Oh Say Can You See?
(CMMS/EAM System Security Sanity)

When thinking about establishing system security within a CMMS or EAM a couple of things must be defined. The first decision must be what the user roles for the system will be. These roles should be developed for each of the day to day users of the system (i.e. Maintenance, Management, Materials Management, Purchasing, etc.). Then, what access, information, and system views do you want each defined role to see and do within the system?

Ideally, a majority of the answers on which roles must be defined could quickly be identified by reviewing the work management workflows and processes defined during implementation. System security must be developed for each specific role defined. Some of the obvious things you'll want to consider making "invisible" to a user could be pay rates and personal contact information. Additionally, consider if a particular field or fields within a record view does not apply to the role make them "invisible". Hiding or making fields "invisible" for unused fields within a system makes it easier to utilize and less cluttered for the users and will only display the information pertinent to that specific role.

People and Processes, Inc.