Cryptographic Key Management Workshop Agenda
National Institute of Standards and Technology
Building 101, Lecture Room D

Tuesday, March 4, 2014	
9:00 – 9:15	Welcome and administrative information – *Elaine Barker*
9:15 – 10:30	SESSION 1: Introduction (Sections 1-3) – *Dennis Branstad* • Cryptographic Key Management Project Overview • Profile Introduction, Scope, Goals, Audience • Framework Requirements (FRs), Profile Requirements (PRs), Profile Augmentations (PAs) and Profile Features (PFs) • Terminology • Framework and Profile Documents (Structure, Differences) • Questions/Comments
10:30 – 11:00	BREAK
11:00 – 12:30	SESSION 2: Basic Concepts, Security Policies and Roles (Sections 4 & 5) – *Elaine Barker* and *Dennis Branstad* • FCKMS vs. CKMS • FCKMS Modules • Security Policies • Security Domains • Roles • Questions/Comments
12:30 – 1:30	LUNCH
1:30 – 3:00	SESSION 3: Secure Architectures (Sections 6 and 10) - *Miles Smid* • Key and Metadata Protection and Management Functions • Access Control • Compromise Recovery • Disaster Recovery • Possible Network Configurations • Questions/Comments
3:00 – 3:30	BREAK
3:30 – 5:00	SESSION 4: Spectrum of Applications – *Elaine Barker and others* • Intended Scope • Email • Mobile – *Lily Chen* • Cloud Security – *Michaela Iorga* • Key and Metadata Storage • Key Establishment • Questions/Comments

Wednesday, March 5, 2014	
9:00 – 10:30	SESSION 5: Measures and Security Controls (Section 6 and 8) – *Elaine Barker and Ron Ross* • Security Strength • FIPS 140-2 Security Level (Cryptographic Modules) • Impact/Sensitivity Level of Data (per FIPS 199, FIPS 200, and SP 800-53) – *Ron Ross* • Low, Moderate, High Requirements • Security Controls • Questions/Comments
10:30– 11:00	BREAK
11:00 – 12:30	SESSION 6: Testing, Evaluation, and Validation (Section 9 and 11) – *Dennis Branstad, Ron Ross, Miles Smid, Elaine Barker* • Types of Testing • Maintenance • FIPS 199, FIPS 200, and SP 800-53 • Assessment • Validation • Questions/Comments
12:30 – 1:30	LUNCH
1:30 – 3:00	SESSION 7: Interoperability and Transitioning (Section 7) – *Elaine Barker* • Interoperability Defaults and Recommendations • Transitioning • Questions/Comments
3:00 – 3:30	BREAK
3:30 – 5:00	SESSION 8: Comments and Feedback – *Elaine Barker* • Presentation and Discussion of Comments Received to Date – *Elaine Barker, Dennis Branstad, Miles Smid* • Outstanding Unresolved Issues • Test Cases • Where do we go from here? • Wrap-up