders are requested to include within their responses, an assessment or comment on the anticipated resource implications posed by the proposed change.

### **Additional information**

21. Additional information concerning this NPRM is available from SQNLDR Derek Reinhardt (03) 9256 3746 or [derek.reinhardt@defence.gov.au](mailto:derek.reinhardt@defence.gov.au).

**DISPOSITION OF COMMENTS RECEIVED**

22. A Summary of Responses will be prepared and published on <http://intranet.defence.gov.au/dgta/> and <http://www.defence.gov.au/dgta/NPRM.htm>. DGTA-ADF will not individually acknowledge or respond to comments or submissions, however the names of all contributors will be acknowledged in the summary of responses.



**C.A. FEALY**  
Captain, RAN  
Director Aviation Regulation  
Directorate General Technical Airworthiness – ADF  
Tel: (03) 9256 3651

13 Oct 2009

**Annex:**

A. NPRM DGTA 01-09 - Comment Sheet

**Enclosure:**

1. Proposed Software Regulations for AAP7001.053

**NPRM DGTA 01-09 Comment Sheet**

AAP7001.053

**PROPOSED SOFTWARE REGULATIONS**

Please return this response sheet by 06 Nov 09, via email attachment to DGTANPRM@defence.gov.au.

Please indicate your acceptance or otherwise of the proposal by ticking the appropriate box below.

Any additional constructive comments, suggested amendments or alternative action will be welcome and may be provided on this response sheet or by separate correspondence.

- The proposal is acceptable without change.
- The proposal is acceptable but would be improved if the following changes were made:  
(Please provide explanatory comment).
- The proposal is not acceptable but would be acceptable if the following changes were made: (Please provide explanatory comment).
- The proposal is not acceptable under any circumstances. (Please provide explanatory comment).

**Explanatory Comments:**

**Assessment/Comment on Resource Implications:**

**Respondent Details**

Your name: \_\_\_\_\_

Position and Organisation: \_\_\_\_\_

Address: \_\_\_\_\_

Tel or Email: \_\_\_\_\_

**Do you consent to your name as a respondent to this NPRM: YES  NO**

Signed: .....

Date: .....

## Regulation 2

### 2.2.12 Software Compliance Findings

- a. The DAR shall ensure that a Software Compliance Finding Plan is documented to support the Design Acceptance of new or modified aviation software.
- b. The DAR shall ensure that the software compliance finding is conducted in accordance with the Software Compliance Finding Plan.
- c. The DAR shall obtain TAR approval of the Software Compliance Finding Plan if the worst credible failure condition of the new or modified aviation software is more severe than Minor (as defined in AC25.1309) or Marginal (as defined in MIL-STD-882C).
- d. Where TAR approval of the Software Compliance Finding Plan is required in accordance with Regulation 2.2.12.c, that TAR approval shall be in the form of either:
  - (1) approval of the Software Compliance Finding Plan for a specific acquisition or modification, or
  - (2) a standing approval of the Software Compliance Finding Plan for on-going software compliance findings for in-service changes to previously accepted aviation software.
- e. In order to obtain TAR approval of the Software Compliance Finding Plan, the DAR shall submit to the TAR, a Software Compliance Finding Plan that:
  - (1) was prepared in accordance with AAP7001.054 Section 2 Chapter 7 Annex C;
  - (2) documents an acceptable approach to implementing the key issues identified in AAP7001.054 Section 2 Chapter 7;
  - (3) defines acceptable software safety and assurance benchmarks, including the application of the TAR recognised software safety and assurance standards in AAP7001.054 Section 2 Chapter 7, or alternative standards approved by the TAR;
  - (4) nominates a compliance finding agency that has the requisite competencies to undertake the compliance finding, or includes details of arrangements to supplement the compliance finding agency competencies using appropriately qualified technical specialists;
  - (5) identifies an acceptable scope of software lifecycle data for evaluation against software safety and assurance objectives;
  - (6) identifies acceptable arrangements for the access to and evaluation of software lifecycle data;
  - (7) defines an acceptable level of Commonwealth involvement; and
  - (8) if compliance finding relies on prior acceptance, includes evidence relating to prior acceptance of the software and any additional supporting information required by Regulation 2.2.7 - *Recognition of Prior Acceptance*.

## **Regulation 3**

### **3.5.3 Software Integrity Management**

- a. Each applicant responsible for the Configuration Item management of aviation software or aviation systems containing software shall establish and maintain a Software Integrity Management System.
- b. The Software Integrity Management System shall include:
  - (1) a Software Management Plan;
  - (2) procedures to assure software integrity of new or modified software; and
  - (3) procedures to provide continuing assurance of the software integrity of accepted software.
- c. The Software Integrity Management System shall ensure that:
  - (1) the Software Management Plan is issued by the SDE and approved by the TAR;
  - (2) any amendment to the Software Management Plan:
    - (i) has been approved by the DAR; and
    - (ii) where there are additions to the Configuration Items listed in the Software Management Plan or a reduction to the assurance of software integrity has been approved by the TAR.
  - (3) all aviation software Configuration Items being managed by the applicant, including the associated software assurance level, are identified in the SMP;
  - (4) all software tools being used by the applicant, including the tool categorisation and qualification, are identified in the Software Management Plan;
  - (5) the Software Management Plan is reviewed as necessary and at least on an biennial basis;
- d. The procedures to assure software integrity of new or modified software shall:
  - (1) ensure software development of safety related software is conducted to satisfy the objectives of either a TAR recognised software assurance standard, or a Software Assurance Matrix approved by the TAR;
  - (2) require a software safety program be established for the development of all software that is safety related;
  - (3) ensure a Plan for Software Aspects of Certification, or equivalent document, is submitted to and approved by the TAR prior to the commencement of development if the worst credible failure condition of the new or modified aviation software is more severe than Minor (as defined in AC25.1309) or Marginal (as defined in MIL-STD-882C);

- (4) provide for direct Commonwealth oversight of all software changes to safety-related systems to permit the Commonwealth to make software compliance findings;
  - (5) implement acceptable arrangements for software load control.
- e. The procedures to provide continuing assurance of the software integrity of accepted software shall:
- (1) implement a framework for software problem reporting, problem assessment, tracking of problem reports and corrective actions to ensure that safety-related errors, faults and failures are identified and resolved within acceptable timeframes;
  - (2) ensure the DAR and TAR are notified of any errors, faults or failures of aviation software which potentially result in a large reduction in safety margins;
  - (3) describe configuration management processes of all aircraft software, including configuration status accounting and reporting of software versions installed on items returned from repair venues.