The following changes are being made:

1. Prevent new user from taking an active license
   1. New users are assigned 'Requestor' by default and must submit a separate request to gain active status. Ensures user access control and compliance with role-based security policies.
2. Update to the Calibration Standards tab
   1. Enhancing the **Calibration Standards tab** by displaying **Lot locations** for calibration records in the Standards Used section of Work Orders, ensuring compliance with calibration data storage requirements, including **instrument categories, calibration limits, and standard tracking**.
3. Update to the View All Equipment Update Requests screen
   1. Adjusting visibility settings in the Equipment Update Requests module by restricting access to the QA Review field, enforcing data access controls per system permissions.
4. Updating the Audit Trail report
   1. Enhancing Audit Trail report functionality by implementing a flagging mechanism when comments exceed 3000 characters, ensuring accurate logging and traceability in compliance with record-keeping standards.
5. Updating the Location on the Work Order Report
   1. Enhancing CMMS **Cognos reporting functionality** by ensuring **Work Order reports** accurately reflect **location data**, improving compliance with system-generated reporting standards and traceability.
6. Removing a Forgot Password button
   1. Strengthening authentication security by **removing the Forgot Password recovery function** to **enforce LDAP authentication policies**, ensuring application login strictly adheres to **corporate IT security policy** and requires standard **network username and password credentials**
7. Fixing spelling mistakes in the Audit Trail
   1. Maintaining **system audit trail integrity** by correcting **event log formatting inconsistencies** in audit records. This ensures compliance with **system-generated audit trail storage, IT Change Control policies, and time-zone-based log retention as configured by the CMMS application server**.
8. Adding ability to see last login of user
   1. Implementing a Last Login timestamp field in the User Setup screen to enhance user authentication tracking and facilitate compliance with login monitoring policies.
9. Modifying the ECDB Menu
   1. Restricting ECDB menu visibility to specific user roles based on access permissions, enforcing compliance with role-based access controls.