US Government Protection Profile for
Database Management Systems in Basic Robustness Environments

General Description of Changes from version 1.0 to version 1.1:

The "US Government Protection Profile for Database Management Systems in Basic Robustness Environments" Version 1.0 was validated on 30 September 2004. Vendor community representatives met on 4 May 2005 and compiled a list of comments and concerns based on the pre-validated version of the Protection Profile (PP). The PP author representatives met with the vendor representatives to discuss their comments and updated the validated DBMS version 1.0 protection profile. This update attempts to address vendor community comments and concerns. Please find below a detailed explanation of the changes made to produce version 1.1.

Detailed Description of Changes from version 1.0 to version 1.1:

1. Changed definition of Authorized Administrator to "An authorized person in contact with the Target of Evaluation who is responsible for maintaining its operational capability."

2. All assumptions, except for A.PHYSICAL, A.NO_EVIL, and A.NO_GENERAL_PURPOSE, were removed because environmental requirements were removed. See below for more details.

3. An assumption, A.OS_PP_VALIDATED, was added that states "It is assumed that the underlying OS has been validated against an NSA sponsored OS PP of at least Basic Robustness."

4. All environmental objectives, except OE.PHYSICAL, OE.NO_EVIL, and OE.NO_GENERAL_PURPOSE, were removed as well as all environmental requirements. These requirements cannot be verified in a PP evaluation. In order for easier concurrence with the published Basic Robustness OS PPs, these requirements, objectives, and assumptions were removed.

5. Environmental objective was created to corresponds to the newly created assumption A.OS_PP_VALIDATED. This objective is called OE.OS_PP_VALIDATED and states "The underlying OS has been validated against an NSA sponsored OS PP of at least Basic Robustness."

6. Since the PP definition of a Discretionary Access Control (DAC) Policy refers to users and or groups, changes were made throughout the document to reflect users and/or groups versus requiring access control to be specific to users or specific to groups.

7. The application note after FMT_MSA.1.1 was updated. In addition to this, "of database users" was removed from the requirement text because this policy refers to all security attributes in the TOE, not only those pertaining to the user.

8. The security attribute "object identity" was added in FDP_ACF.1.1.

9. An application note was added to FDP_ACF.1.2 to state that an explicit deny list is not needed to satisfy this requirement.

10. An application note was added to FAU_SEL.1 to clarifying the intent to capture enough audit data, not necessarily capture only needed audit data.

11. The term "subjects and" was removed from requirement FMT_REV.1.1(2).

12. The explicit requirement FPT_ITD_(EXP).1 was removed.

13. The second element of FPT _SEP_(EXP).1 was mislabeled as FPT_SEP_(EXP).2. It was changed to read FPT_SEP_(EXP).1.2.

14. An application note was added to FPT_SEP_(EXP).1 to clarify that the security domain in the first element does not need to have the same scope as the security domain mentioned in the second element.5

15. An application note was added to FPT_TRC_(EXP).1 to state this requirement is only necessary if the TOE is physically separated, otherwise it can be trivially met by stating the TOE has no physically separated parts.

16. Requirement FTA_TAB.1 was removed from the PP. TOE access banners cannot be met by a basic robustness PP. Since there is no requirement for a client within the TOE, there is no way to display an access banner.

17. FTA_TAH.1 was removed and replaced with an explicit requirement stating the TOE must store and retrieve the login history, instead of display the access history. References to location and method were removed from the explicit requirement. FTA_TAH.1 as it was written could not be satisfied by a software-only basic robustness DBMS. Since the client is not part of the TOE, the TSF cannot require the client to display such a notice.

18. The FTA_TSE.1 requirement was removed because it makes assumptions based on the client, which is not part of the TOE boundary.

19. The requirement for TSF testing, FPT_TST_(EXP).1, was removed.

20. The element FMT.MSA.3.2 was removed and the component FMT.MSA became an explicit component (i.e., FMT.MSA_EXP), which only has one element that requires default restrictive values upon, object creation. This explicit requirement makes the component more restrictive by requiring the security attributes of the objects on creation to be restrictive and not allowing any user to be able to override the restrictive default values.

21. FAU_GEN.2.1-NIAP-0410: This requirement was replaced by FAU_GEN_(EXP).2. It is basically the same requirement with 'user identity' replaced with 'user identity and/or group identity'.

22. FAU_SEL.1.1-NIAP-0407: This did not need to be made explicit since the change was made within an assignment. 'User Identity' was changed to 'User Identity and/or Group Identity'.

23. FTA_TSE.1.1: This did not need to be made explicit since the change was made within an assignment. 'User Identity' was changed to 'User Identity and/or Group Identity'.

24. Section 6.3: Rational was updated to reflect the notion of user identity and/or group identity.

25. Named Object in the glossary was updated to allow user and/or group identity.

26. The application note for FPT_SEP_(EXP).1 was updated.

27. A reference to the "TOE boundary" figure was removed since the actual figure was removed in a previous version because the TOE boundary changed.

28. The following text was added to T.ACCIDENTAL_AUDIT_ COMPROMISE: "Even though the audit mechanism may be provided by the TOE, and included in the ST, it is not required for this basic robustness DBMS".

29. Added an application note to FDP_ACF.1.2-NIAP-0407."

30. FDP_ACF.1.3-NIAP-0407. Requirement modified to "[selection: assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects], "no additional rules"]." Because the previous version did not allow for a selection (misplaced brackets).

31. An application note was added to FIA_ATD.1.1 to clarify the intent of this particular requirement.

32. FTA_MCS.1.2. Previous version did not indicate that this is a refinement and did not allow for a selection (misplaced brackets).

    FDP_ACF.1.2-NIAP-0407 was changed to specify to sets of DAC rules in more detail within a selection.

33. Other changes were made throughout the document were grammatical in nature (i.e. misuse of punctuation, irregular capitalization, etc).

34. All explicit requirements were changed from (EXP) to "EXP", which is consistent with conventions in othe NSA protection profiles.

35. Requirement FDP_RIP.2 was changed to FDP_RIP.1 for compliance to Basic Robustness Protection Profile requirements.