Change Proposal – F40/01 (Page 1 of 2)	CP No: 933 v2 *(mandatory by BSCCo)*

Title *(mandatory by originator)*

NHHDA and EAC/AA Systems – Management of System Security

Description of Change *(mandatory by originator)*

At present the NHHDA and EAC/AA applications provide no facilities for the maintenance of user accounts through the front end. The users are currently created by the Database Administrator who sets both the username and the password. User passwords do not expire and there is no facility for users to modify their passwords. This has been raised as an issue during a number of audits.

CP933 v1.0 was discussed by the Software Technical Advisory Group (STAG), who requested that a new version of the Change Proposal be raised to detail a revised solution, which would allow a suitably privileged user to create accounts, modify accounts and change passwords.

Proposed Solution(s) *(mandatory by originator)*

It is proposed that the initial user would be created by the Oracle Database Administrator and granted the System Manager role. The System Manager role will be able to create, modify and delete accounts within the application. They will also be able to change user passwords, enable and disable user accounts, and grant roles to each user. All other users would be able to view their own information only and modify their own password.

It is proposed that the following account information is audited using the existing audit log (currently only used to for the change to the smoothing parameter):
- Creation/Deletion of new users
- Granting/Revoking of roles
This information will only be audited if details are changed through the front end of the application.

It should be noted that locked accounts can only be unlocked by a System Manager changing the user's password and that expired accounts will require the user to enter a new password when they next login. It should also be noted that a System Manager needs to enter their own password and not the current password of the user whose details are being modified.

Justification for Change *(mandatory by originator)*

Enhancement of system security to meet audit controls.

Other Configurable Items Potentially Affected by Proposed Solution(s) *(optional by BSCCo)*

Impact on Core Industry Documents *(optional by originator)*

Related Changes and/or Projects *(mandatory by BSCCo)*