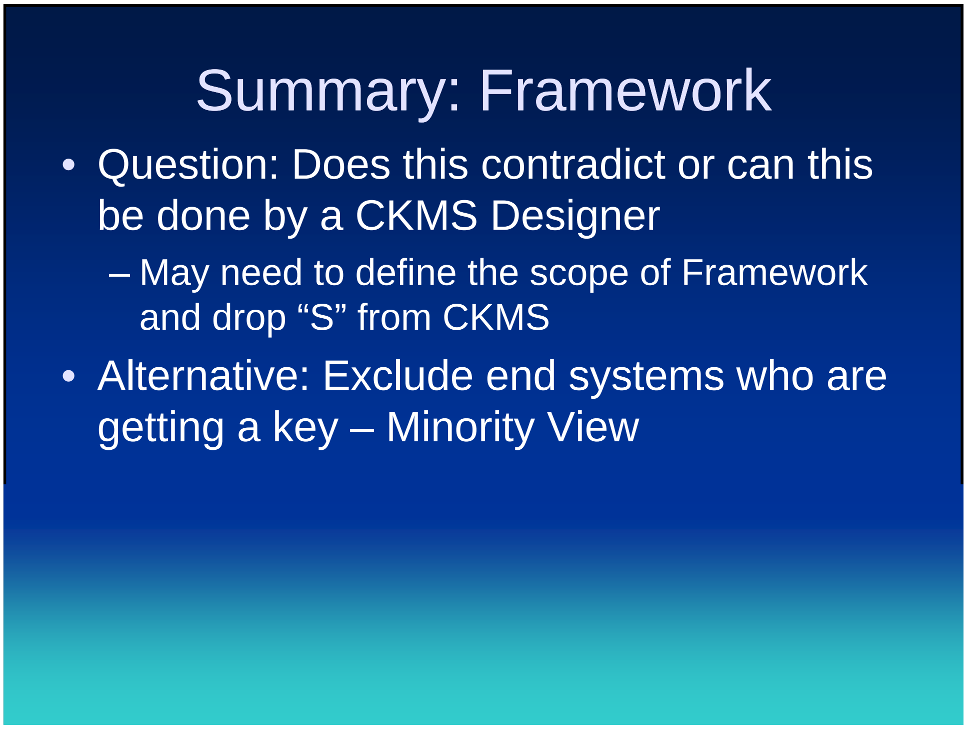
Workshop Summary

Santosh Chokhani

NIST Key Management Workshop

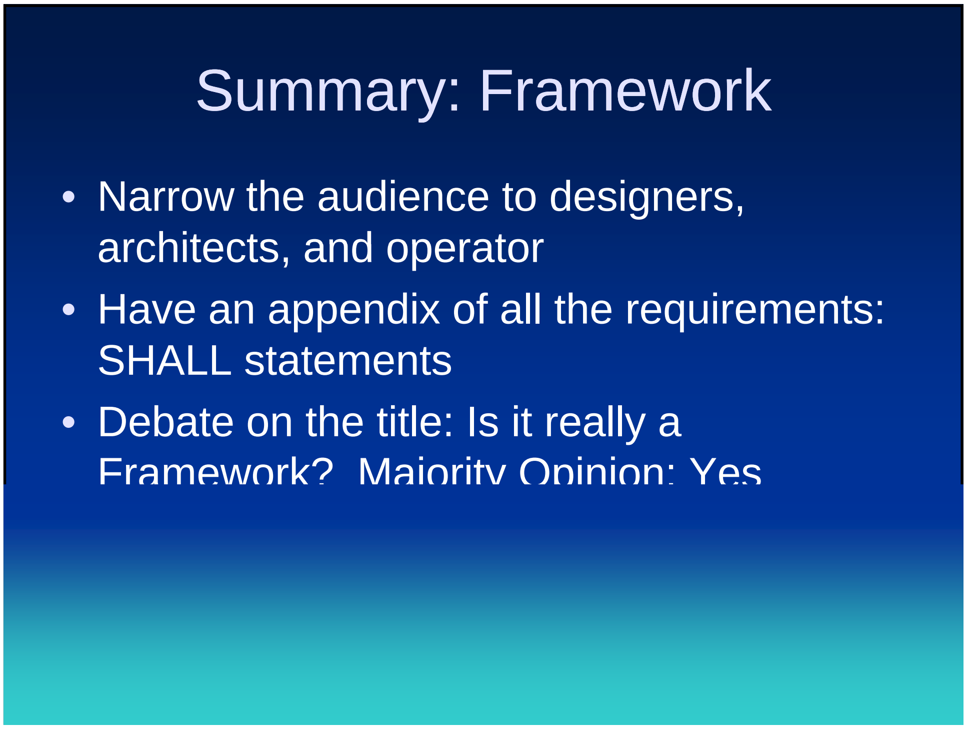
Summary: Framework

- Think about CKM requirements on IS as opposed to thinking about a CKMS as being distinct
  - – Scope includes any device or system that generates, stores, uses or otherwise touches a key or associated critical security parameters



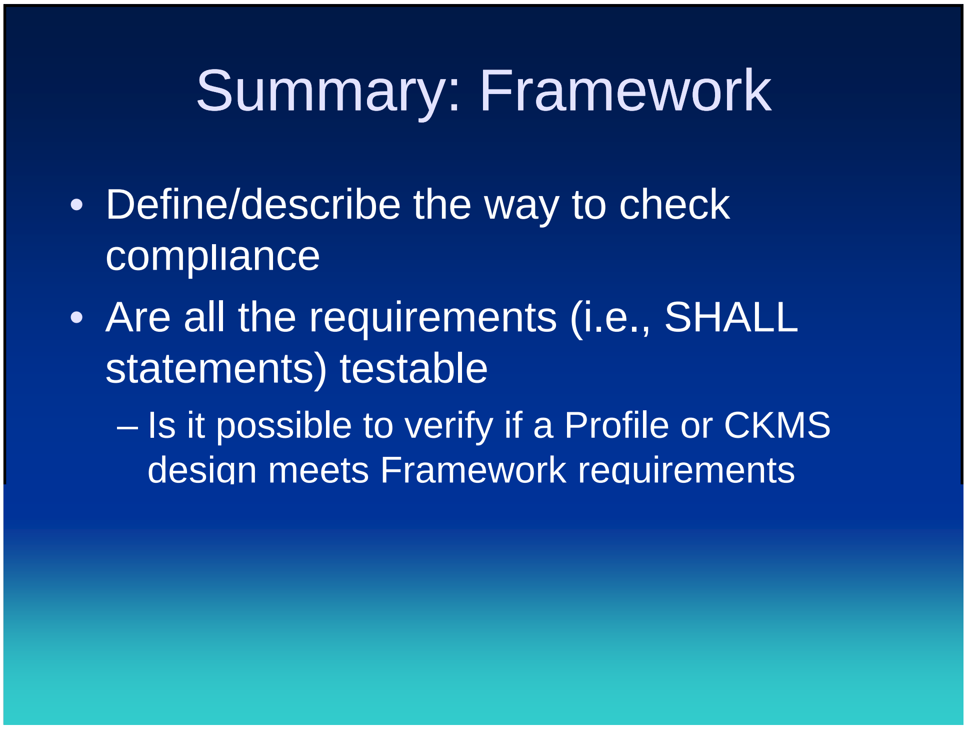
Summary: Framework

- Question: Does this contradict or can this be done by a CKMS Designer
  - May need to define the scope of Framework and drop “S” from CKMS
- Alternative: Exclude end systems who are getting a key – Minority View



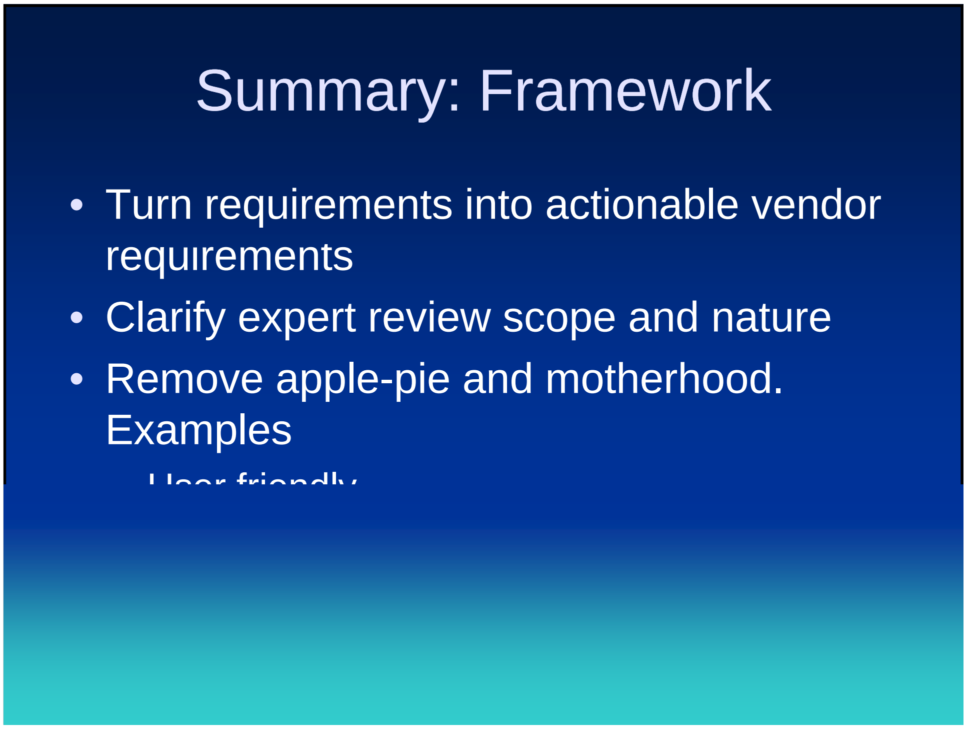
Summary: Framework

- Narrow the audience to designers, architects, and operator
- Have an appendix of all the requirements: SHALL statements
- Debate on the title: Is it really a Framework? Majority Opinion: Yes



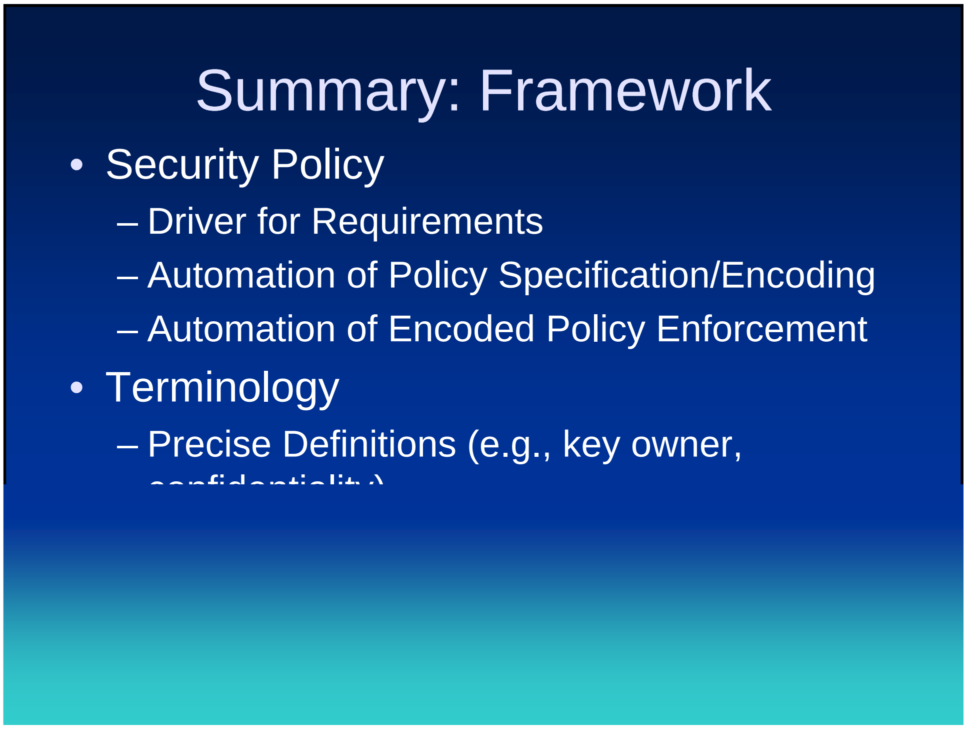
Summary: Framework

- Define/describe the way to check compliance
- Are all the requirements (i.e., SHALL statements) testable
  - Is it possible to verify if a Profile or CKMS design meets Framework requirements



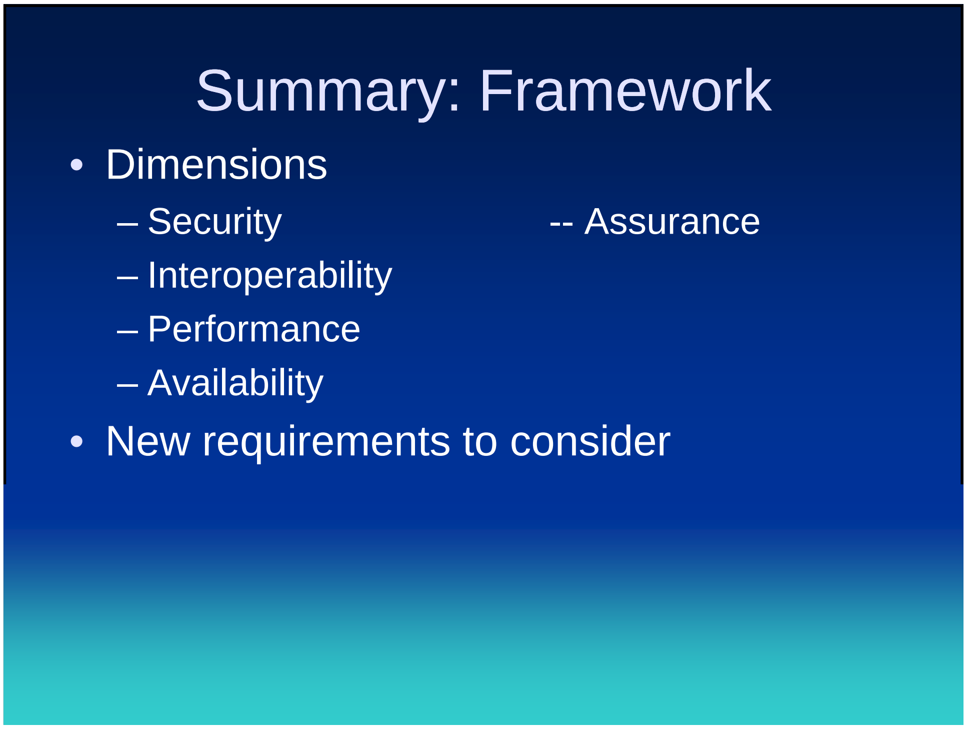
Summary: Framework

- Turn requirements into actionable vendor requirements
- Clarify expert review scope and nature
- Remove apple-pie and motherhood. Examples
  - User friendly



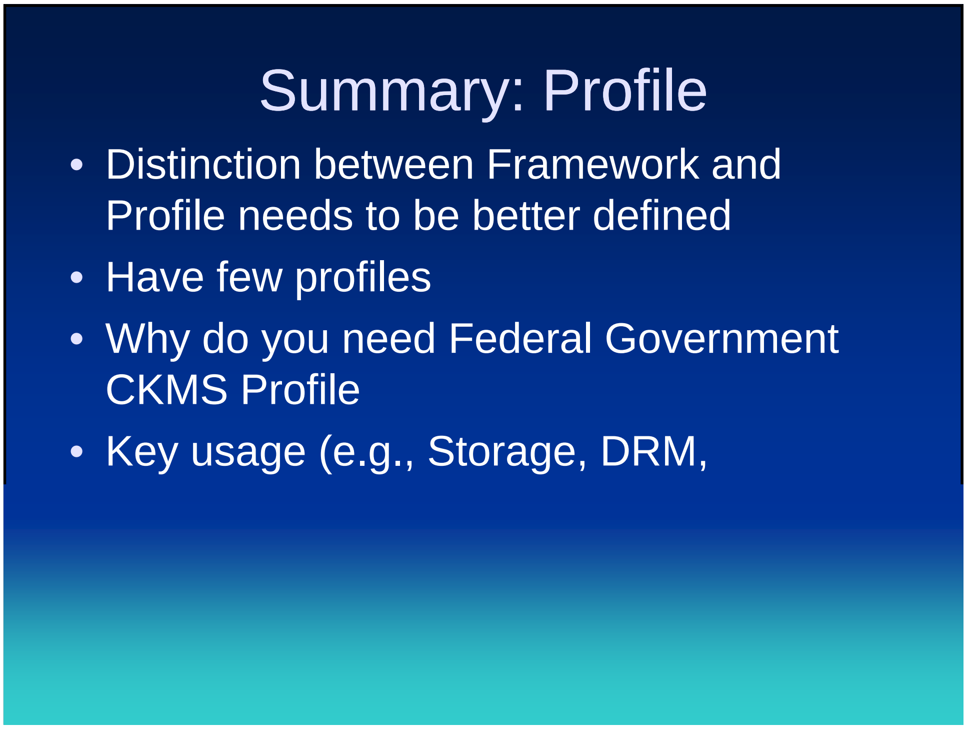
Summary: Framework

- Security Policy
  - Driver for Requirements
  - Automation of Policy Specification/Encoding
  - Automation of Encoded Policy Enforcement
- Terminology
  - Precise Definitions (e.g., key owner, confidentiality)



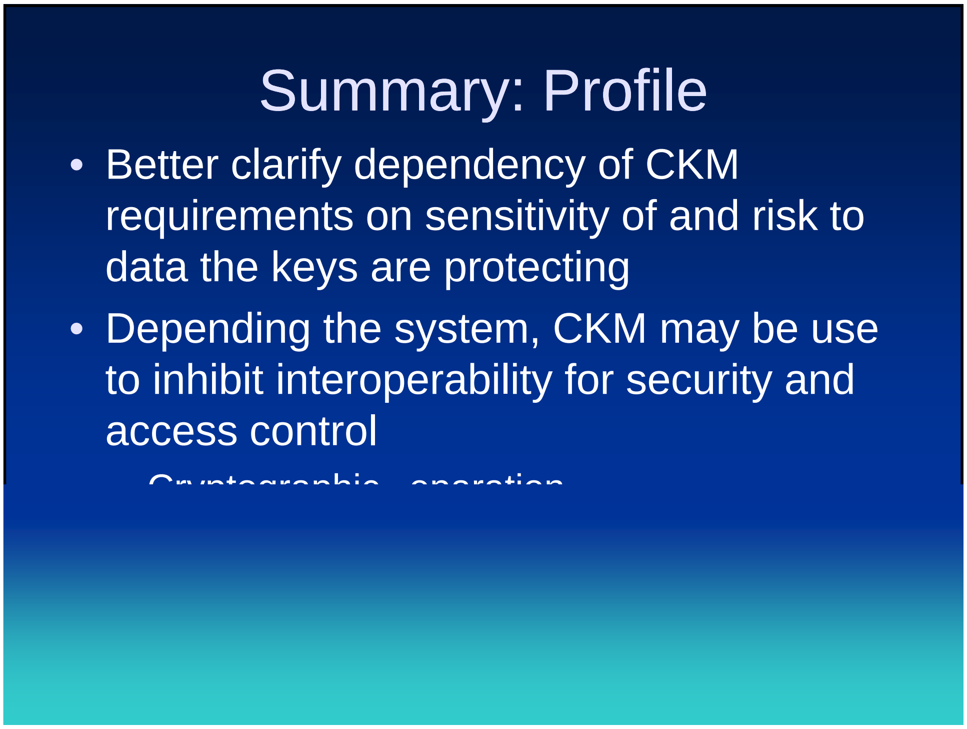
Summary: Framework

- Dimensions
  - Security -- Assurance
  - Interoperability
  - Performance
  - Availability
- New requirements to consider



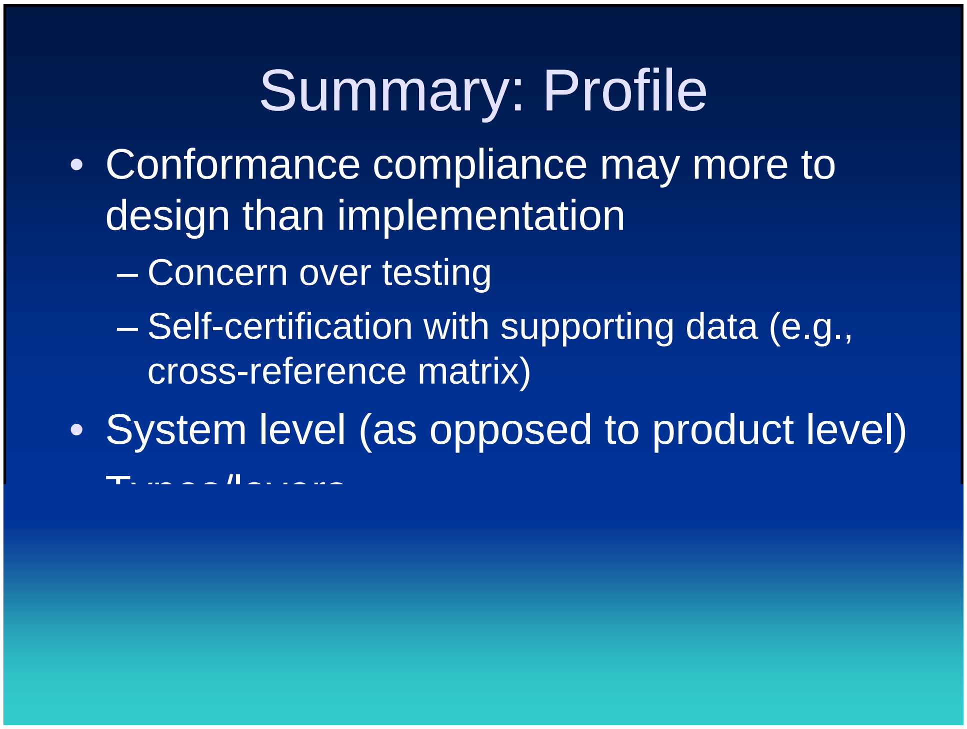
Summary: Profile

- Distinction between Framework and Profile needs to be better defined
- Have few profiles
- Why do you need Federal Government CKMS Profile
- Key usage (e.g., Storage, DRM,



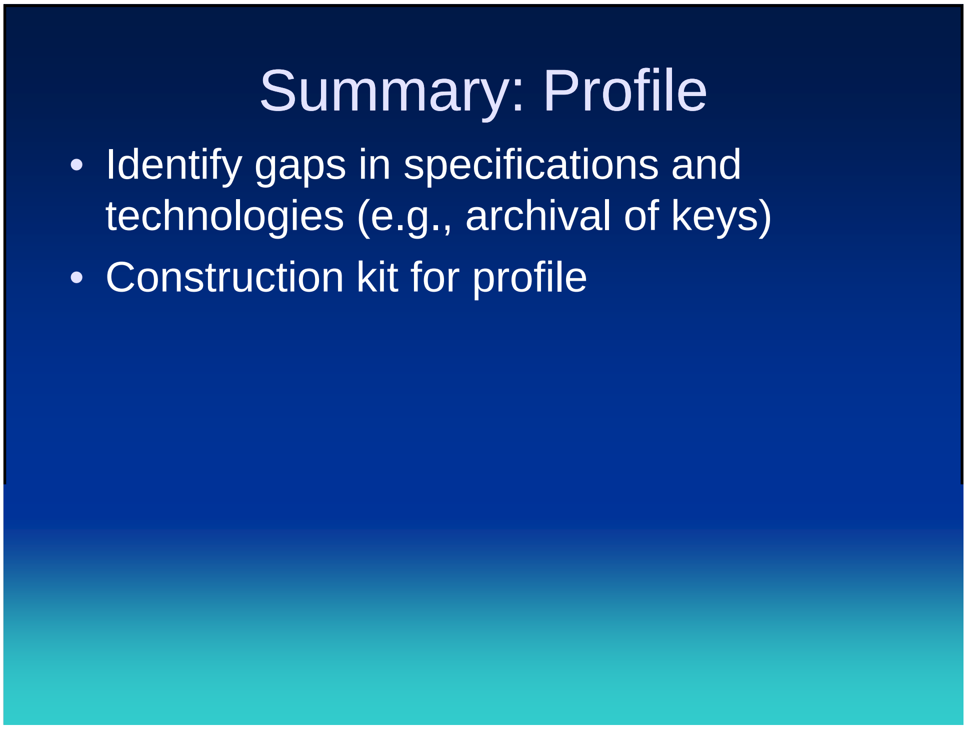
Summary: Profile

- Better clarify dependency of CKM requirements on sensitivity of and risk to data the keys are protecting
- Depending the system, CKM may be use to inhibit interoperability for security and access control
  - Cryptographic operation



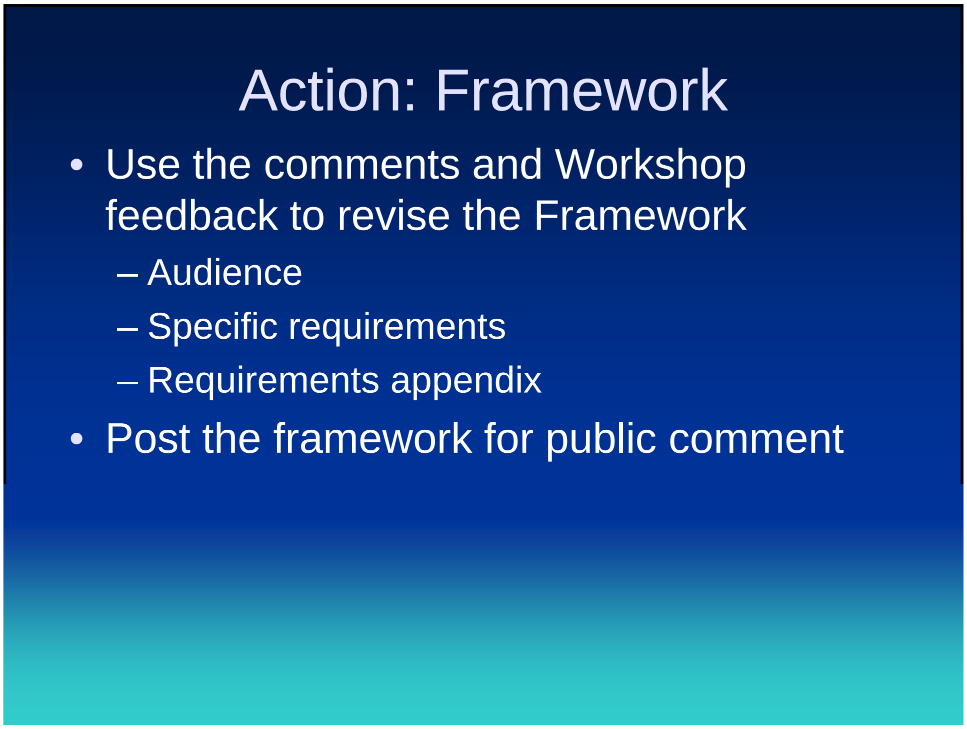
Summary: Profile

- Conformance compliance may more to design than implementation
  - Concern over testing
  - Self-certification with supporting data (e.g., cross-reference matrix)
- System level (as opposed to product level)
- Types/layers



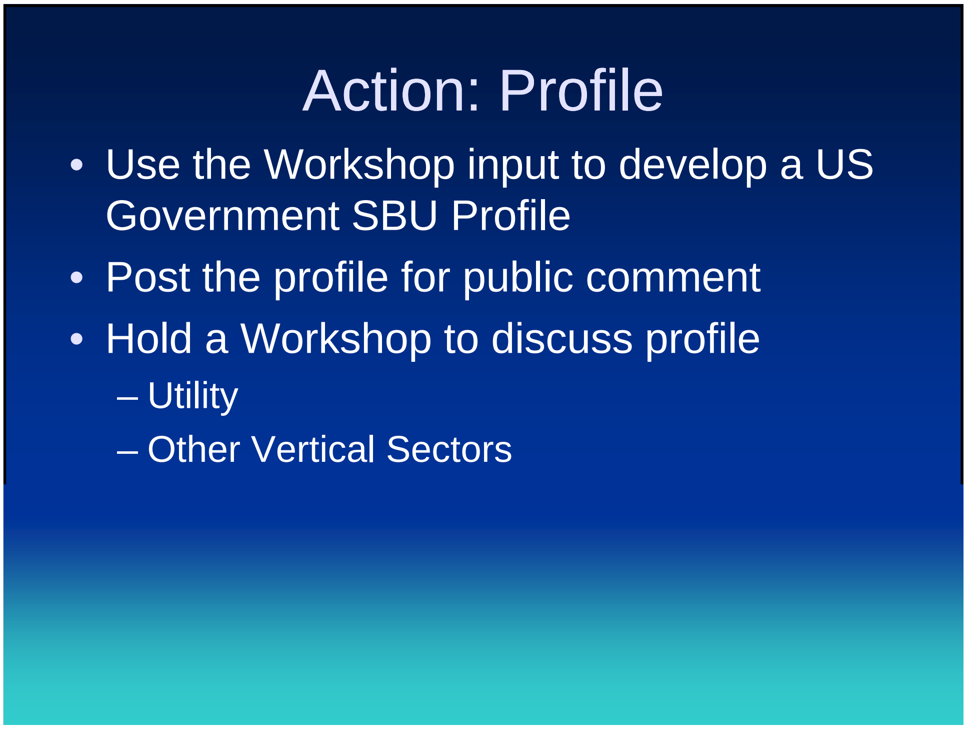
Summary: Profile

- Identify gaps in specifications and technologies (e.g., archival of keys)
- Construction kit for profile



Action: Framework

- Use the comments and Workshop feedback to revise the Framework
  - Audience
  - Specific requirements
  - Requirements appendix
- Post the framework for public comment



Action: Profile

- Use the Workshop input to develop a US Government SBU Profile
- Post the profile for public comment
- Hold a Workshop to discuss profile
  - Utility
  - Other Vertical Sectors

Discussion?