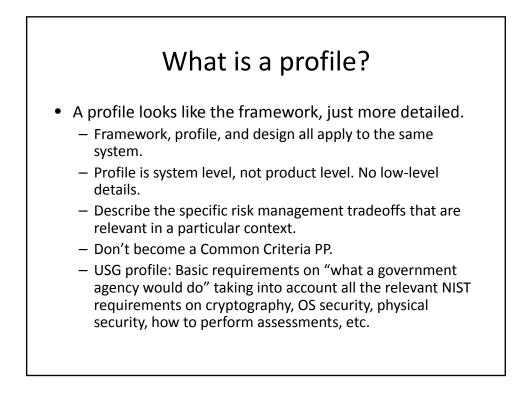
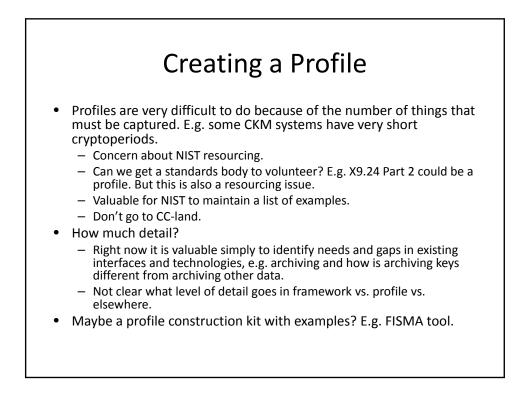
Profile Breakout – Group A

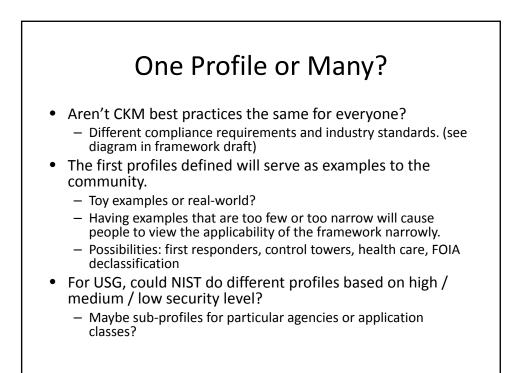
- Most discussion about:
 - Scope of profiles
 - Construction of profiles
 - Conformance
- Still lots of discussion about scoping and what various words mean profile, design, etc.
- However, this is a very complex area and the consensus was that having a framework and profile is valuable.

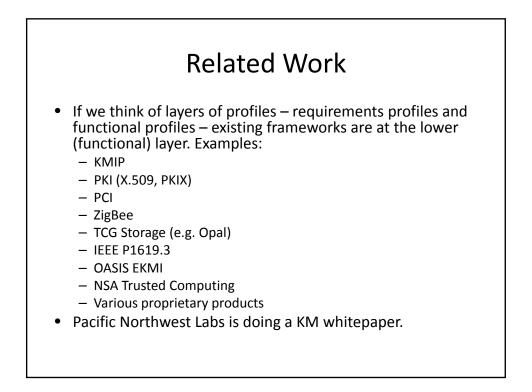


Layers of Profiles

- Is the profile really a requirements profile or a design profile? E.g. customers could generate requirements profiles and vendors could generate design profiles that try to match.
 - Or maybe we say "security requirements" vs. "design requirements".
 - Or maybe we have profiles for functional units.
 - Or maybe application classes (e.g. web apps).
- Layers of profiles
 - Each profile fleshes out the parent profile for a specific context. Refine until you get to a vendor profile.
 - But too many profiles would get confusing. More than two layers is probably overkill.
- How do "company policy and standards" interact with this? Are they outside the profile or part of it?







Assessments

- Who is responsible?
 - Customer does the assessment for the as-deployed system.
 - Profile needs to specify assurance procedure and product responsibilities
 - Vendor tries to meet profile in their design
- What do we measure conformance of?
 - Profile: Body that writes the profile has a review process.
 - Design document: Product should be well documented and enable safe implementation choices. Profile should specify what needs to be documented.
 - Specific deployment: Too hard
- What is NIST's role?
 - These are complex systems, and the only artifact is documentation.
 - NIST could do validation for the USG profile. Maybe just an RFI-style process would be enough.
 - Don't want to end up with another expensive CC-style process.
 - Maybe we need to wait until we have a profile so we can understand this further. Not clear how much value is added by complex validation.

