

SUMMARY OF RESPONSES TO NPRM DGTA 03-09

AAP 7001.054 SECTION 2 CHAPTER 24

FLIGHT AND MISSION PLANNING SYSTEMS

INTRODUCTION

General

1. This Summary of Responses outlines DGTA's responses and intended actions to the comments received for NPRM DGTA 03-09 *Flight and Mission Planning Systems* and finalises the consultation process. Any person having views or arguments to support an appeal against the decisions documented in this Summary of Responses may petition DGTA to consider such an appeal.

Background

2. On 23 Dec 09, DGTA-ADF released NPRM DGTA 03-09 for comment. The NPRM proposed new guidance on the technical approval, service release and management of Flight and Mission Planning Systems. The period for comment on the proposals contained in NPRM DGTA 03-09 closed on 20 Feb 10.

3. There were 10 responses to the NPRM, providing representation from both Commonwealth and Commercial AEOs. A list of respondents who have consented to their names being published has been included at annex A.

ANALYSIS OF COMMENTS

General

4. A wide range of constructive comments has assisted with refining and improving the robustness of the proposed Flight and Mission Planning Systems chapter. The disposition of comments is shown in Figure 1.

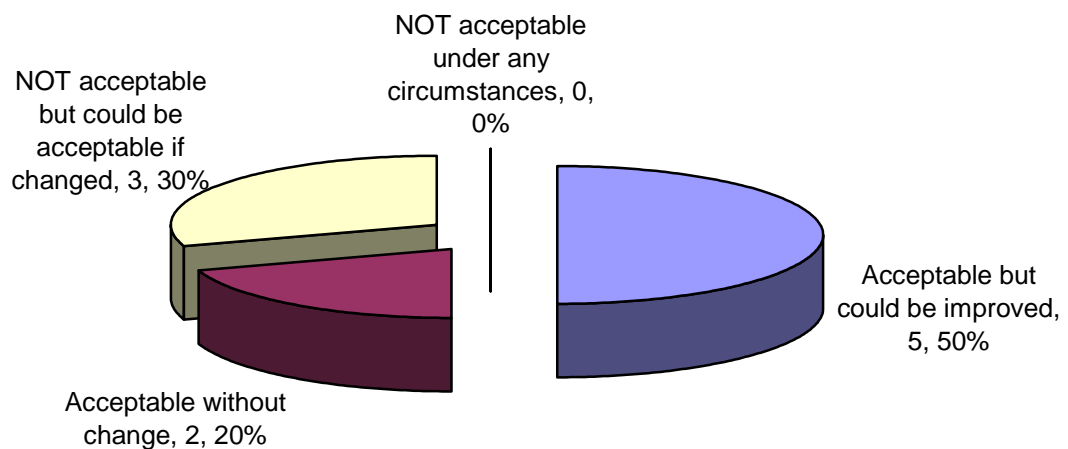


Figure 1: Disposition of Comments

5. Overall, 70% (total 7 of 10 responses) were in support of the proposed Flight and Mission Planning System chapter and 30% (total 3 of 10 responses) would be in support of the proposed chapter if some changes were made. Therefore, DGTA has assessed that there is widespread agreement that the proposed chapter is warranted. However, most respondents suggested that improvements were required, and these ranged from minor grammatical improvements through to suggestions for new inclusions. The suggestions for improvements to the proposed chapter have been specifically analysed throughout this Summary of Responses and minor changes to the proposed chapter incorporated to resolve relevant areas identified for improvement.

6. DGTA intends to publish the Flight and Mission Planning System chapter with changes incorporated from the specific comments presented in this Summary of Responses. The amended chapter is presented at enclosure 1.

RECEIVED COMMENTS

7. The following comments were received from the respondents. Note that multiple similar comments have been grouped in general terms for the sake of brevity and clarity of the DGTA Summary of Responses. A DGTA analysis and response is included against each group of comments, and the resulting disposition of the comments is presented.

8. Please note that all references in this document to paragraph numbers in the proposed chapter are references to the version of the proposed chapter that was included as enclosure 1 to NPRM DGTA 03-09. As additional paragraphs have been added as a result of the responses to NPRM DGTA 03-09, the paragraph numbers in the proposed chapter as presented at enclosure 1 to this document do not necessarily align with the responses to comments below.

Comment – Recognition of Prior Acceptance (RPA)

9. The comments received were as follows:

- a. *My overall concern with this NPRM is, for MPS acquired with MAA oversight, what appears to be an inconsistent approach to the issue of RPA compared to that described in NPRM 02-09. The premise of NPRM 02-09 is that a CRE comparison is the fundamental driver in determining the applicability of any compliance finding (as an element of the prior acceptance) made by the NAA.*
- b. *My reading of NPRM 03-09 (paras 18-19 & 37-42), is that the only time a CRE comparison is relevant is for the acceptance of a non-common component of the MPS. So the fundamental driver in determining the applicability of any prior acceptance is whether the configuration is common. For those components of the MPS that are common, the fact that we may have a substantially different CRE to that of the MAA does not appear to be relevant. This seems to be inconsistent with the principles of informed RPA elaborated in NPRM 02-09 (particularly paras 24-25, most particularly 24c).*
- c. *It is possible that the guidance on retention of risk for MPS common components is addressing this. If that is the case, then surely the risks needs to be examined from the point of view of applicability and acceptability to the ADF given our CRE. Presumably it is possible that the MAA has retained risk that they consider acceptable but may not be acceptable to the ADF given our a/c CRE differences. If this is the intent of 40(b)(3) then I believe the CRE differences needs to be emphasised.*

- d. *In summary, I think the document would benefit from some more guidance for the non-MPS experts on why a CRE comparison is not relevant to common components of the MPS and should emphasise that examination of risks retained by the MAA needs to be done in the context of the ADF CRE.*
- e. *Para 19. The definition “assessment” for design features is not clear. Some guidance on the expected level and depth of assessment for components such as error detection is suggested – otherwise the task could easily become a project in its own right.*

Response

10. The proposed chapter is intended to be consistent with NPRM DGTA 02-09 and RPA guidance. An assessment of Configuration, Role and Environment (CRE) differences is required when applying RPA to common MPS components. While this is briefly discussed in paragraph 19 of the proposed chapter it was inadvertently omitted from paragraph 40. The proposed chapter will be amended to remove this inconsistency.

11. The assessment of design features described by paragraph 19 of the proposed chapter is intended to confirm that the design features of the MPS are appropriate for the aeronautical data that will be processed. This assessment should seek to determine whether the MPS has the necessary design features to assure that errors are not introduced to the aeronautical data. A direct assessment of the integrity of the design features is not required as long as RPA can be relied upon. Paragraph 19 also refers to paragraphs 37 through 42 as providing additional information on the assessment approach.

Disposition

12. The proposed chapter will be updated to clarify the need for a CRE assessment for common MPS components. This amendment will remove any inconsistency between the proposed chapter and RPA guidance.

Comment – Identification and Treatment of Risks

13. The comment received was as follows:

- a. *Retrospective application represents a serious risk to in-service systems. Ultimately the DAR will decide on the adequacy of new or existing systems. However, some aircraft may be grounded or the system made unserviceable and circuit breakers pulled or the equipment removed dependent on the level of unknown risk the DAR and OAR are willing to accept. If retrospective assessment determines the MPS system non-compliant then OEM customisation is expensive or not given.*

Response

14. An MPS that is not appropriately assured for the functions it performs presents a risk to the airworthiness of an aircraft whether or not that risk is identified. Conduct of the analysis described in the proposed chapter will not create risks to airworthiness, though it may identify them. Identifying and analysing risks to airworthiness enables treatments to be applied. There are a range of treatments that may be suitable depending upon the nature of the risk, including design changes, additional verification activities, procedural workarounds and risk retention. Implementation of some of these treatments may have significant cost, schedule and

capability implications and this would need to be carefully weighed against the benefit to be gained.

Disposition

15. The need to treat risks to airworthiness posed by a failure to meet a suitable safety benchmark is not unique to MPS. The proposed chapter establishes a suitable safety benchmark for ADF use of MPS. Shortfalls against a safety benchmark can be treated in accordance with existing system safety or aviation risk management processes. The above response will not result in changes to the proposed chapter.

Comment – Access to Data

16. The comments received were as follows:

- a. *Reliance on RPA to satisfy adequate safety and reliability of an MPS is discussed with known limitations dues to ITARs, Intellectual Property etc.*
- b. *There will be reluctance by OEMs to reveal their intellectual property and this is usually demonstrated by protracted communication or none to absorb time. Resulting in delays to meet DAR and TAR levels of data acceptance and milestones.*
- c. *Specific guidance on evidence required to meet TAREG 2.2.7b(4) (changed to 2.2.7d(4) in NPRM 02/09). This is necessary as regularly acquisition projects using RPA centrally in their DAS will acquire the platform and MPS separately, as CISSO manages JMPS and PFPS on a whole of government basis while the platform is acquired by the nominal Project Office. Access to evidence and data may be impacted by these acquisition boundaries.*
- d. *Para 40(b). With MOTS MPS such as PFPS acquired through FMS, has the ADF been able to access the information in sub-paras (1) to (4)? Is this a realistic requirement for the suggested ADF assessment activity?*
- e. *Para 28. In the absence of an accredited data supplier, type 2 LOA may require access to proprietary data. This could present possible contractual/access issues if not addressed early in a project's lifecycle – suggest a note to this effect be included.*
- f. *Para 37 RPA – Release of FMS data. WRT RPA, same set of concerns as per RPA NPRM comments. In particular the releasability of certification support products from the US under FMS arrangements is often beyond the control of the relevant PO/SPO – even if agreements to supply the data had been originally made.*

Response

17. Obtaining access to sufficient data is a challenge faced by many projects, particularly for established contracts that do not include sufficient data access provisions and acquisitions that are subject to foreign disclosure restrictions. As with all aviation materiel, an assessment that an MPS is safe and fit for purpose depends on access to sufficient data, either to support a direct technical assessment or to apply RPA. Without access to sufficient data, the ADF cannot be confident that an MPS is safe and fit for purpose.

18. The challenges of accessing sufficient data to support the Design Acceptance process will vary with the acquisition strategies being employed. These challenges are not unique to MPS. The extent of data required for MPS is similar to that required for other aviation software items, though it is acknowledged that this may be beyond the data available to projects that are already on contract or already subject to foreign disclosure restrictions.

19. DGTA is aware that obtaining access to sufficient data can be a significant challenge for some projects. However, the purpose of AAP 7001.054 is to define airworthiness requirements that set an appropriate benchmark for safety. It would be inappropriate to degrade a safety benchmark simply because a number of projects may not be able to demonstrate that a system meets the benchmark due to data restrictions. AAP 7001.054 does, and should, describe acceptable levels of safety that acquisition organisations should strive to satisfy. When this cannot be achieved, an appropriate authority would be required to retain risk if the system is to be operated.

Disposition

20. Although obtaining access to sufficient data can be a challenge, it is not one that is unique to MPS. The above responses will not result in changes to the proposed chapter.

Comment – Consistency with Chapter 22 EFBs

21. The comments received were as follows:

- a. *The new chapter has some inconsistencies with the Sec 2 Chap 22 (EFBs). The Assurance requirements imposed by the EFB chapter (para 15a) for portable EFBs hosting Type B applications only drive a software assurance level of 'D'. Since many ADF Mission Planning System applications would be equivalent to Type B EFB applications (performance calculations, chart viewers, checklists). In fact this chapter directly states that from a functionality perspective, many MPS's such as PFPS, would generally be considered Type B applications. Why then, does the new MPS chapter potentially impose additional certification requirements on MPS's, over and above what would be required for EFB Type B applications (e.g. need for data criticality analysis, differing assurance levels for each category of criticality, etc.). DGTA would need to clarify which of the chapters would apply to MPS's such as PFPS, JMPS, ..., ..., etc.*
- b. *Para 46. Where it states 'fortunately, these measures are usually only required if the MPS applications are hosted on an EFB' is not entirely correct (as CAST 14 applies to integrated EFBs or portable EFBs hosting Type C applications). This should be clarified.*

Response

22. There are a number of systems within the ADF that could be considered both an MPS and an EFB. In these cases, the system must be appropriately assured to perform all assigned functions and both the EFB and MPS chapters would apply. Where one policy imposes higher assurance requirements than the other, the higher requirements must be satisfied.

23. The primary difference between the EFB and MPS chapters is the hazard analysis technique used to identify necessary design assurance requirements. The EFB chapter clearly allocates out common EFB functions to different 'Types' which in turn translate to assurance requirements. The MPS chapter, on the other hand, defines only a framework that enables the identification of assurance requirements: it does not directly assign them.

24. To further explain this, consider weight and balance calculations. Weight and balance calculations are a function that may be performed by either an EFB or an MPS. Under the EFB chapter, weight and balance calculations are a Type B application (assuming a civilian like application) requiring assurance to DO-178B Level D. Under the MPS chapter, the weight and balance calculation function must be assigned a severity and have treatments applied as identified in Table 3 of the proposed MPS chapter. The MPS chapter does not directly assign a severity to weight and balance calculation failures, but does describe a framework within which a severity could be assigned. Whether the MPS chapter imposes additional certification requirements would then depend on which severity is assigned.

25. It should also be noted that the EFB chapter imposes a number of requirements on an EFB that would not be imposed on an MPS. Although they may perform similar functions, the use of an EFB in flight necessitates consideration of, among others, reliability, availability and aircraft interface that are not necessarily airworthiness issues for an MPS.

26. CAST 14 requires a number of issues to be resolved before a COTS operating system can be used in an airborne environment. These issues do not need to be resolved if the hosted software application is not going to be used in an airborne environment provided the verification of the software application accounted for the configuration of the COTS operating system. As an EFB, by definition, is used in the airborne environment, the issues identified by CAST 14 must be resolved. The CAST 14 issues do not need to be resolved for an MPS that is never used in an airborne environment (i.e. one that is never used as an EFB).

27. The statement in paragraph 46 ‘fortunately these measures are usually only required if the MPS applications are hosted on an EFB’ was intended to be read within the context of the chapter. The measures in CAST-14 are required for all EFBs, though discussion of EFBs is beyond the scope of the MPS chapter (hence a reference to the EFB chapter is provided). The discussion of CAST-14 in the proposed chapter is restricted to consideration of MPS.

Disposition

28. The proposed chapter will be amended to more clearly articulate that, where a system is both an MPS and an EFB, both the MPS and EFB chapters would apply.

Comment – Data Quality

29. The comment received was as follows:

- a. *Para 9. One of the key steps in the FAA guidance set forth in DO-200A is the specification of data quality requirements at each phase of the Aeronautical Data chain. This para only focuses on the assurance level as derived from a functional safety assessment of the aircraft (for functions associated with the aeronautical data in question). The FAA guidance in fact only considers the assurance level as a subset of data quality requirements which also includes accuracy, resolution, assurance level, traceability, timeliness, completeness and format requirements. Since this chapter leverages heavily on FAA guidance, it is pertinent that this important step in the approach taken by the FAA is stated and clarified in this chapter.*

Response

30. The purpose of the proposed chapter is to define requirements for assessing the contribution of MPS to aeronautical data processing. It is acknowledged that there are other data quality attributes that are not treated by the proposed chapter. Generally, this is because

an MPS plays only a minimal role in achieving that attribute (e.g. an MPS has very little to do with the timeliness of aeronautical data). If the proposed chapter was intended to cover the entire aeronautical data processing chain, then the inclusion of such attributes would be warranted.

31. However, MPS may have a greater role in achieving data quality attributes than is clearly articulated by the proposed chapter. An MPS can degrade the accuracy, resolution and completeness of aeronautical data. The ADF should assure that an MPS does not degrade the accuracy, resolution or completeness of aeronautical data unless such degradation is required for systems compatibility or is tolerable (e.g. the resolution of aeronautical data at the input to the MPS is higher than that required by the target aircraft system).

Disposition

32. The proposed chapter will be amended to describe the role of an MPS in maintaining pertinent data quality attributes.

Comment – Flight Performance Models

33. The comment received was as follows:

- a. *Para 49. There is no guidance as to the software assurance 'practice' or software assurance level that it recommends to Flight Performance Models (FPM). DO-201 will not help in the classification of this data, and output of this analysis will not lead to any on aircraft failure. Using that reasoning and the limited guidance offered here, one could easily argue that no software assurance need be applied at all. If DGTA have a level of assurance in mind, it would be best if they provide more guidance in what they consider to be an acceptable assurance level for FPMs.*

Response

34. The level of assurance required for flight performance models will be driven by the criticality of the aeronautical data the flight performance model is used to generate (e.g. take off and landing data, fuel usage, etc). In this regard, a flight performance model is no different to any other aspect of an MPS or link in the aeronautical data processing chain. DGTA cannot identify a level of assurance that would be applicable to all flight performance models as the required level of assurance is context dependent.

35. Contrary to the above response, a flight performance model can have a negative impact on the safety of an aircraft. For example, an MPS may use the flight performance model to perform take off and landing data calculations. In this example, an erroneous flight performance model could contribute to erroneous take off and landing data calculations and the severity of the calculation failure modes can also be assigned to the flight performance model. DGTA would expect a flight performance model to be included as an MPS component in an assessment structured similarly to Table 4 of the proposed chapter. The MPS functional guideword 'Generate' is likely to be the most appropriate. The assurance requirements for a flight performance model can then be identified using Table 3 of the proposed chapter.

Disposition

36. The proposed chapter will be updated to reflect that the level of assurance required of flight performance models is to be determined by the criticality of the functions to which the flight performance model contributes.

Comment – Inadvertent Modification

37. The comment received was as follows:

- a. *Para 9.f(2&3). When this line discusses 'inadvertent modification', is this by the user, system or both? And what about where data has to be modified to meet on-board system requirements? i.e. navaid names may require modification to ensure uniqueness or to meet on-board formatting requirements (e.g. minimum characters in beacon name).*

Response

38. The focus of the proposed chapter is the technical contribution of MPS to aircraft functional failure conditions. This contribution may arise from flaws in the MPS components, or the failure of the MPS to detect operator errors that are reasonably foreseeable and detectable. There is a wide range of operator action that can lead to similar results for which the MPS could never account (e.g. incorporating a valid, but incorrect, number of passengers into a weight and balance calculation). Modification of data to meet on-board system requirements should not be considered inadvertent modification and the correctness of such changes should be assured.

39. In specific response to the above comment, 'inadvertent modification' in paragraph 9.f(2&3) refers to both inadvertent modification by the user and inadvertent modification by the system. However, only reasonably detectable inadvertent user modifications (e.g. entry of out of range data) need to be considered during the technical assessment. Modifying data to meet on-board system requirements should not be considered inadvertent modification.

Disposition

40. Paragraph 9 only summarises the FAA policy with regard to aeronautical data processing. It has been included only to provide background to the generation of the ADF policy for MPS, it does not actually describe the ADF policy for MPS. The above response will not result in changes to the proposed chapter.

Comment – Compliance Plans

41. The comment received was as follows:

- a. *DO-200A extensively covers the development of a Compliance Plan. This chapter should provide guidance in the ADF context for submission of a compliance plan (or equivalent) to DGTA. Currently, there is no advice as to how this should be documented (i.e. in a PSAC, a Certification Package, within a projects AMP or TCP, etc) Also, evidently classification of information criticality is required before the provision of a complete certification package that would be provided just prior to system acceptance or use in service. By what means would information criticality classification be agreed by DGTA?*

Response

42. DGTA does not intend to constrain the form in which the MPS technical assessment is communicated. The proposed chapter provides example technical assessment structures, but this is not intended to restrict other approaches that may be appropriate. However, it would almost certainly be inappropriate to present the details of an MPS certification plan in an AMP, TCP or PDAS (though these documents may provide summaries).

43. The best method, but not the only method, for seeking DGTA agreement with a certification strategy is to conduct an MPS component functional assessment such as the example provided in Table 4 of the proposed chapter. It would probably be best for this type of assessment to be contained in a standalone document.

44. The classification of information criticality is required well before the timeframe suggested by the above respondent. The classification of information criticality will drive software assurance requirements on the MPS components. The software assurance requirements translate into design and verification objectives that must be satisfied. As such, the classification of information criticality should occur prior to the commencement of MPS development. This is similar to the conduct of a system functional hazard assessment prior to, or early in the process of, system design.

45. When reviewing the criticalities that have been assigned, DGTA will as far as is possible draw on existing FAA policy considered in the context of ADF system use. The allocation of EFB functions to application types is an example of where the FAA has considered the criticality of failure conditions. As many of the functions performed by EFBs are also performed by MPSs, EFB policy may provide some guidance in assigning criticalities to MPS functions. If this is not of assistance, or if ADF use of the MPS varies to greatly from similar civil functions, DGTA will be looking for a logical application of the hazard and data criticalities described in Table 1 of the proposed chapter. Where an aircraft level function (e.g. navigation) is involved, the aircraft level functional failure condition may be informative but not necessarily instructive. Where the aeronautical data directly contributes to the aircraft level function, it is likely that the criticalities of the function and the data will be the same. However, where there is a distinction between the function and the data (for example, the difference between operating an aircraft with an out of range centre of gravity and erroneously calculating that an aircraft centre of gravity is in range) it may be appropriate to reduce the criticality of the data by taking into account other factors that contribute to the aircraft level failure (e.g. consideration of the obscurity or novelty of the aircraft loading condition required to produce the worst case result, the limited range of variables considered by the calculation, etc).

Disposition

46. The above response will not result in changes to the proposed chapter.

Comment – MPS Impact on Type 2 LOA

47. The comment received was as follows:

- a. *Para 28-30. Type 2 Letters of Acceptance seemingly only applies to compatibility of data items with an aircraft avionics system. How does this address compatibility for the same data item with the MPS. The start of this section refers to assessing the adequacy of source data used by the MPS. If the MPS further formats, or manipulates this data prior to distributing to the target application (i.e. aircraft), will Letters of Acceptance (on the original source data) be no longer be applicable, as it has been modified? The considerations listed in 30a-c only addresses the preservation of accuracy and integrity of the data passed through, manipulated or generated by the MPS. Compliance to DO-200A which is what the LOA attests will also require evidence that the other data quality requirements (e.g. format, completeness, resolution, etc.) are preserved. As previously raised, those other data quality requirements have not been covered adequately by this chapter.*

Response

48. A Type 2 Letter of Acceptance is evidence that the aeronautical data provided by a particular supplier is appropriately assured and compatible with a particular avionics system. In issuing a Type 2 Letter of Acceptance, the FAA will have considered how the aeronautical data is transferred to the avionics system. A Type 1 Letter of Acceptance is evidence only that the aeronautical data provided by a particular supplier is assured to a certain level and has known quality attributes (which may or may not be sufficient for, or compatible with, a particular application). If the ADF uses a different MPS to process aeronautical data than was considered in issuing Type 2 Letter of Acceptance, then the relevance of the Type 2 Letter of Acceptance has been lost. The ADF will need to conduct an assessment of the MPS but should still be able to rely on the Type 2 Letter of Acceptance as evidence that the aeronautical data provided by the supplier (i.e. prior to processing by the MPS) has been assured to a certain level. Effectively, by introducing a new MPS, the Type 2 Letter of Acceptance has been reduced to a Type 1 Letter of Acceptance.

49. The consideration of other data quality attributes (format, completeness, resolution, etc) is discussed above in paragraph 30.

Disposition

50. The above response will not result in changes to the proposed chapter.

Comment – Scope of Chapter

51. The comment received was as follows:

- a. *Para 32. The guidewords of Manipulate and Generate go beyond the intent of the 'Data Preparation' functional link as per DO-200A, which includes the phases of Assemble, Translate, Select and Format, and is really only applicable to static aeronautical data. With MPSs we are also largely dealing with dynamic data supplied through interfaces to external information systems or human input. The guidance in this chapter needs to clarify this point as it implies that the guidance therein is fully derived from DO-200A. By introducing guidance for dealing with dynamic data, this chapter has gone beyond the scope of DO-200A which deals only with the data preparation and data transmission functional links for static aeronautical information.*

Response

52. As discussed in paragraphs 8 and 13 of the proposed chapter, the ADF policy for MPS has been adapted from a range of FAA policies covering both aeronautical data processing and EFBs. This approach is necessary because of the ADF use of MPS to both process and generate data that may have safety implications for the aircraft. Contrary to the above response, the proposed chapter does not imply that the guidance has been fully derived from DO-200A.

53. The respondent is correct in stating that DO-200A generally only considers static aeronautical information. The respondent is also correct in stating that ADF use of MPS incorporates the generation of aeronautical data (e.g. weight and balance calculations, take off and landing data calculations). It is for these reasons that the ADF policy on MPS has had to expand on the FAA policy for aeronautical data processing. There is no intention to limit ADF policy to DO-200A considerations and this is already discussed in paragraphs 8 and 13 of the proposed chapter.

Disposition

54. The above response will not result in changes to the proposed chapter.

Comment – Validation by Application

55. The comment received was as follows:

- a. *Para 57. This paragraph states that critical data should be validated by application prior to blanket authorisation of navigation operations using the data. Clarification will need to be provided for critical data that is updated on a monthly basis (e.g. WWNDB updates?). As it reads, one could interpret that each month data update will need to be validated by application. Example: Once a particular version of critical data has been validated, and applicable data checks are in place, monthly updates of this data will not need require further validation by application.*

Response

56. Validation by application is required prior to the initial widespread release of Critical aeronautical data. Subsequent updates to that data also require validation by application. It is presumed that, in the example given by the NPRM respondent, the changes made to the database on a monthly basis do not directly affect Critical data. Where it can be shown that an update to a database does not alter Critical data (i.e. appropriate mechanisms are in place to detect or prevent changes to that part of the database), validation by application is not required. Where changes are made to Critical data within a database, validation by application will be required.

57. Consider, for example, a navigation database that contains a range of information including Required Navigation Performance (RNP) 10 airspace boundaries and approach data for RNP Authorisation Required Approaches (AR APCH). The RNP 10 data would probably be considered Essential and would not require validation by application. The RNP AR APCH data would be Critical and would require validation by application. Once the RNP AR APCH data is initially validated by application, further updates to the database that can be shown to only affect the RNP 10 data would not require validation by application. However, further updates to the RNP AR APCH data would require validation by application.

58. A further point that is brought out by this response is the level at which aeronautical data is classified. The presence of Critical aeronautical data in an aeronautical database does not make the whole aeronautical database Critical. Each type of data within the aeronautical database still carries its' own criticality that is determined by the usage of that data. For example, it is possible that a World Wide Navigation Database will contain a mix of Critical, Essential and Routine data.

59. However, when dealing with aeronautical databases, it may be simpler to implement digital error detection across the entire database rather than focus on those aspects of the database that are Essential or Critical. In such a case, the digital error detection technique must be assured commensurate with the highest data criticality handled but this does not mean that all data within the aeronautical database acquires the highest criticality.

Disposition

60. The proposed chapter will be amended to clarify that validation by application is not required where changes to databases can be shown not to affect Critical aeronautical data.

Comment – Independent Verification

61. The comment received was as follows:

- a. *Paragraph 36 – Treatment of identified deficiencies. Another method of managing deficiencies associated with the levels of assurance of safety critical software, especially for a mission planning system is verification. That is, confidence can be built on a mission by mission load basis if each mission load can be independently verified prior to the loading of the mission onto the aircraft. This verification is obviously reliant upon considerations such as:*
- (1) *the level of independence / difference between the platform used to develop the mission compared to that used to verify it,*
 - (2) *the ability to configuration manage and control the data transfer device once the mission load has been verified – i.e. loads are not changed after being checked and prior to loading onto an aircraft,*
 - (3) *the ability of the verification software to be able to check a set of parameters sufficient enough to provide the required level of confidence, and*
 - (4) *confidence that the process/system used for verify the load does not change the mission load.*

Response

62. In some cases, a deficiency in the assurance of an MPS can be treated through independent verification of the output data. The proposed chapter already accounts for independent verification by another software tool, but it is also possible that the output data can be manually verified. There are, however, some substantial limitations to the applicability of this treatment. Firstly, manual inspection of data is notoriously unreliable. Manual inspections should not be the sole treatment where there are substantial amounts of data or if the data is considered Critical (i.e. procedural controls alone are insufficient for Catastrophic and Hazardous failure conditions). Secondly, manual inspection of data only provides confidence in the data that has been reviewed. It is not a replacement for assurance. If the treatment for a deficiency is manual inspection, the manual inspection must be performed every time data is generated or processed. Finally, manual inspection is only possible where the output can be otherwise produced through manual calculations. It may not be possible to manually verify all aeronautical data that is generated by an MPS.

63. To illustrate these points, consider the following examples:

- a. **Weight and balance calculations.** These types of calculations may be relatively straightforward to perform by hand (this is the traditional method for making these calculations). As such, it is possible to independently verify weight and balance calculations by hand (though doing so removes the efficiency gains provided by the MPS).
- b. **Transfer of an aeronautical database.** Aeronautical databases can contain millions of data entries. It is simply not possible to rely on manual error detection for transfer of databases of this size (noting of course that the manual error detection would have to occur every time the transfer occurs). Manual verification

is not a suitable treatment for lack of assurance or protection of an aeronautical database transfer process.

64. Another common misconception is that a period of MPS use (e.g. 6 or 12 months) is a sufficient replacement for design assurance. While operational use of an MPS can contribute to confidence in the system, such confidence can only be obtained if the operational use is structured to achieve assurance objectives and the required level of confidence is at the lowest level. For example, it may be possible to analyse a period of operational use against satisfaction of the DO-178B Level D objectives but without specific consideration, it is unlikely that the robustness test criteria would be sufficiently covered. A period of unstructured operational use provides only minimal confidence (insufficient for Essential or Critical data) due to the following:

- a. Design assurance concepts provide confidence in the correct operation of a system not only through verification of correct functionality for the range of expected use, but also through verification that system responses to unexpected usage are appropriate. Verifying system response to unexpected inputs is critical to assuring safe operation as, while every effort is made to assure correlation, there is often a difference between the expected range of use and the actual range of use. Furthermore, the most common cause for systematic failure condition contributions to accidents is exposure to unexpected inputs or usage. A period of operational use early in the MPS lifecycle is unlikely to expose the MPS to the same range of unexpected inputs that would be seen through application of design assurance concepts.
- b. MPS usage early in the lifecycle is likely to differ from MPS usage later in the lifecycle. There are a number of potential reasons for this difference, including expansion of the types of mission plans, optimisation of operational processes, increased operator familiarity with the system and so on. Any confidence that can be obtained through the initial phase of use cannot be extended to latter phases as it is possible that the different usage later in the lifecycle may expose faults that were not seen for the limited range of use early in the lifecycle.

Disposition

65. The proposed chapter will be amended to include manual verification as an option for treating deficiencies in limited circumstances. The proposed chapter will also be amended to more clearly state that a period of operational use is not a substitute for design assurance.

Comment – Verification of Reversal Checks

66. The comment received was as follows:

- a. *Para 33, Table 3, Manipulation / generation Data Assurance Level 1 & 2. The reversal program should be tested independently from the generation program, to reduce the chance of introduced errors being ‘undone’ as part of the error checking process. A ‘reverse’ data conversion code fragment is likely to have been coded using the same rules as the conversion code itself, so it may end up correcting erroneous data instead of highlighting it. Eg:*

(1) *Correct data → Fault on conversion → data error on avionics system → corrected by reversal program → correct check result provided.*

- (2) *Continual checking of the reversal program will also be required to incorporate MPS version updates.*

Response

67. Reversal checks are only appropriate treatments where the process of reversal is a different design implementation to the original process (e.g. differentiation vs. integration, multiplication vs. division, etc). The code that implements the reversal check must still be assured to the appropriate level. If a reversal check is the mechanism whereby the introduction of errors will be detected the reversal check must be conducted each time aeronautical data is processed, not just when the MPS is modified.

Disposition

68. The above response will not result in changes to the proposed chapter.

Comment – Central Management of Flight and Mission Planning Systems

69. The comments received were as follows:
- a. *Given that say the same system is fitted to different aircraft and or types then assessment is required for each leading to duplication of assessments for basically the same system. Surely precedence can be used where suitable.*
 - b. *Para 52(c) Responsibility for configuration control of data products used in the planning process. JMPS uses data derived from many external agencies (AusDAFIF, ECHUM, DTED, Mapping Data) etc. This NPRM is suggesting that this is the responsibility of the end user platform supporting SPO. In many cases the data provided by these agencies is provided to several platforms for mission planning purposes. Whilst the end user SPO must be responsible for the configuration control of the data used on their relevant platforms, configuration management of the products and data sources delivered by these agencies needs to be the responsibility of the supplying agency (CISSO). Individual SPOs managing the configuration processes used by these agencies will invariably mean replication and inefficiencies. Suggest that establishing certification frameworks for these agencies, and assessment against said framework, to provide confidence in the products provided, is within the purview of DGTA SCI.*

Response

70. It is the responsibility of the relevant aircraft DAR to assure that an MPS is suitable for use with a particular aircraft. In assessing whether an MPS is suitable, and establishing a framework to assure that it continues to be suitable, the DAR may draw on the support of a number of organisations and rely on them to fulfil certain roles. Given that a number of MPS are in use across multiple aircraft, and some are already centrally managed, it is possible that a number of aircraft DARs may rely on the same organisation to perform the same or similar functions for a common MPS. However, even though an MPS may be common to a number of aircraft, the extent to which the MPS is relied upon not to introduce errors to aeronautical data will vary depending upon the use to which that data is put. As such, regardless of any central management of MPS, the relevant aircraft DAR will be responsible for identifying the need for design features and design assurance for those aspects of the MPS that process or generate Critical or Essential aeronautical data for the subject aircraft. This assessment, for which the proposed chapter outlines a suitable process, will drive the extent of support that any organisation centrally managing MPS will need to provide. Importantly, where the level

of support provided by a supporting organisation is not sufficient to meet an appropriate safety benchmark, the relevant aircraft DAR will need to seek additional data or support as appropriate.

71. The established AEO framework would be a suitable mechanism for assuring that an organisation centrally managing MPS components has sufficient organisation, people processes and data to fulfil the assigned functions. SCI-DGTA and ACPA are currently working to establish a framework for the accreditation of agencies that produce aeronautical databases for wide distribution (e.g. RAAF AIS), though this is only peripherally related to the subject of the proposed chapter.

72. Establishing arrangements for the central management of MPS components is a resource issue and is outside the purview of DGTA. The concern of DGTA is that an MPS is appropriately assured for use with a particular aircraft type. This outcome can be achieved with either centralised or decentralised management of an MPS. DGTA will not mandate a specific allocation of resources to this particular task, but if centralised management of MPS does emerge through agreements within DMO the guidance in the proposed chapter may be updated.

73. The use of precedence where suitable is covered by the policy on Recognition of Prior Acceptance (RPA). Importantly, the ADF cannot blindly rely on the certification of a system by another airworthiness authority, or within the ADF for another aircraft type. The use of an MPS, and the extent of reliance, may vary between aircraft types. In conducting the Design Acceptance process, a DAR seeking to rely on RPA must consider whether the relevant configurations, roles and operating environments are sufficiently similar. The process for doing this is already covered in paragraphs 37 to 42 of the proposed chapter.

Disposition

74. DGTA would be supportive of moves to centrally manage MPS components where resource efficiencies can be obtained. Regardless of the distribution of effort amongst DMO elements, it must still be assured that the MPS is suitable for the context of use with a particular aircraft. The relevant aircraft DAR is responsible for assuring that an appropriate organisation has been allocated to each aspect of MPS management. The above responses will not result in changes to the proposed chapter.

Comment – Functions Other than Aircraft Functions

75. The comment received was as follows:

- a. *Paragraph 9a – FAA framework. Functions other than ‘aircraft functions’ need to be considered here, (e.g. table 2 lists kneeboard plate, as well as maps, safe escape data, etc). It is presumed that any MPS output that has a safety impact is to be included in this assessment.*

Response

76. All MPS outputs need to be included in the assessment. An output cannot be considered to have no safety implications until the output’s contribution to aircraft level functions is determined. The proposed chapter does not levy requirements on MPS functions or outputs that do not have safety implications, but does require that an assessment demonstrate that a particular function is not safety related.

77. In any event, paragraph 9 is a summary of the FAA framework for aeronautical data. The ADF approach to MPS will need to consider functions that are not considered by the FAA framework (e.g. safe escape data). However, as paragraph 9 is a summary of the FAA framework, ADF specific considerations will not be included here.

Disposition

78. The above response will not result in changes to the proposed chapter.

Comment – Hardware Issues

79. The comments received were as follows:

- a. *Para 46. The USAF, in particular Air Mobility Command (AMC), certifies MPS, including pre-flight planning systems, to be operated on specific hardware brands and models. FMS purchases operating in the ADF and utilising RPA assessment, could have difficulties satisfying these tight controls, particularly due to costs and availability of these specific models in Australia, not to mention ongoing availability.*
- b. *According to US contractors/government testers, there is no example to date where government testing has produced erroneous results relating to the hardware the OS is operating on. Further guidance on this issue would be useful in the proposed chapter.*

Response

80. Inevitably there will be differences between the hardware upon which a foreign military has certified an MPS for use and the hardware employed by the ADF. This is particularly true when an MPS is to be hosted on the DRN or DSN. MPS must be compatible with target hardware. It is possible that different brands and models of target hardware will present no compatibility issues. For lower assurance levels, differences in target hardware can be treated through analysis (e.g. by determining that lower level components are identical or that differences are negligible) or verification (e.g. conduct of a targeted subset of test cases to verify that target hardware differences do not negatively impact operation of the MPS). At higher assurance levels, the burden of demonstrating correct operation of the MPS on different target hardware may be substantial. Acquirers of higher assurance level MPS should consider whether the effort required to verify the MPS on the different target hardware is worth any cost and schedule benefits obtained through the acquisition of different target hardware.

81. While the experience gained by US contractors/government testers may be informative, it is not instructive. Firstly, the absence of evidence of target hardware issues is not evidence of the absence of target hardware issues. Secondly, device driver compatibility issues are exceptionally common. If the ADF is to rely on an MPS to correctly perform a safety related function, then that reliance extends not just to the MPS but to the target hardware as well.

Disposition

82. Additional guidance will be added to the proposed chapter to clarify the need for compatibility with target hardware as opposed to employing identical hardware.

Comment – COTS Products and CAST-14

83. The comment received was as follows:

- a. *Para 46 – DO-178B Level D Certification consideration for COTS products. Understood that this aspect applies generally to EFBs however CAST 14 has been withdrawn for rework by the FAA – unable to comment on the verification aspects of a Level D software system (such as Windows XP which is used exclusively for F/A-18 JMPS).*

Response

84. COTS operating systems that were not developed for use in the aviation environment inherently have limitations that will prevent a high level of integrity being assured. While most COTS operating systems can satisfy the DO-178B Level D objectives, the presence of unnecessary features and an inability to access design data and source code will prevent the Level C or higher objectives being satisfied. DGTA has published additional guidance in a paper titled *Use of Commercial Off the Shelf Operating Systems to Host Aviation Software Applications* available through the DGTA website.

85. The respondent is correct in stating that CAST-14 considerations generally only apply to software that is used in flight (e.g. EFBs). The discussion of CAST-14 has been included in the proposed chapter as there are a number of MPS that may be used both on the ground and in flight. In flight use of an MPS should address the CAST-14 issues. Fortunately, for those MPS that are only used in the ground environment, the CAST-14 issues do not need to be considered provided that verification of the MPS accounted for the configuration of the operating system.

86. The reason that CAST-14 applies to software used in flight and not software used on the ground is the difference in environments and the ability to treat issues. The available treatments for software issues in flight is limited. The time critical nature of in flight software use also means that reliability and availability are important considerations. This is less true in a ground based mission planning environment. While it may be inconvenient to reboot a PC or revert to manual mission planning, such options are available and reduce the extent of reliance on ground based software compared with in flight software. As such, the integrity requirements are somewhat relaxed. The integrity requirements for ground based software are generally focused on preventing erroneous software outputs, whereas in flight software integrity requirements also add reliability and availability considerations.

Disposition

87. The guidance on applying software assurance concepts to COTS operating systems is already sufficient. The above response will not result in changes to the proposed chapter.

Comment – Other Applications Hosted on the COTS OS

88. The comment received was as follows:

- a. *Para 50.b. Is this para intended to restrict a computer system to running the MPS application only? Continually assessing COTS operating systems and hardware along with applications hosted on the COTS OS would involve significant time, effort and costs. If implemented as read, an assessment would be required for each update of the MPS, COTS OS or associated applications.*

Response

89. COTS operating systems can react poorly to system upgrades, changes to device drivers and registry settings and other changes associated with the installation or modification of software applications. The proposed chapter does not restrict a computer system from running applications other than the MPS, however where this is done, there will be a burden in assuring that the installation or modification of other software applications does not negatively interfere with an MPS component requiring Data Assurance Level 1 or 2.

Disposition

90. The above response will not result in changes to the proposed chapter.

Comment – Modifications

91. The comment received was as follows:

- a. *Due to the dynamic nature of software, continual version updates could require this entire process to be updated each time (in the absence of detailed software change logs), particularly for level 1 version changes i.e. from 3.1 to 4.1.*
- b. *Para 53. This section should further address or refer to guidance for considerations when upgrading or modifying existing MPS through software builds, etc.*

Response

92. There is a popular misconception that software modifications should be straightforward. In comparison to hardware technologies, the installation of software modifications is relatively straightforward. Unfortunately, the ease of installation has been extrapolated over time to create a myth that software modifications as a whole are straightforward. This is rarely true. Care must be taken when modifying software that functions that are not intended to be changed are not negatively affected.

93. The entire process does not need to be conducted each time an MPS is updated; but a subset of the process will always be required. In introducing a change to an MPS, the ADF must assure that any new or modified functionality is appropriately assured and that retained functionality is not negatively affected. The proportion of the process that must be repeated for a modification to an MPS will depend upon the extent of functionality introduced or modified and the design of the MPS (e.g. the ability to partition functions).

94. The process for introducing modifications to an MPS shares many parallels with the introduction of modifications to on-aircraft software. Each time aircraft software is modified, an analysis is required to determine whether any new safety related functions are introduced and whether the new functionality affects the required assurance level. The new and modified software must be developed to meet an appropriate assurance level and be shown not to negatively affect the software that has not been modified. The same process is required for an MPS. MPS modifications should be assessed to determine whether new aeronautical data transfer, formatting, manipulation or generation functions are introduced and whether the new functions process Essential or Critical data. The new or modified functions need to be assured in accordance with the treatment options described in Table 3 of the proposed chapter.

Disposition

95. Paragraph 51 of the proposed chapter already covers reassessment following changes or updates to the MPS or changes in operational use. The above responses will not result in changes to the proposed chapter.

Comment – Suitability of RTCA/DO-178B

96. The comment received was as follows:

- a. *There is a reluctance to use RTCA/DO-178B for software verification by OEMs of COTS equipment as it is expensive and complex. To find an equivalent including European systems will be daunting for retrospective RPA for equipment already fitted and in use.*

Response

97. DO-178B is the preferred standard for software assurance as it is widely recognised, can be applied retrospectively and well supported by available tools and guidance. Alternate standards and benchmarks may also be suitable, provided a level of safety comparable to DO-178B is achieved. DO-178B and the European counterpart, ED-12B, are widely accepted and adopted within the European aviation community.

Disposition

98. The above response will not result in any changes to the proposed chapter.

Comment – Criticality of Flight and Mission Planning Systems

99. The comment received was as follows:

- a. *The use of MPS in the ADF is normally categorised as a non primary navigation system. Hence, failure is mission critical and not airworthiness critical. Thus the new chapter is aimed at all MPS as this distinction is not addressed.*

Response

100. Historically, the safety implications of MPS use by the ADF have been limited. MPS use in recent times has evolved to the point where the correct functioning of an MPS is integral to the airworthiness of an ADF aircraft. MPS now process data associated with airspace boundaries and precision approaches where even slight errors can result in Catastrophic consequences or increased risk to the public at large. A number of MPS currently, or soon to be, in use in the ADF are most definitely safety related systems.

101. It is also incorrect to state that the proposed chapter does not distinguish between safety related and mission related functions. A key element of the assessment described by the proposed chapter is to determine the data that is generated or processed by the MPS and assign criticalities to that data. The assurance process then focuses on Critical and Essential data (i.e. data with safety implications). Data that is mission related will fall into the Routine category and no assurance requirements are levied. If an MPS that is currently in-service is truly limited to mission related functionality, then the proposed chapter imposes no new requirements other than to confirm, via a structured and defensible analysis, that the MPS does not generate or process any safety related data.

Disposition

102. The above response will not result in changes to the proposed chapter.

Comment – Minor Failure Conditions

103. The comment received was as follows:

- a. *Table 1: Minor Aircraft FF is grouped with an ‘Essential’ Data Criticality, should Minor be grouped with Routine as the definitions more closely align? e.g.:*
 - (1) *Minor: a slight reduction in safety margins.*
 - (2) *Essential: a significant reduction in safety margins.*
 - (3) *Routine: would not significantly reduce aircraft safety margins.*

Response

104. Ambiguity will always be present in severity definitions as they inherently include subjective descriptions such as ‘significant’, ‘large’ or ‘slight’. While it is possible to interpret the definition of ‘Minor’ consistently with the definition of ‘Routine’, such an alignment is not consistent with FAA policy nor does it result in an outcome that is reasonable. A Minor failure condition will have some impact on the safety of an aircraft, albeit slight. The proposed chapter imposes no assurance requirements on data that is Routine. To align Minor with Routine would effectively require no treatment of failure conditions that can reduce aircraft safety margins. From an airworthiness perspective, such an outcome is untenable and inconsistent with international practice.

Disposition

105. The above response will not result in changes to the proposed chapter. Data that can contribute to Minor failure conditions will be considered Essential.

Comment – When Qualification is Required

106. The comment received was as follows:

- a. *Table 3. This table uses the principles of Table A-5 which is derived from DO-200A, however it fails to clarify the necessary considerations to determine whether or not qualification is required in the first place (i.e. not all tools need to be qualified, which Table 3 suggests for Critical and Essential data).*

Response

107. This response has mistaken the proposed chapter for an ADF implementation of DO-200A despite the guidance in paragraphs 8 and 13 of the proposed chapter. As previously discussed, the proposed chapter is intended to guide the Design Acceptance of MPS. Part of that process will consider aeronautical data processing consistent with DO-200A, but this is not the entirety of the process. Table 3 uses the principles of Table A-5, but also incorporates other considerations that are relevant to the ADF and not found in civil aeronautical data processing standards. Table 3 is intended to apply to MPS (the subject of the chapter). Table 3 is not intended to apply throughout the aeronautical data processing chain (for example, Table 3 is not intended to apply to producers of aeronautical data).

108. Furthermore, Table 3 does not require qualification of all MPS components. For example, Table 3 does not require qualification of MPS components that only process Routine data. Table 3 also doesn't require qualification of MPS components that process aeronautical data where that processing is protected by other mechanisms. For example, if an MPS transfers an aeronautical database that contains Critical data with a CRC value calculated by the aeronautical data producer (i.e. not calculated within the MPS) and the on-aircraft system that receives the database compares the database to that CRC value, then there are no assurance requirements levied on the MPS transfer of that data.

Disposition

109. The above response will not result in changes to the proposed chapter.

Comment – Depth of Criticality Assessment

110. The comment received was as follows:

- a. *Annex C: the sections addressing datalinked data has been copied directly out of I would imagine a more generic description of data exchange messages should be put in rather than specific details of every supported message. Specifying that level of detail does not add any value unless a classification of criticality is applied to it by DGTA.*

Response

111. The functions listed in annex C of the proposed chapter are only examples intended to guide the reader in determining the functions that are performed by the MPS that is the subject of a technical assessment. The level of detail in this list may not be appropriate for a particular application: more or less detail may be required.

112. The level of detail in a technical assessment of an MPS needs to be refined until refining it further would not add value. Further levels of detail would not add value if:

- a. all data within a group has the same criticality, and
- b. it is readily apparent to external parties reviewing the assessment that all data within the group should have the same criticality.

113. The criticality of aeronautical data is driven by the function for which it is used, not by the medium over which it is transmitted. Aeronautical data that is transferred over a common path will not necessarily have the same criticality. Where appropriate, the MPS component functional assessment (e.g. Table 4 of the proposed chapter) should group data by function and not by transfer medium.

Disposition

114. The proposed chapter will be amended to include additional guidance on the required depth of technical assessment but the examples in annex C will not be changed.

Comment – HMI Requirements

115. The comment received was as follows:

- a. *Para 44 mentions HMI should provide a consistent and intuitive user interface. Whilst this is a true motherhood statement, to what specification/document is to be met for verification?*

Response

116. There are a number of suitable standards for the development and analysis of HMI aspects of a system such as an MPS. Additional guidance on HMI standards is available in AAP 7001.054 Section 2 Chapter 13. The proposed chapter was not intended to reproduce the HMI guidance provided elsewhere in AAP 7001.054.

Disposition

117. A reference to the HMI chapter within AAP 7001.054 will be added to the proposed chapter.

Comment – Downloading Data

118. The comment received was as follows:

- a. *Do we need to recognise data transfers between agencies such as RAAF AIS and the SQN? e.g. internet/intranet transfer.*

Response

119. The intent of the MPS framework described in the proposed chapter is to assure the integrity of aeronautical data that is generated or processed by the MPS. More broadly, the ADF also needs to assure that no link in the aeronautical data processing chain can introduce errors, though for the most part, this is outside the scope of the proposed chapter. As aeronautical data can be transmitted over the internet or intranet, mechanisms must be put in place to assure that these links do not introduce errors. MPS may contribute to the mechanisms that protect the transmission of aeronautical data over network links.

120. This does not mean that the integrity of the internet or intranet links needs to be assured. What is required is that the aeronautical data is protected as it is transmitted, usually via some form of checksum or Cyclic Redundancy Check (CRC). Aeronautical data that is protected in such a fashion can be transmitted over network links that have not been assured, though the software that generates the checksum or CRC and the software that detects errors will need to be assured to a level commensurate with the criticality of the data. As the MPS may be relied upon to detect such errors, certification of the MPS may need to consider aeronautical data transfers over the internet or intranet.

Disposition

121. The proposed chapter will be updated to clarify the role of MPS in assuring that errors are not introduced when aeronautical data is transmitted over network links.

Comment – Source Data Configuration Control

122. The comment received was as follows:

- a. *The configuration control of source data should be defined to avoid confusion in the level of configuration control to be applied by the end user. The version of source data is changed on a monthly basis (e.g. AusDAFIF 0908, for the 8th release of 2009), whereas the Edition (e.g. AusDAFIF Ed 8) of the data remains the same for that particular format. Version control should be applied to the format identifier as opposed to the cycle identifier. Perhaps a more clear definition of terms may resolve this issue. Source data format vs. source data cycle.*

Response

123. The configuration control of source data needs to be sufficient to enable differing versions, that may differ by no more than a single bit, to be distinguished based solely on the unique identifier alone. The level (e.g. version, cycle, etc) at which configuration control can achieve this will vary depending upon the source data being considered.

Disposition

124. The proposed chapter will be amended to provide additional guidance on the objective of configuration control.

Comment – CASA Input

125. The comment received was as follows:

- a. *Has DGTA sought advice from CASA on this?*

Response

126. The policy described in the proposed chapter has been developed from FAA policy and advice has been sought from the FAA. As CASA accept FAA policy, and very few MPS of interest to the ADF are developed under CASA oversight, consultation with CASA was not considered necessary.

Disposition

127. The above response will not result in changes to the proposed chapter.

Comment – EW Systems

128. The comment received was as follows:

- a. *Will the requirements in this chapter be made applicable to EW support systems also?*

Response

129. The proposed chapter generally does not apply to EW support systems. Most EW support systems are used in the generation of EW libraries which are subject to dedicated verification activities prior to use. Whereas data processed or generated by an MPS is rarely subsequently subject to verification prior to use. If an EW support system was used in such a

manner that the output data is not subject to verification prior to use (i.e. the only mechanism for assuring the correctness of the data is to assure the correct operation of the EW support system), then the proposed chapter would apply. However, as the vast majority of data produced for EW systems is not safety related, it is unlikely that the proposed chapter would impose any additional assurance requirements.

Disposition

130. The above response will not result in changes to the proposed chapter.

Comment – Definitions

131. The comments received were as follows:

- a. *Para 3. Discusses various performance levels associated with system design/production i.e. approved, accredited, etc. Suggest that a formal definition be published for such terms so that document users know exactly what is meant by certified, approved, accredited, assured, etc. When this is cross referenced to the DAL levels and MPS functional words, there then should be no dispute between customer and supplier/designer as to what is required.*
- b. *Whilst I understand the intent of the column titled 'Absence', the term is not explained in Annex A as indicated in para 33. Although reference is made in para 23 and in Table 4 (top RHS cell) to Absence, a better introduction to the meaning of the term should be provided.*

Response

132. While succinct definitions of certified, approved, accredited, assured and other similar concepts may be useful in resolving contractual disputes, these are complex and involved concepts and as such, any succinct definition would be at the expense of accuracy or would be so simple as to provide little value.

133. It is agreed that the proposed chapter would benefit from an introduction to the meaning of the term 'absence' within the context of MPS and software assurance.

Disposition

134. The proposed chapter will be updated to clarify the meaning of the term 'absence'.

Comment – Extent of Guidance Provided by the Chapter

135. The comments received were as follows:

- a. *This proposal brings substantial clarification to the DGTA's expectations for assessing and providing design acceptance of MPS systems, particularly those applications supporting the conduct of operations involving critical aeronautical data. In the ... context, this guidance provides structure to what has previously been a non-existent or ad hoc assessment approach.*
- b. *As a precursor to my specific criticism, it's worth talking about the audience of this chapter of the 054. Obviously this is aimed at both MPS "experts", given the exhaustive discussion of the FAA framework, but also at project engineers who are establishing their design acceptance strategy and data requirements. Projects working out their design acceptance strategy and data requirements for*

solicitation (be it FMS, DCS or Cooperative acquisition) will not be necessarily staffed with engineers familiar with the details of mission planning systems. [...] is certainly no exception to this. So the guidance in this NPRM relevant to those projects needs to be understood by engineers who may not be familiar with the detail of mission planning systems.

- c. *It is understood that mission planning has not previously been addressed well (to date) in either operational or technical regulations. For this reason, the draft chapter serves to inform users on many aspects of MPS so that informed assessments can be undertaken. Whilst this is the intent of the chapter, this has not been achieved within the draft chapter. It is considered important to explain the users the possible applications of an MPS and hence establish a basic Use Profile that can be adapted to particular platforms. With respect to assessments of MPS, I also consider it important to have considerable operational input to the process.*
- d. *It would be ... preference to provide users with a basic understanding of the MPS framework that is typically used to define an MPS, as the airworthiness of all components can be assessed in relation to the interaction of these components, in consideration of the platform it shall support.*
- e. *This frameworks [Figure 2] supports a clear allocation of responsibilities that can be applied to common MPS or unique MPS products. The airworthiness of a platform is supported by an MPS only when all these elements are integrated well. Ideally, the chapter should be aligned with this framework, with discussion on each of the considerations being contained in annexes. Most of this is already within the draft chapter, to differing degrees.*

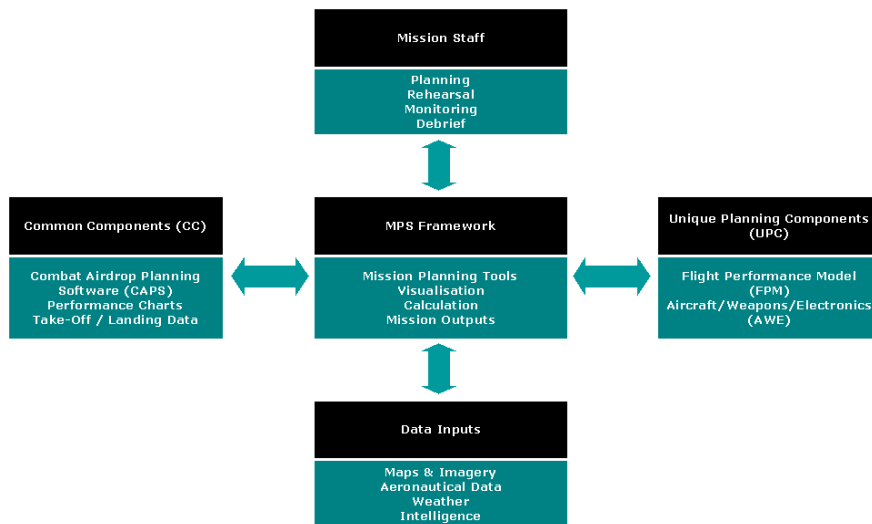


Figure 2: Framework Proposed by an NPRM Response

Response

136. The focus of the proposed chapter is to define a framework that will adequately treat technical sources of safety risk posed by MPS. It is acknowledged that MPS fit into a larger framework and that there are other sources of risk posed by MPS and mission planning in general. The proposed chapter is not intended to comprehensively cover ADF use of MPS and aeronautical data as many aspects would be beyond the responsibility and authority of the Technical Airworthiness Regulator. The proposed chapter does touch on aspects of MPS use

that are not technical where it is required to provide context to the identification, analysis or treatment of technical sources of safety risk.

137. It should also be noted that there are three important influences on the extent of guidance provided in this chapter:

- a. **Introduction of safety related functions.** Use of MPS on legacy aircraft, such as F-111 and F/A-18A/B, generally had limited effect on the safety of an aircraft. More modern and complex aircraft rely on MPS to a greater extent from a safety perspective. As such, it is important that the proposed chapter provide some background to personnel who may have extensive experience in MPS that do not perform safety related functions to minimise the likelihood that those personnel will apply the same approaches to MPS that perform safety related functions.
- b. **Absence of higher level regulation and guidance.** The above respondents are correct in the identification of other contributors to hazards resulting from MPS use (e.g. finger trouble) and the fact that the technical consideration of MPS can only occur within the broader context of MPS use. However, at this stage, the regulations and guidance covering operational use of MPS are still maturing or in development. As such, the proposed chapter considers some aspects of MPS use that will eventually be covered by operational regulations and guidance. Once these frameworks are in place, the proposed chapter may need to be amended. However, the generation of DGTA guidance on Design Acceptance of MPS cannot be delayed much longer as a number of projects are already, or are about to be, engaged in the Design Acceptance of MPS.
- c. **Complicated policy basis.** The ADF policy on MPS requires consideration of a number of policies from other airworthiness authorities. Generally, it is a combination of aeronautical data processing and EFB considerations from the FAA that has been adapted for the ADF use of MPS and focus on system acceptance. This complicated policy base makes it difficult, in the absence of the proposed chapter, to provide detailed guidance to practitioners. It also means that the proposed chapter must provide some guidance on how ADF policy has been derived such that personnel who understand FAA policy are able to adapt.

138. The target audience for the chapter are ADF engineers involved in the Design Acceptance process for MPS. As the development of an MPS is only a subset of the aeronautical data processing framework, and the scope of responsibility of most contractors is limited to development of an MPS, it is necessary for the ADF to fully understand the need for and practical application of aeronautical data processing assurance requirements. Where a Project Office is staffed with personnel who do not have a sufficient understanding of MPS, and are unable to obtain such understanding, external assistance should be sought.

Disposition

139. The above responses will not result in changes to the proposed chapter.

Comment – Operational Procedures

140. The comments received were as follows:

- a. *Para 56.d. Completeness of data loaded and maintained may not be possible, particularly when the file size is changed during the manipulation process. Further guidance on potential non-compliance of this issue may be needed.*

- b. *Para 56.f. Enforcing security measures, at least in a software context, would be unlikely to be achieved. Unless it is probable that the users may inadvertently modify the MPS or other listed components, this may be more appropriately addressed by policy or practices.*

Response

141. Where a database is modified or manipulated to such an extent that the file size or structure changes simple mechanisms for verifying completeness of a database may not be possible. If an MPS modifies or manipulates a database to such an extent, then generally the integrity of the MPS will need to be relied upon to assure that the completeness of the database is maintained. Following modification or manipulation, simple mechanisms (such as checksums) may again be employed to assure database completeness in downstream activities (e.g. loading to the aircraft).

142. For example, consider an MPS that receives an aeronautical database and simply truncates the database to provide a subset to the aircraft. Simple digital error detection techniques may not be able to detect errors introduced through this process. The integrity of the MPS, or a cross check against the original database, may need to be relied upon. However, in this case, the procedural requirements identified in paragraph 56.f of the proposed chapter still applies but this time the completeness of the loaded data is measured between the data loaded to the aircraft and the output of the MPS. As such, the MPS may need to recalculate a CRC or checksum value on the data subset to enable the data loading process to be verified.

143. Enforcing security measures for software applications can be, and is regularly, achieved. For higher assurance levels, the ADF may expend significant effort assuring that an MPS is of sufficient integrity to perform a certain function. An unauthorised modification can quickly and easily negate all of that effort. Simple security measures (such as disabling unnecessary CD/DVD drives and USB ports, not connecting to the internet, etc) can be used to minimise the likelihood that unauthorised modifications will be made. These measures should be accompanied by policies and procedures.

Disposition

144. The above responses will not result in changes to the proposed chapter.

Comment – Resource Implications

145. The comments received were as follows:

- a. *No additional resources above and beyond those required for a DAS based on RPA as per NPRM 02 09.*
- b. *If made mandatory, this MPS chapter has the potential to create a large resource implication to both contract changes to existing MPS development contracts and retrospective assessments of existing in-service MPSs.*
- c. *The only resource impact as a result of this additional guidance will be for MPS changes / introduction where design acceptance and service release activities were historically overlooked. The resourcing implications for future activities are reasonable given the role of these assessments in assessing the suitability of MPS applications for processing critical aeronautical data.*

- d. *This will require extra system safety, systems and software engineers to determine whether the new guidance section can be met. The number of engineers will vary with the MPS complexity but it is envisaged that this will take months at best to identify and receive RPA and determine the gaps.*
- e. *Have any trials been done to demonstrate that this will work and a determination of how onerous or otherwise compliance is?*
- f. *There will be an obvious impact on resources, particularly with systems requiring Type 2 LOA data from a supplier who is not accredited; and there are plenty more examples. However, this chapter highlights the level of detail and assurance Mission Planning Systems now require due to their technological advances; hence it should reiterate the need for resource planning in the early stages of a project.*

Response

146. DGTA acknowledges that the resources required to implement the policy described in the proposed chapter are different to the resources that have historically been applied to MPS. However, this difference is primarily driven by the increased use of MPS in safety related functions. The approach that has been taken to the assessment of legacy MPS, which generally had limited safety implications, is not sufficient to assure that MPS in use with modern ADF aircraft are safe and fit for purpose.

147. For those MPS that do not have safety implications (i.e. those that only generate or process Routine data), there will be a light increase in resources required to conduct the analysis that will confirm that the MPS does not have safety implications. For those MPS that have safety implications, but where steps have already been taken to assure the integrity of the MPS commensurate with the severity of the failure conditions, there will be little or no increase in required resources. Those MPS that have safety implications where steps have not been taken to assure the integrity of the MPS will require a substantial increase in resources and may suffer cost increases and schedule delays if the risk of employing an MPS with insufficient integrity is not tolerable to the relevant authority.

Disposition

148. The resource implications of the proposed chapter are limited unless the current approach to assuring the MPS is inadequate. As with any airworthiness issue, the relevant authority may elect to retain the risk associated with not assigning the required resources to appropriately assure the MPS. The proposed chapter will at least ensure informed risk retention.

Comment – Wording Changes

149. Numerous minor wording changes to the proposed chapter were received. A brief summary of the proposals and disposition is as follows:

- a. *Para 2: Electronic transfer media should also include CD/DVD. Not incorporated – these are examples not an all inclusive list.*
- b. *Para 9.f.1: Typo ‘ascribed’. Not incorporated – use of ascribed is correct.*
- c. *Para 15: Leads reader to guidance in Annex A - para 6-10. However the guidance at para 6-10 of Annex A is further clarified/amended in para 32 of the main body of the chapter (i.e. use of different guidewords). This section should*

also therefore refer to the para 32 guidance to avoid confusion, given that para 32 emphasises that the ADF approach defines a different set of functional guide words for MPS applications. Agreed – change incorporated.

- d. *Para 17: Should change reference to para 14 and 15 to para 15 and 16. Agreed – change incorporated.*
- e. *Para 19: Reword 'intolerable risk' to 'any risks which the ADF can not reasonably tolerate'. The MAA wouldn't retain risks they can't tolerate - if they retain it, it means they can tolerate it. The question is can we tolerate those risks? Agreed – change incorporated.*
- f. *Para 21: 1st line typo 'is to establish of the adequacy'. Agreed – change incorporated.*
- g. *Para 22a: Add 'and to determine data quality requirements at the aircraft level'. Not incorporated – this is covered at para 22.b.*
- h. *Para 23: Should reference to paragraph 21 be paragraph 22? Agreed – change incorporated.*
- i. *Para 39: Change 'Involvement as' to 'Involvement of'. Not incorporated – some Military Airworthiness Authorities (MAA) have dual roles as program management and airworthiness authorities. Although the specific organisation that is the MAA may have been involved, it is necessary to determine whether that organisation was involved as an airworthiness authority and not just as a program management authority.*
- j. *Para 41.b.2: Rewrite second sentence to 'The CRE assessment of each MPS component should be based on how the ADF intends to use the MPS, including...'. Agreed – change incorporated.*
- k. *Para 46: Reference to para 49 should be changed to para 50. Agreed – change incorporated.*
- l. *The MPS Design considerations paragraphs 46 and 48 refer to specific remediation techniques to meet requirements rather than the need to address a specific outcome. This risks current technology binding the procedure. Inclusion of "such as" in key spots in the paragraphs would provide more flexibility in actual remediation techniques employed. Agreed – changes incorporated where appropriate.*
- m. *Para 46: Should the reference to para 49 be para 47 instead? Not incorporated – reference to para 49 should be to para 50.*
- n. *Para 54-57: This section on operational considerations should also refer to MILAVREG requirements for operational permits required on Aviation support tools. Not incorporated – there are no MILAVREG requirements specific to MPS. Though in the past it has been suggested that an MPS be treated as an Aviation Support System, this is not the current approach and is not reflected in the current MILAVREGs.*
- o. *Para 54: Should cross-reference relevant Operational Airworthiness regulations for operational approval of MPS. Not incorporated – A cross-reference to a*

publication not within DGTA's control presents an administrative burden that is not reflective of the value to be added.

- p. *Para 55.b: Typo: 'emphasis' should be 'emphasise'.* Agreed – change incorporated.
- q. *Para A-6: What is Essential(Critical) data?* Essential (Critical) data is data that is considered Critical when used in a particular manner but which data suppliers for commercial aircraft generally assure as Essential. This terminology was retained for consistency with the FAA. However, as the terminology has created some confusion, the paragraph will be amended to read 'Critical' instead of 'Essential (Critical)'.
Essential (Critical) data is data that is considered Critical when used in a particular manner but which data suppliers for commercial aircraft generally assure as Essential. This terminology was retained for consistency with the FAA. However, as the terminology has created some confusion, the paragraph will be amended to read 'Critical' instead of 'Essential (Critical)'.
- r. *Table 3. Use consistent terminology. Against the functional guideword of 'format', the word 'translation' (which is more applicable to the manipulation guideword) is used in the Absence column. Suggest that Translation be changed to 'Formatting' in these instances.* Agreed – change incorporated.
- s. *Table 3. Notes 2, 4 and 6: There appears to be an inconsistency between these Notes and the Requirements in Annex A Table A-5. Note 4 states level D or Verification, whereas Note 2 and 6 do not include 'or Verification Tools Requirements'. Table A-5 includes Verification Tools Requirements for the two cases of Notes 2 and 6. The inconsistency between Notes 4 and 6 will be resolved by the inclusion of Verification Tool Requirements for Note 6. Table A-5 is a summary of the Tool Qualification Requirements of DO-200A. The Tool Qualification Requirements described in DO-200A are somewhat ambiguous and not necessarily clear and as such, annex A contains a summary. In summarising DO-200A, some resolution has been lost. Note 2 is an example of this. The Note 2 requirement as stated in the proposed chapter is correct. Table A-5 will be revised to remove the ambiguity with Note 2.*
- t. *Table 4. Data Element B, Essential, MPS Component P, Transfer "No Evidence..." does not appear to align with Table 3, Transfer, Essential, "Digital Error Detection".* Table 4 is intended to provide an example that includes some of the shortfalls that may be encountered. The guidance surrounding Table 4 will be revised to make this clearer.

DGTA-ADF POSITION

150. The comments received for this NPRM were useful and many have resulted in improvements to the Flight and Mission Planning System chapter. These improvements are described in each of the 'response' sections presented in the previous section of this document. The revised Flight and Mission Planning System chapter, presented at enclosure 1, will be incorporated into the next amendment of AAP 7001.054.



J. ADAMS

Group Captain

Director Aviation Engineering

Directorate General Technical Airworthiness – ADF

Tel: (03) 9256 3358

29 ^{November}
~~October~~ 10

Annex:

A. List of Respondents

Enclosure

1. Revised AAP 7001.054 Section 2 Chapter 24 Flight and Mission Planning Systems

NPRM DGTA 03-09 LIST OF RESPONDENTS

Commonwealth Respondents:

WGCDR Andrew Gillman, PEM AIR7000
WGCDR Rick Pacey, CENGR ALSPO
WGCDR Scott Parry, HUG PEM TFSPO
SQNLDR Wendell Fox, MRH Avionics Engineering Manager
SQNLDR Damien Hare, CENGR AMTDU
FLTLT Justin Taylor, ENG2C AIR7000
MR Tim Wedding, Airworthiness Engineer – MPS, CISSO

Commercial Respondents:

MR Pieter de Waard, SDE MRHPMO, Australian Aerospace

Respondents that did not consent to being named: 2 respondents

Total of 10 Respondents