InCommon Certificate Service - DRAO Responsibilities

Responsibilities of the DRAO

1. Should know how to use the InCommon Certificate Manager Admin Tool for managing certificates as documented in the InCommon Certificate Manager Administrator Guide (mainly chapters 1 and 2)
2. Request from the RAO only subdomains in campus DNS you should be allowed to approve certificate requests for in your department
3. Communicate to your department the process for people to request SSL certificates (see example)
4. When new requests come in, you should do ALL of the following before approving a request:
   a. Verify email address of requester is in the UCI directory, be careful of similar looking letters/numbers
   b. Verify you know the person making the request, or contact them if they don't
   c. Verify they are an "owner" of the system and that the CN is registered properly in DNS
   d. Verify there is a legitimate business need for the request
   e. Verify all required information submitted with the CSR is correct from the user
      i. Verify certificate type is proper
      ii. Verify subject alternative names (if applicable) are valid