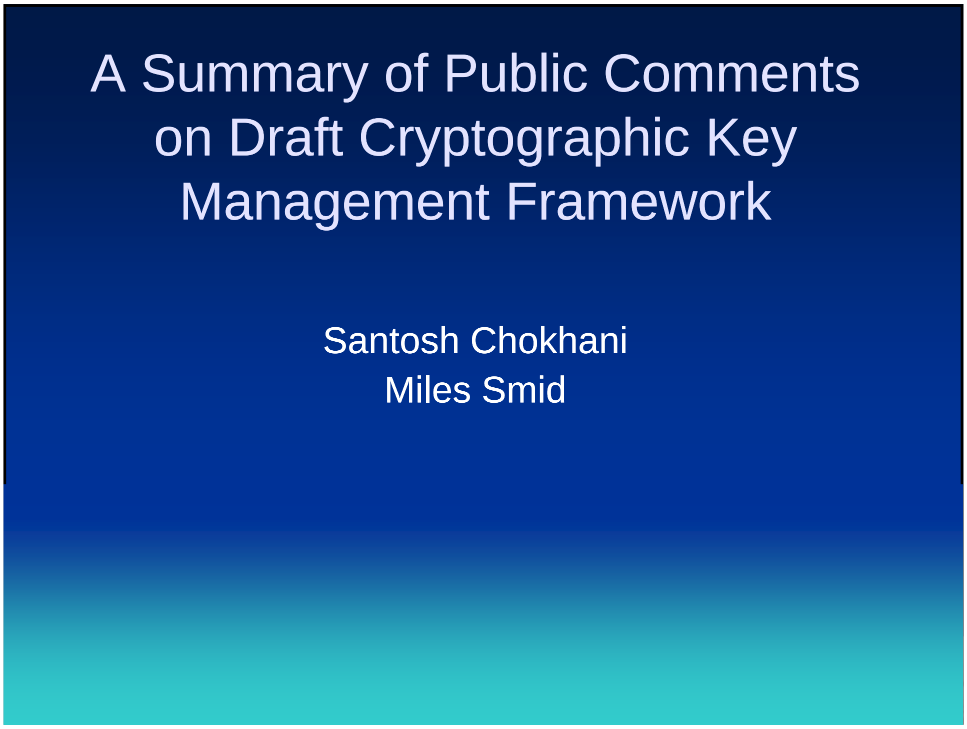
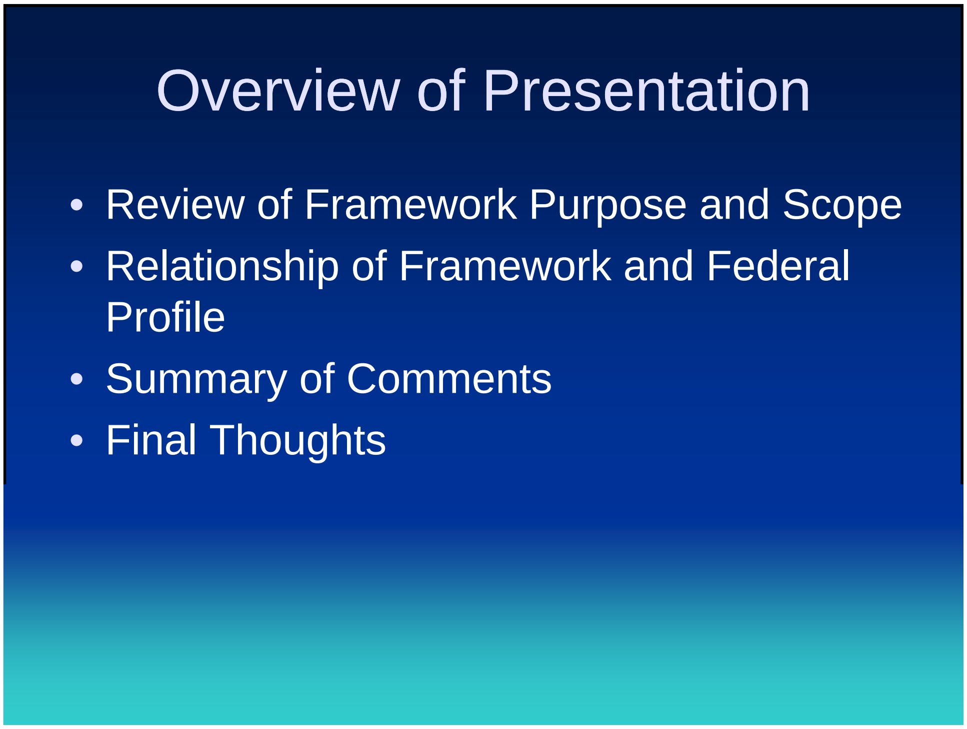


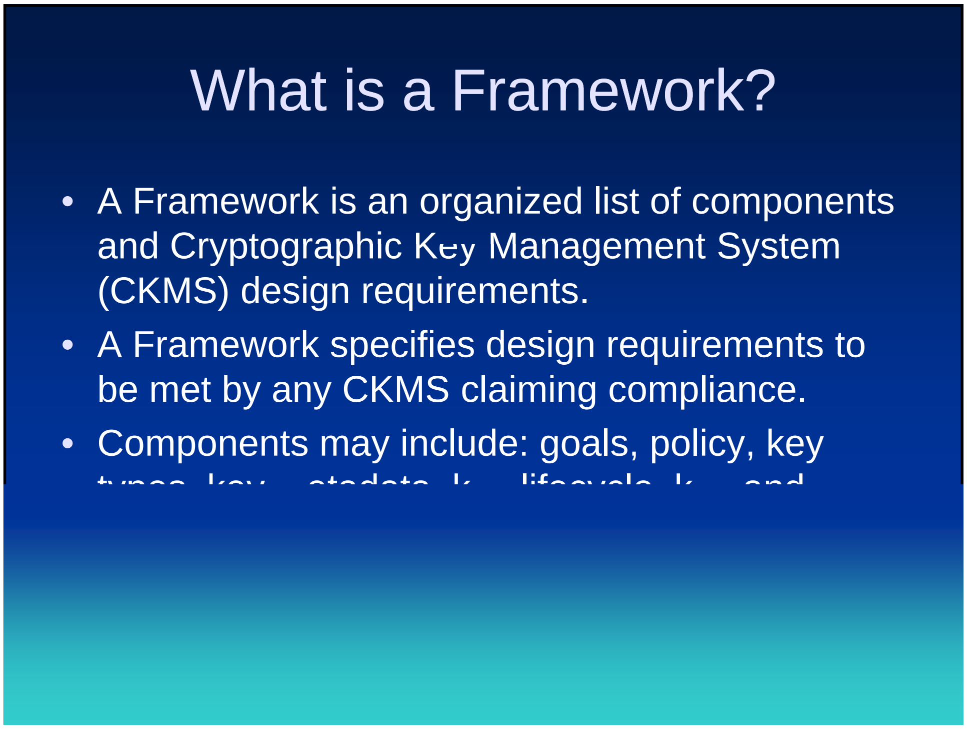
A Summary of Public Comments on Draft Cryptographic Key Management Framework

Santosh Chokhani
Miles Smid



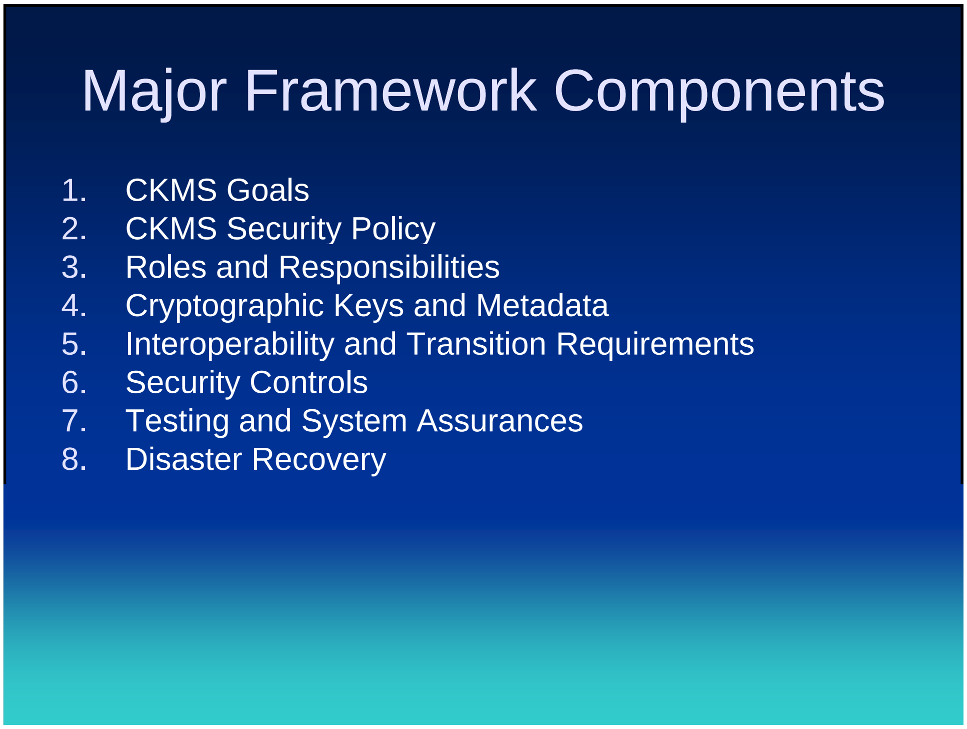
Overview of Presentation

- Review of Framework Purpose and Scope
- Relationship of Framework and Federal Profile
- Summary of Comments
- Final Thoughts



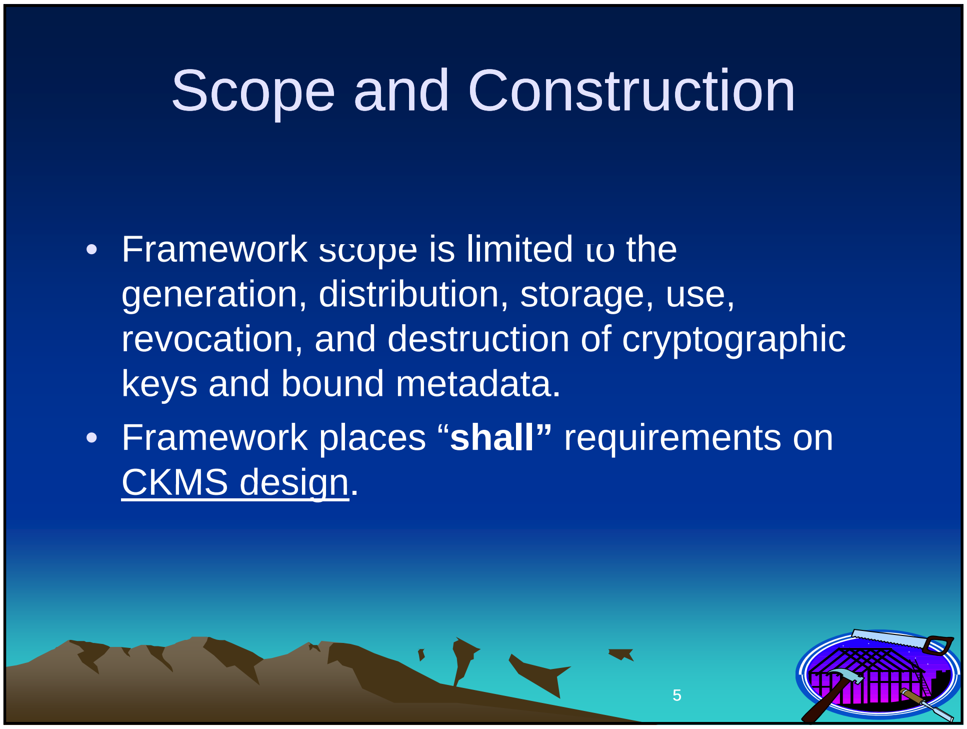
What is a Framework?

- A Framework is an organized list of components and Cryptographic Key Management System (CKMS) design requirements.
- A Framework specifies design requirements to be met by any CKMS claiming compliance.
- Components may include: goals, policy, key types, key metadata, key lifecycle, key and



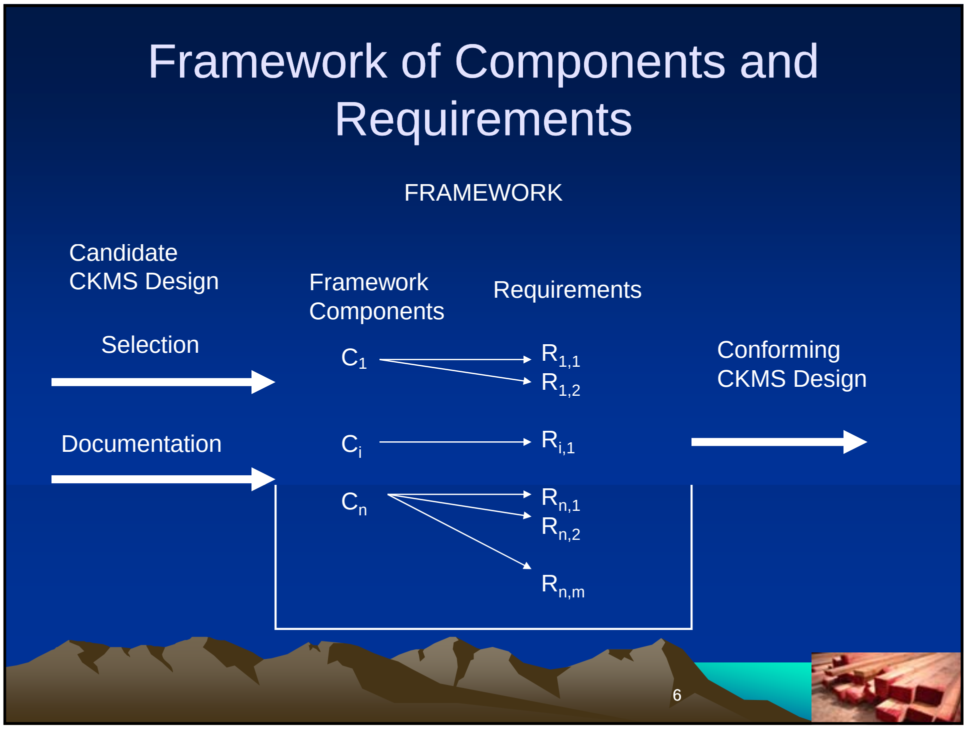
Major Framework Components

1. CKMS Goals
2. CKMS Security Policy
3. Roles and Responsibilities
4. Cryptographic Keys and Metadata
5. Interoperability and Transition Requirements
6. Security Controls
7. Testing and System Assurances
8. Disaster Recovery



Scope and Construction

- Framework scope is limited to the generation, distribution, storage, use, revocation, and destruction of cryptographic keys and bound metadata.
- Framework places “**shall”** requirements on CKMS design.



Framework of Components and Requirements

FRAMEWORK

Candidate CKMS Design

Selection

Documentation

Framework Components

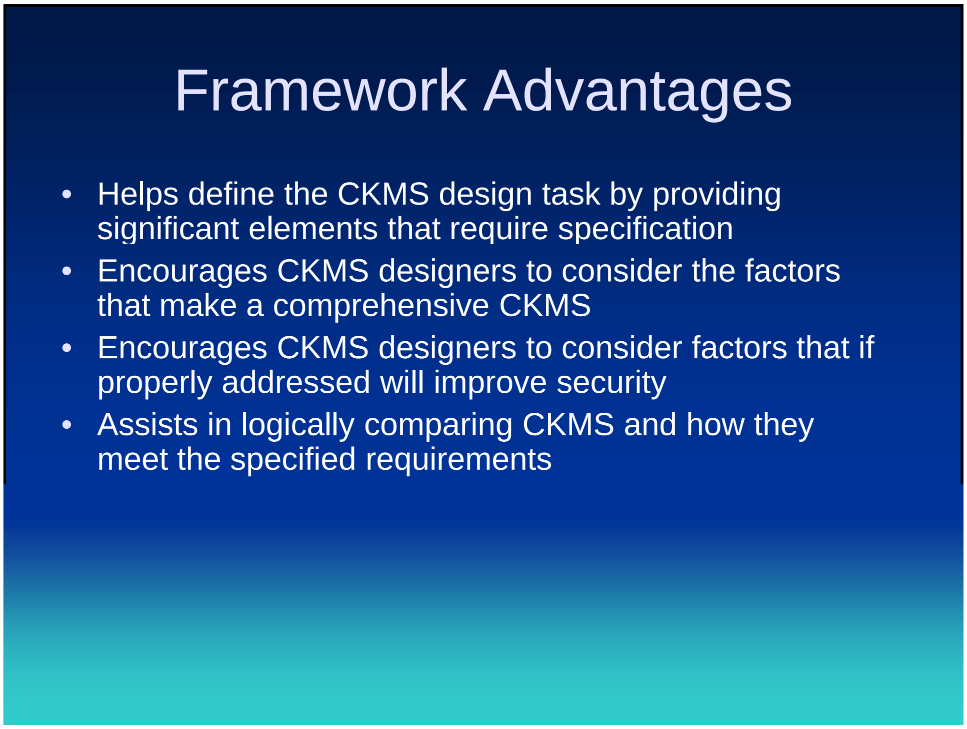
Requirements

C_1 → $R_{1,1}$, $R_{1,2}$

C_i → $R_{i,1}$

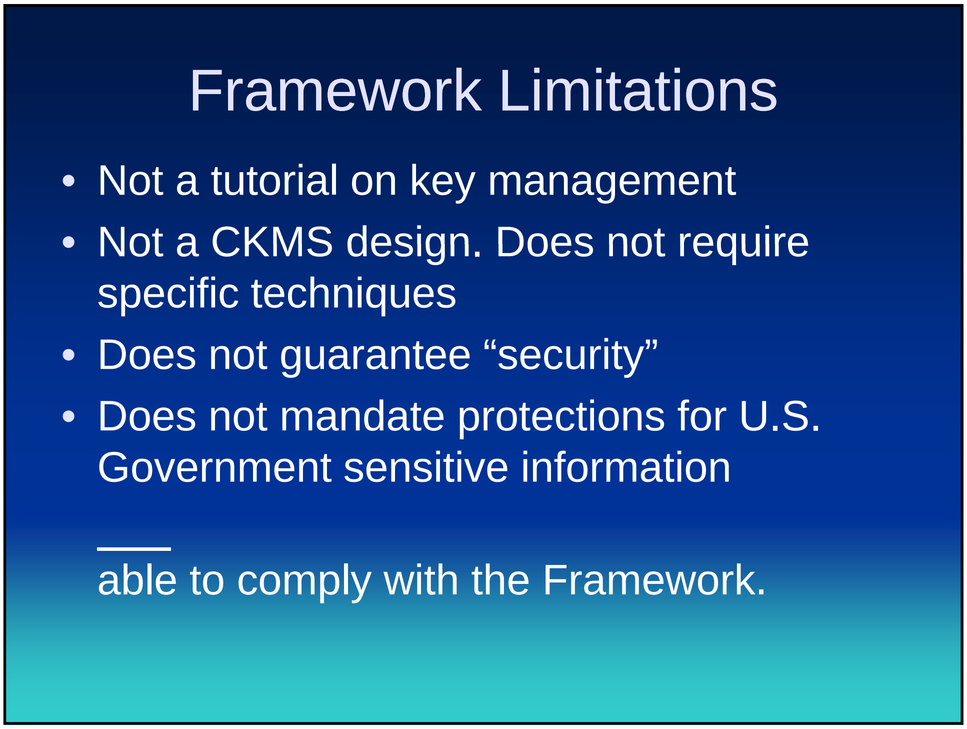
C_n → $R_{n,1}$, $R_{n,2}$, $R_{n,m}$

Conforming CKMS Design



Framework Advantages

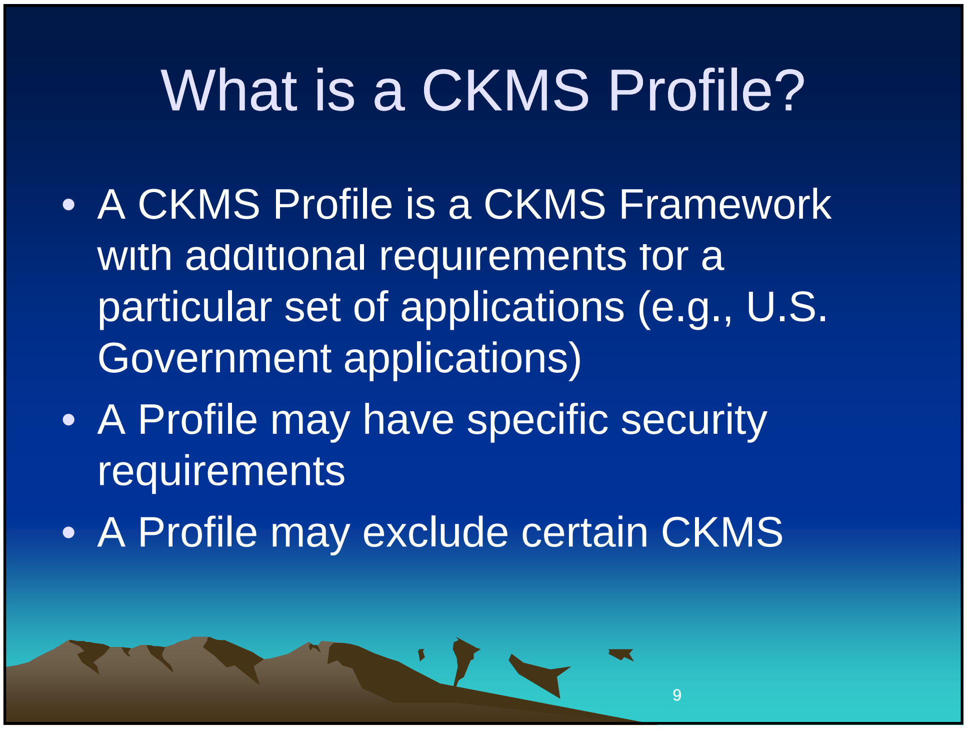
- Helps define the CKMS design task by providing significant elements that require specification
- Encourages CKMS designers to consider the factors that make a comprehensive CKMS
- Encourages CKMS designers to consider factors that if properly addressed will improve security
- Assists in logically comparing CKMS and how they meet the specified requirements



Framework Limitations

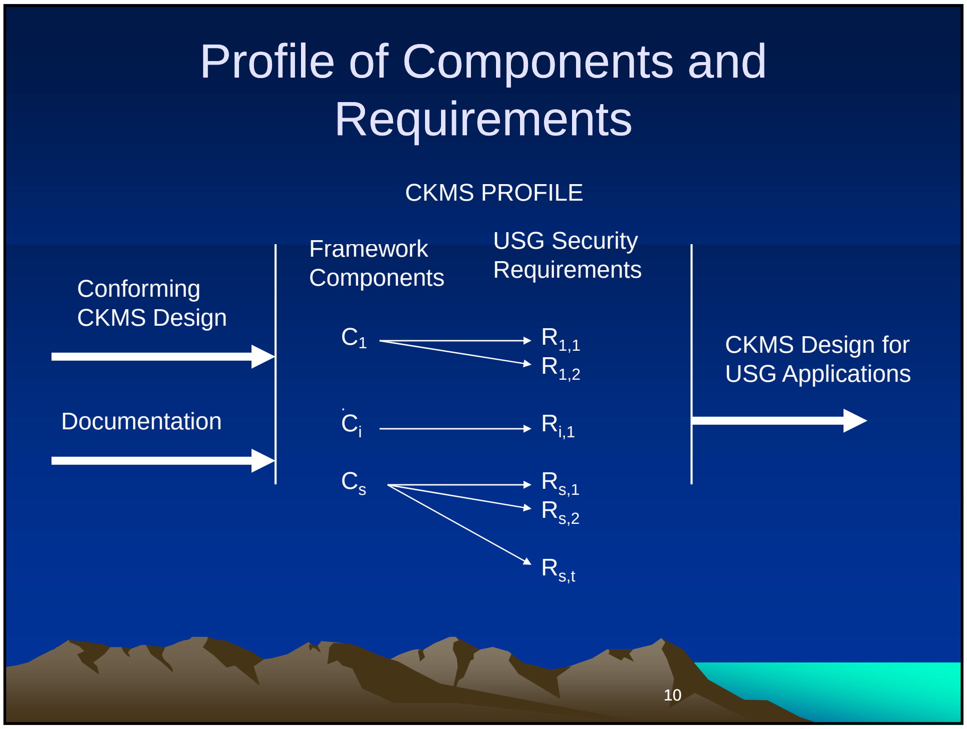
- Not a tutorial on key management
- Not a CKMS design. Does not require specific techniques
- Does not guarantee “security”
- Does not mandate protections for U.S. Government sensitive information

able to comply with the Framework.



What is a CKMS Profile?

- A CKMS Profile is a CKMS Framework with additional requirements for a particular set of applications (e.g., U.S. Government applications)
- A Profile may have specific security requirements
- A Profile may exclude certain CKMS



Profile of Components and Requirements

CKMS PROFILE

Conforming CKMS Design

Documentation

Framework Components

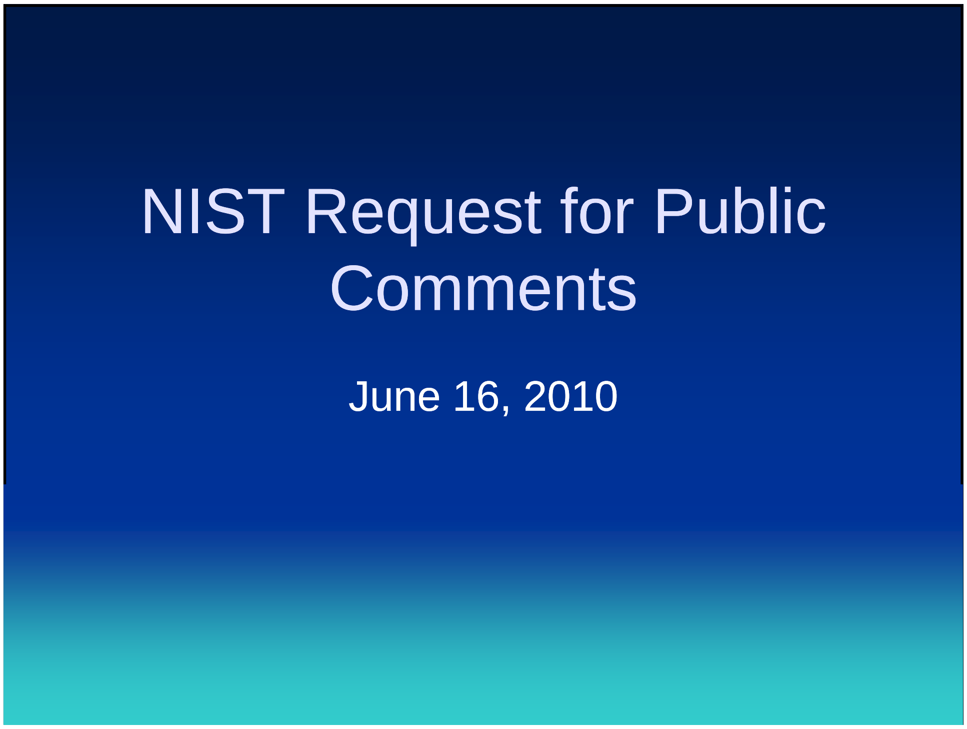
USG Security Requirements

C_1 → $R_{1,1}$, $R_{1,2}$

C_i → $R_{i,1}$

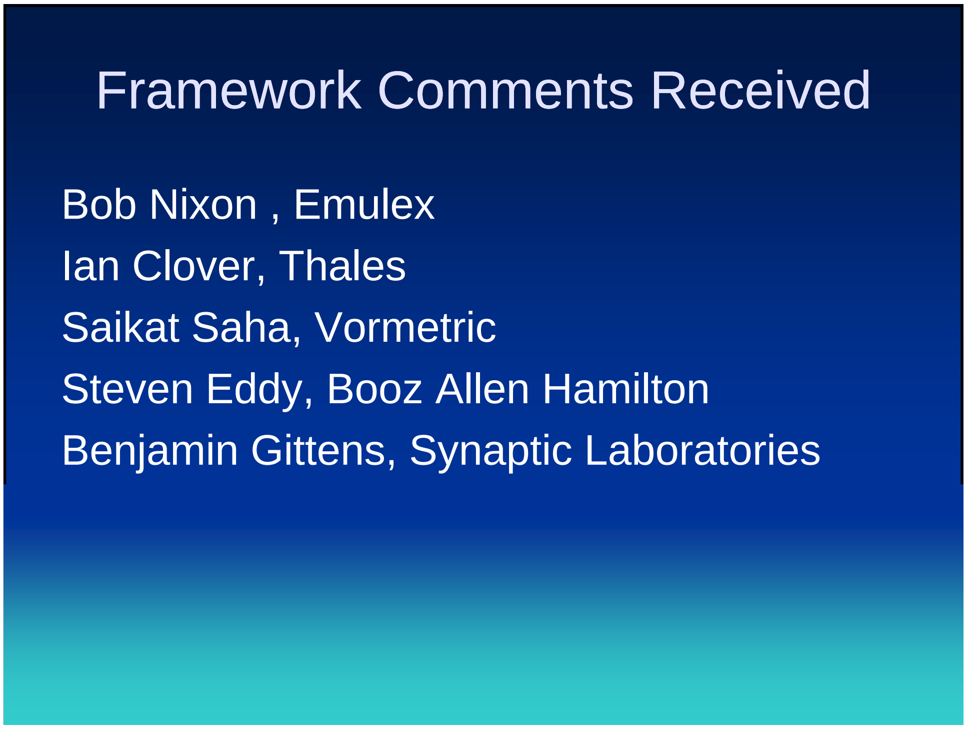
C_s → $R_{s,1}$, $R_{s,2}$, $R_{s,t}$

CKMS Design for USG Applications



NIST Request for Public Comments

June 16, 2010



Framework Comments Received

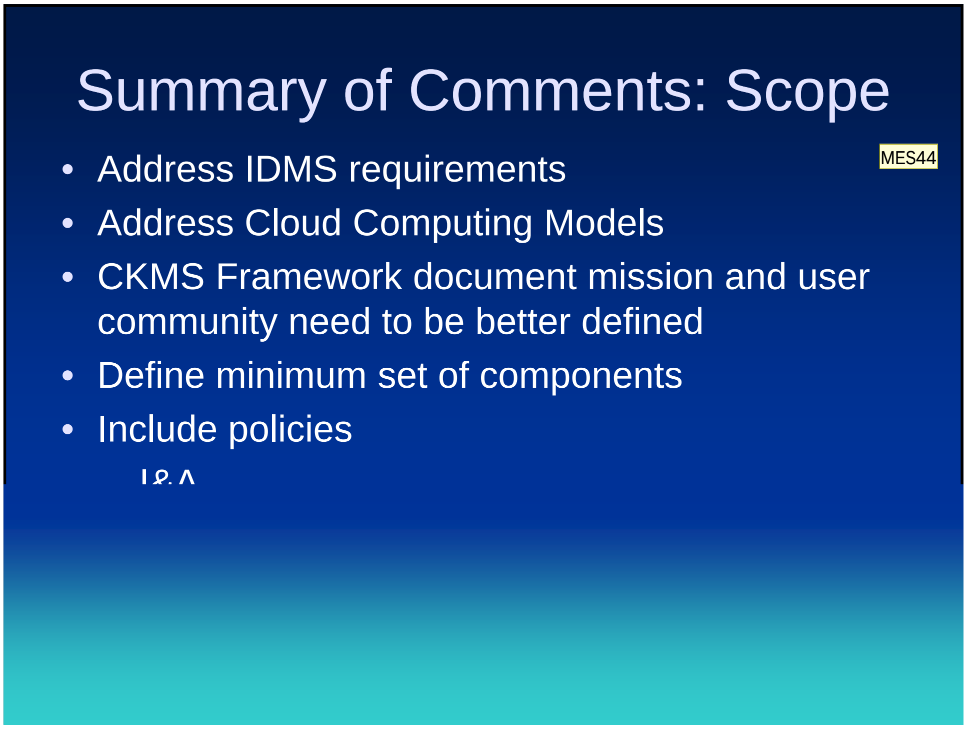
Bob Nixon , Emulex

Ian Clover, Thales

Saikat Saha, Vormetric

Steven Eddy, Booz Allen Hamilton

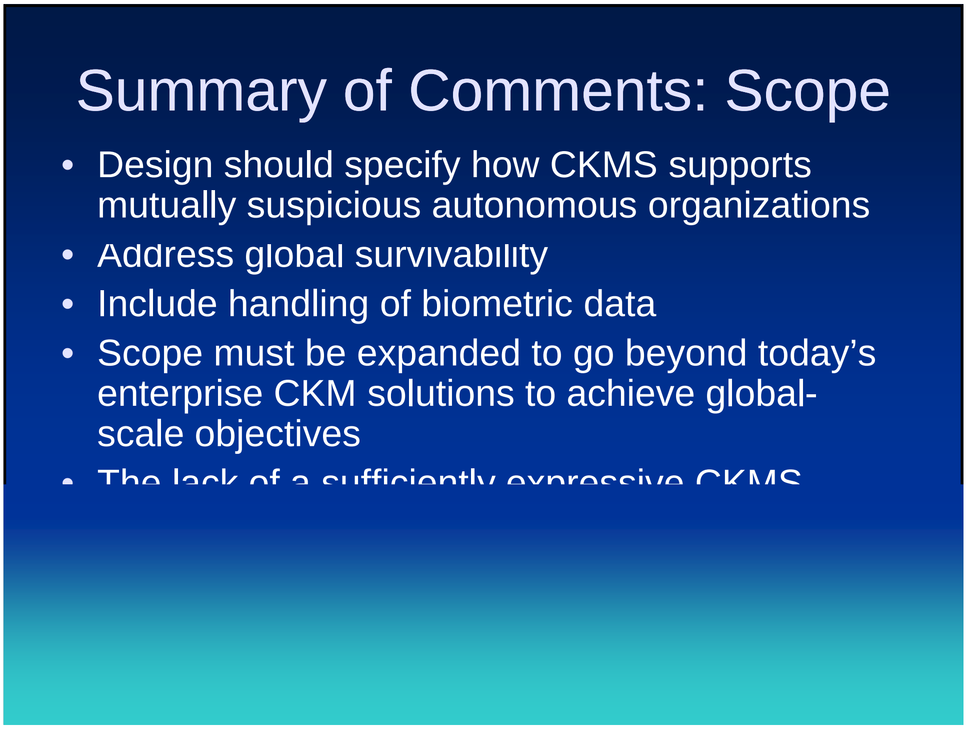
Benjamin Gittens, Synaptic Laboratories



Summary of Comments: Scope

MES44

- Address IDMS requirements
- Address Cloud Computing Models
- CKMS Framework document mission and user community need to be better defined
- Define minimum set of components
- Include policies
  - I&A



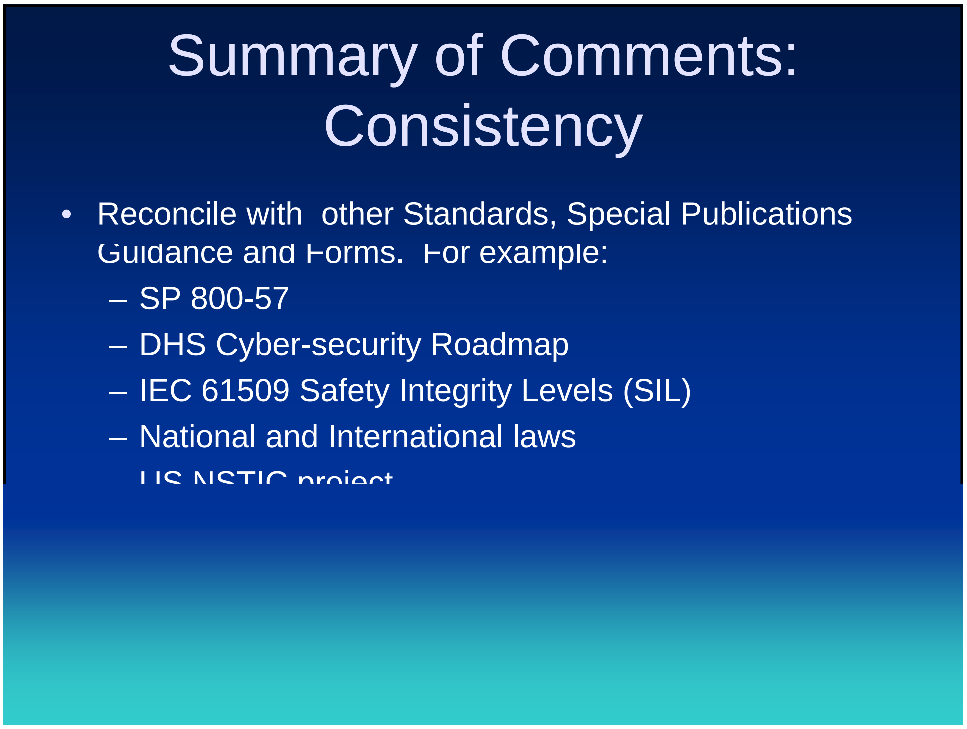
Summary of Comments: Scope

- Design should specify how CKMS supports mutually suspicious autonomous organizations
- Address global survivability
- Include handling of biometric data
- Scope must be expanded to go beyond today's enterprise CKM solutions to achieve global-scale objectives
- The lack of a sufficiently expressive CKMS

Slide 13

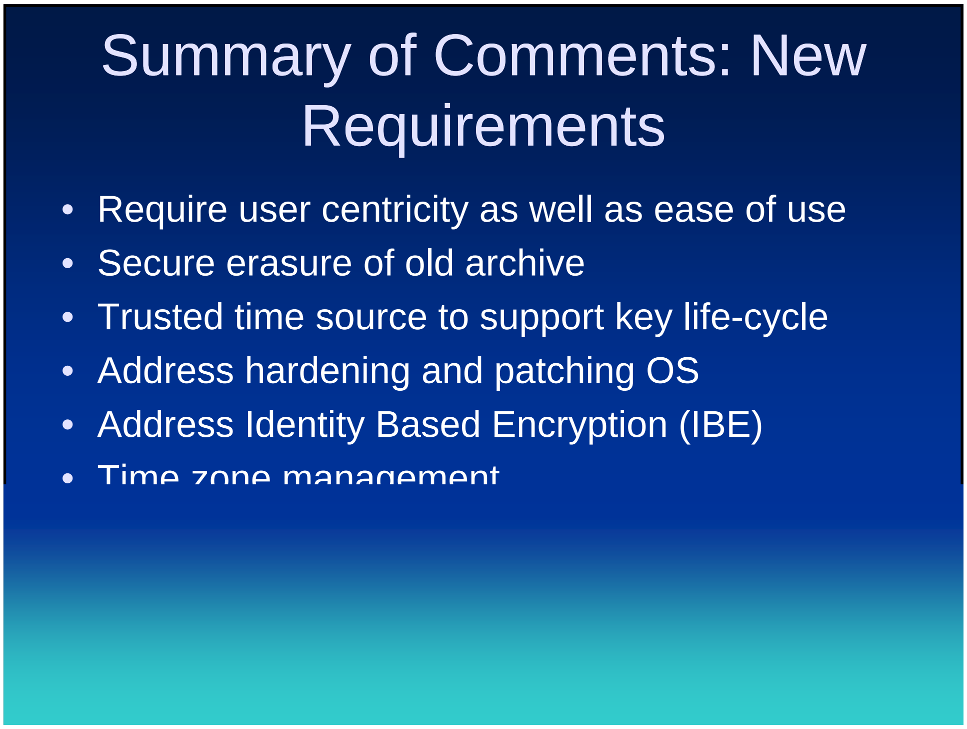
MES44 Listing doesn't imply agreement

Miles Smid, 9/16/2010



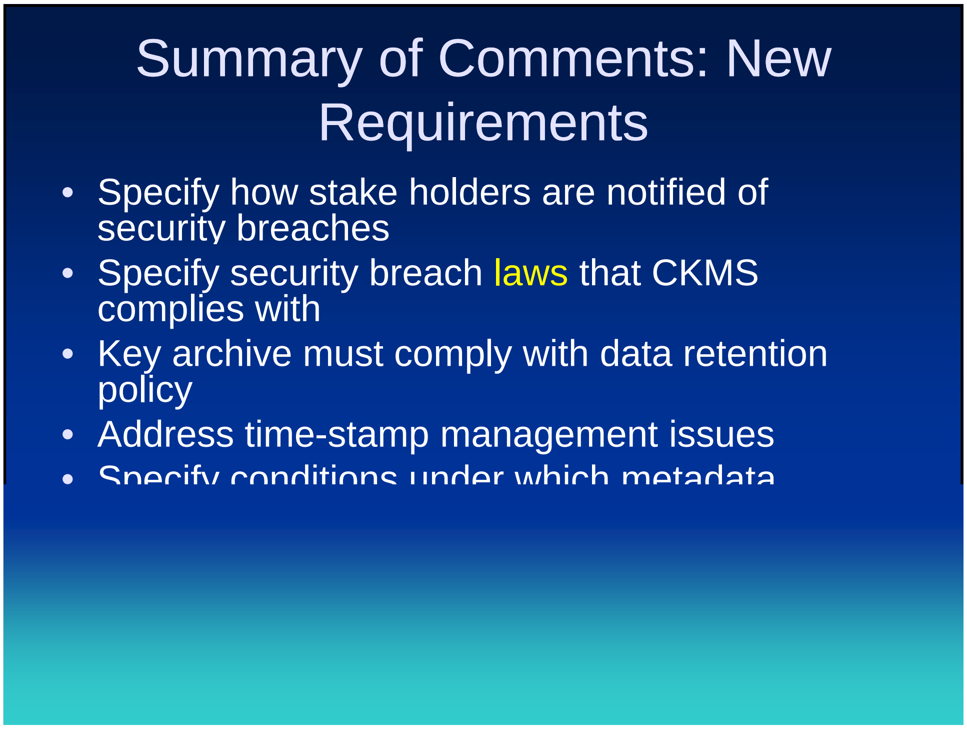
Summary of Comments: Consistency

- Reconcile with other Standards, Special Publications Guidance and Forms. For example:
  - SP 800-57
  - DHS Cyber-security Roadmap
  - IEC 61509 Safety Integrity Levels (SIL)
  - National and International laws
  - US NSTIC project



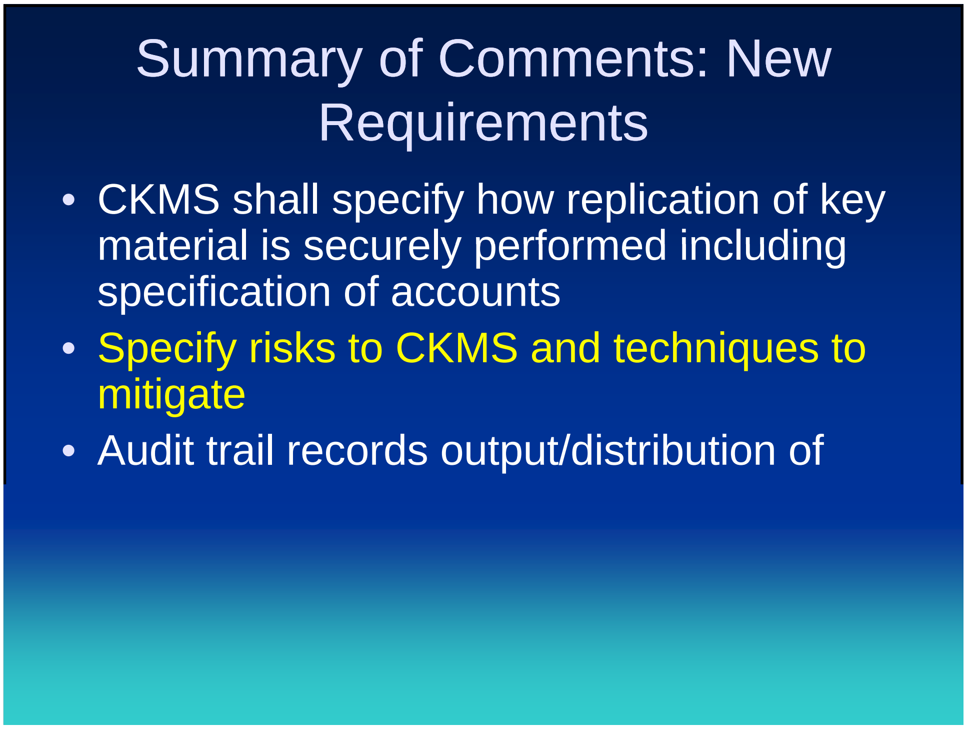
Summary of Comments: New Requirements

- Require user centricity as well as ease of use
- Secure erasure of old archive
- Trusted time source to support key life-cycle
- Address hardening and patching OS
- Address Identity Based Encryption (IBE)
- Time zone management



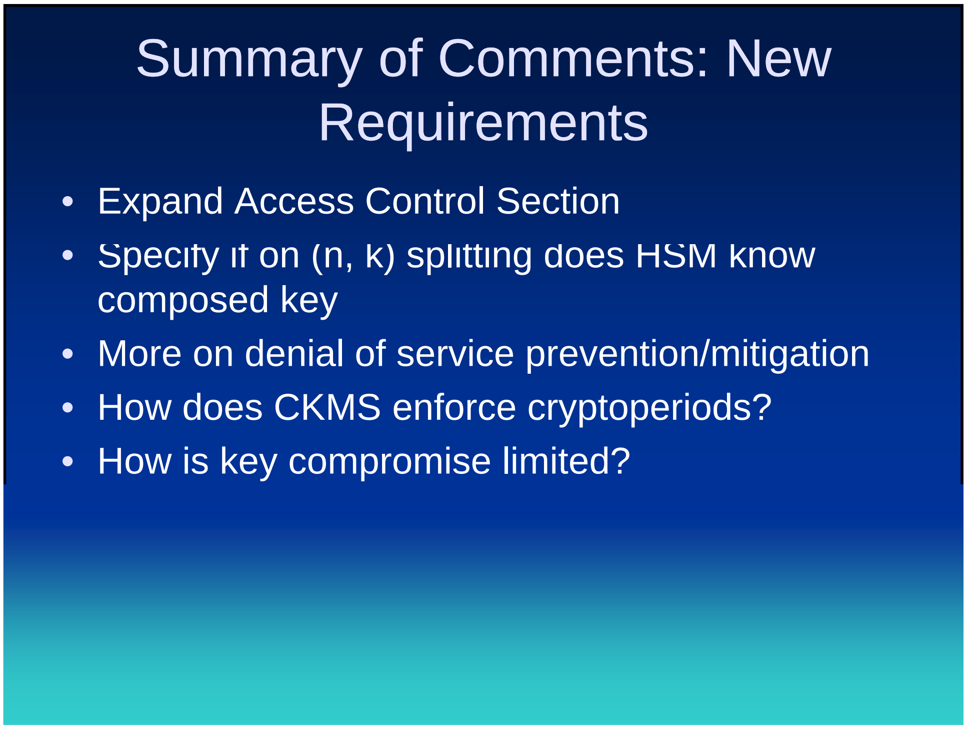
Summary of Comments: New Requirements

- Specify how stake holders are notified of security breaches
- Specify security breach laws that CKMS complies with
- Key archive must comply with data retention policy
- Address time-stamp management issues
- Specify conditions under which metadata



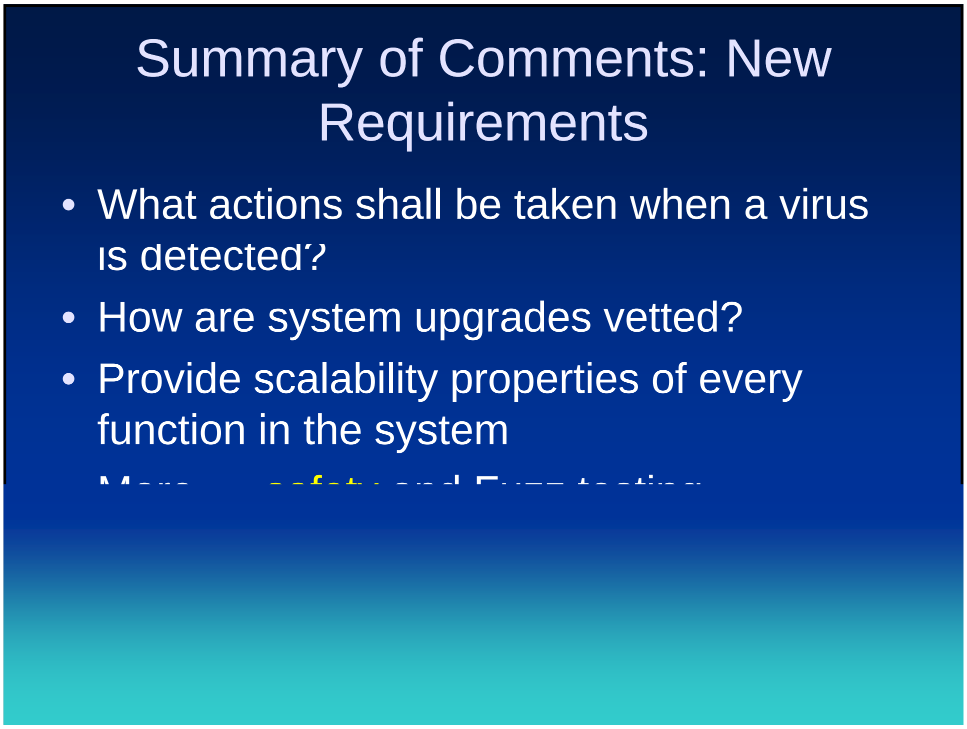
Summary of Comments: New Requirements

- CKMS shall specify how replication of key material is securely performed including specification of accounts
- Specify risks to CKMS and techniques to mitigate
- Audit trail records output/distribution of



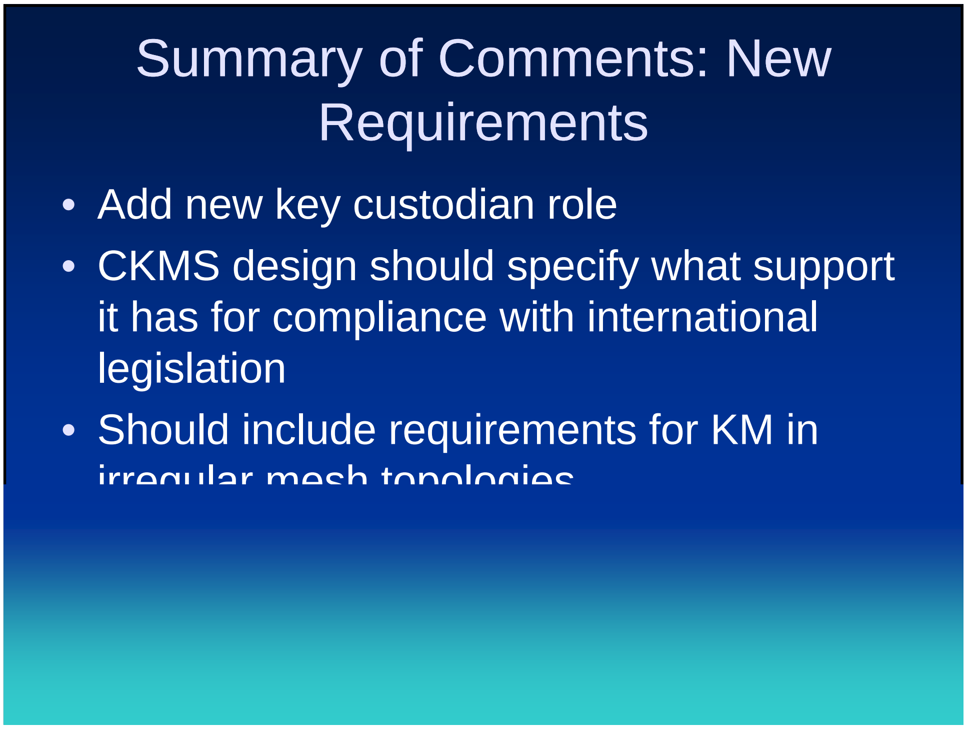
Summary of Comments: New Requirements

- Expand Access Control Section
- Specify if on (n, k) splitting does HSM know composed key
- More on denial of service prevention/mitigation
- How does CKMS enforce cryptoperiods?
- How is key compromise limited?



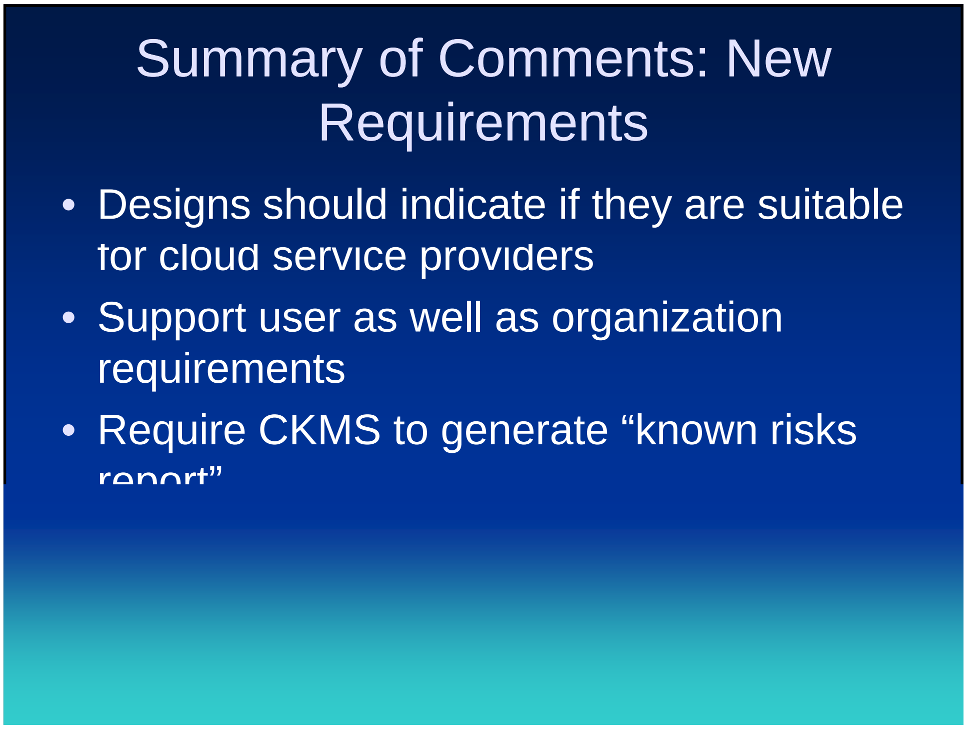
Summary of Comments: New Requirements

- What actions shall be taken when a virus is detected?
- How are system upgrades vetted?
- Provide scalability properties of every function in the system
- More safety and Fuzz testing



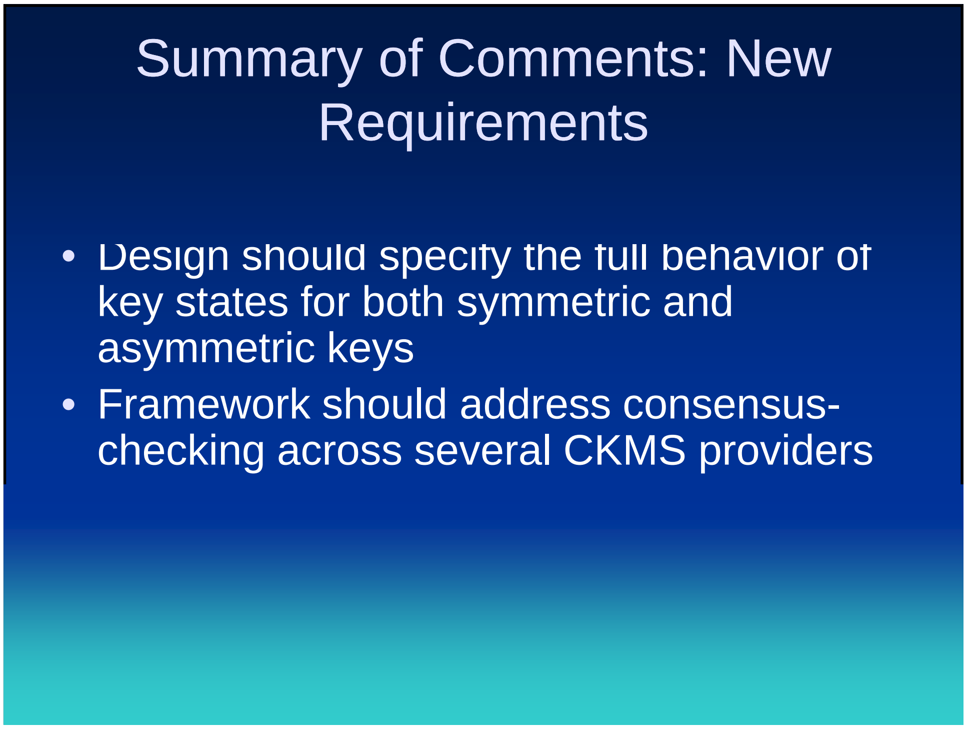
Summary of Comments: New Requirements

- Add new key custodian role
- CKMS design should specify what support it has for compliance with international legislation
- Should include requirements for KM in irregular mesh topologies



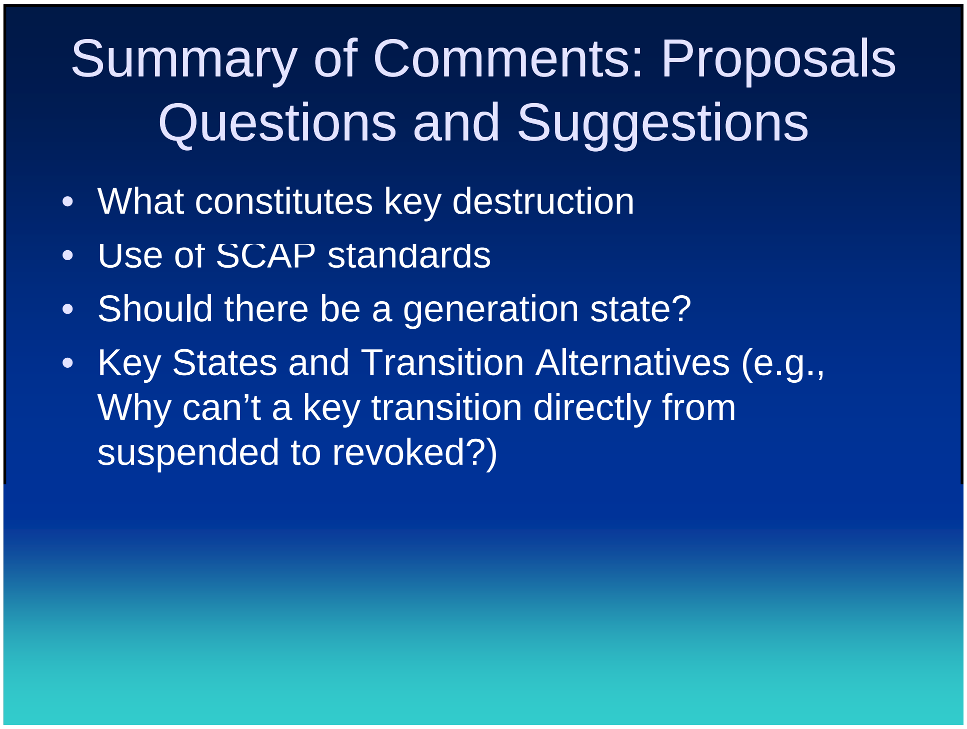
Summary of Comments: New Requirements

- Designs should indicate if they are suitable for cloud service providers
- Support user as well as organization requirements
- Require CKMS to generate “known risks report”



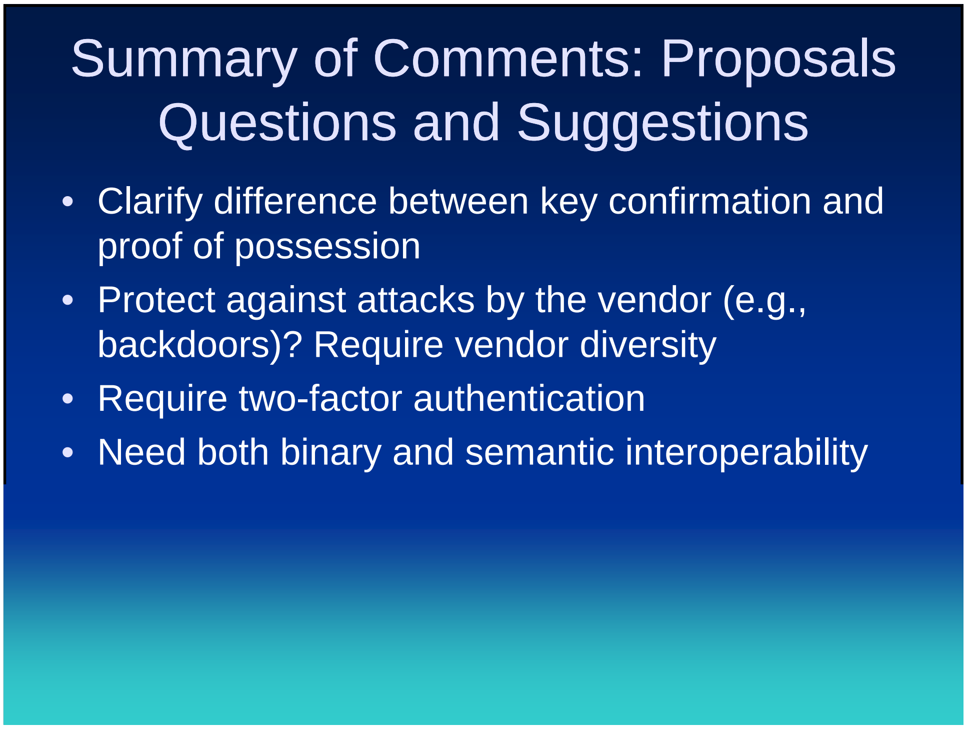
Summary of Comments: New Requirements

- Design should specify the full behavior of key states for both symmetric and asymmetric keys
- Framework should address consensus-checking across several CKMS providers



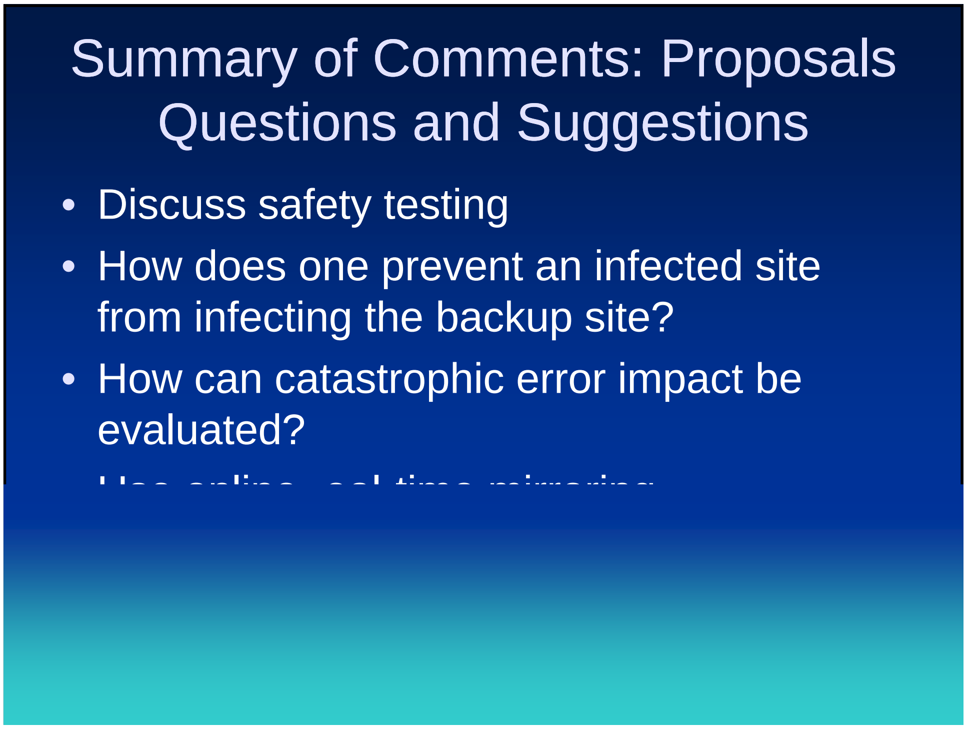
Summary of Comments: Proposals Questions and Suggestions

- What constitutes key destruction
- Use of SCAP standards
- Should there be a generation state?
- Key States and Transition Alternatives (e.g., Why can't a key transition directly from suspended to revoked?)



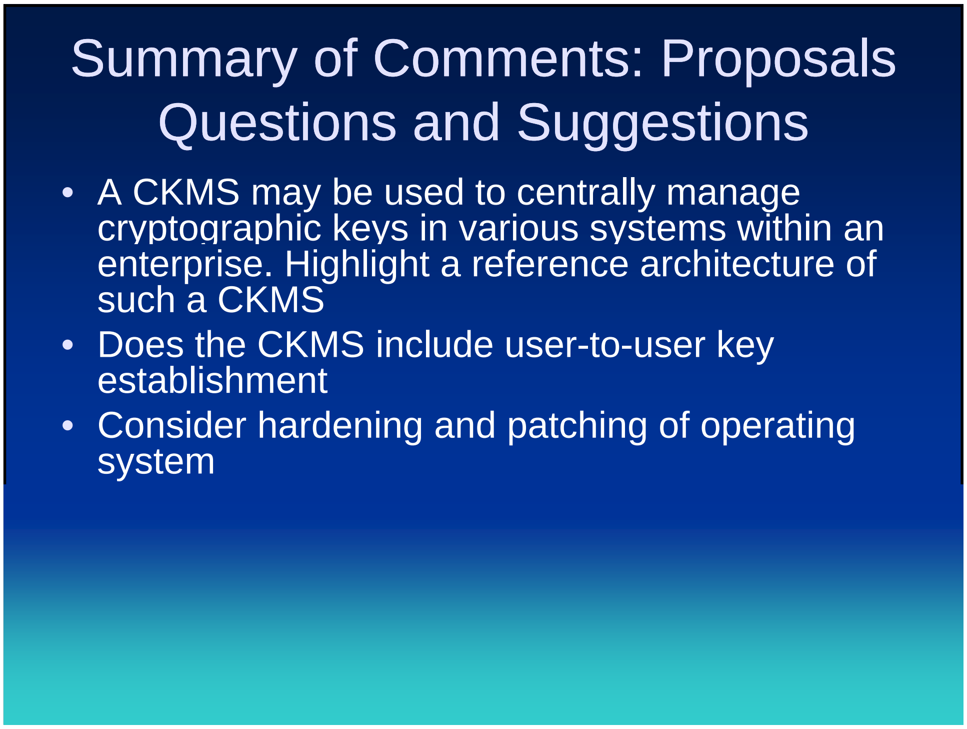
Summary of Comments: Proposals Questions and Suggestions

- Clarify difference between key confirmation and proof of possession
- Protect against attacks by the vendor (e.g., backdoors)? Require vendor diversity
- Require two-factor authentication
- Need both binary and semantic interoperability



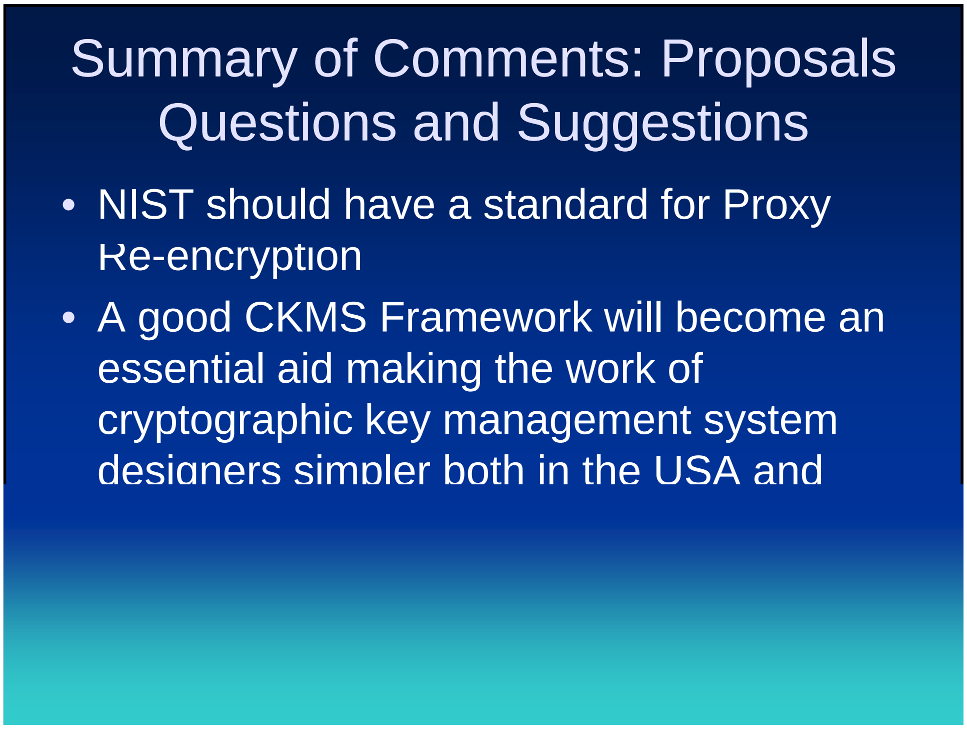
Summary of Comments: Proposals Questions and Suggestions

- Discuss safety testing
- How does one prevent an infected site from infecting the backup site?
- How can catastrophic error impact be evaluated?
- Use online, real-time mirroring



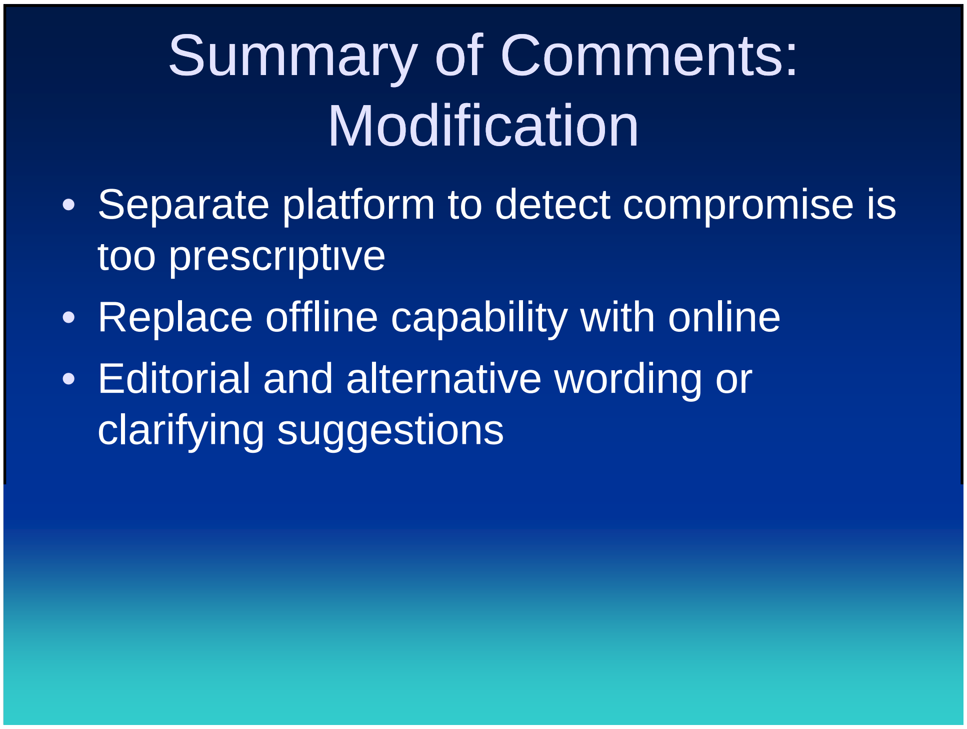
Summary of Comments: Proposals Questions and Suggestions

- A CKMS may be used to centrally manage cryptographic keys in various systems within an enterprise. Highlight a reference architecture of such a CKMS
- Does the CKMS include user-to-user key establishment
- Consider hardening and patching of operating system



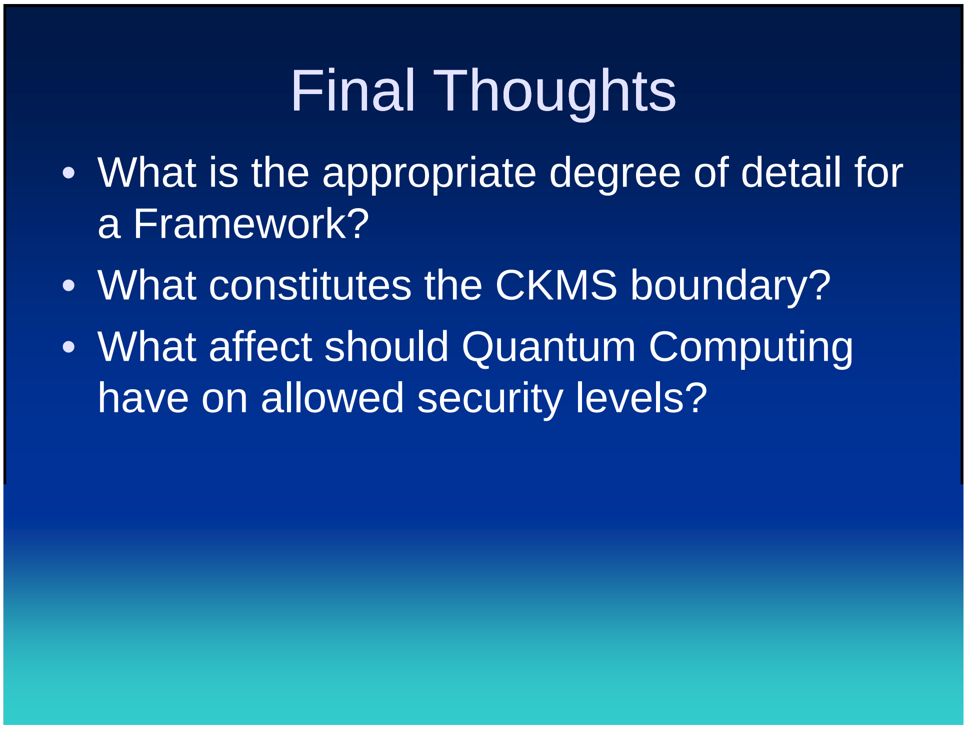
Summary of Comments: Proposals Questions and Suggestions

- NIST should have a standard for Proxy Re-encryption
- A good CKMS Framework will become an essential aid making the work of cryptographic key management system designers simpler both in the USA and



Summary of Comments: Modification

- Separate platform to detect compromise is too prescrıptıve
- Replace offline capability with online
- Editorial and alternative wording or clarifying suggestions



Final Thoughts

- What is the appropriate degree of detail for a Framework?
- What constitutes the CKMS boundary?
- What affect should Quantum Computing have on allowed security levels?

Discussion?