Cryptographic Key Management Workshop

National Institute of Standards and Technology
Information Technology Laboratory
Computer Security Division
Curt Barker, Chief

Administrative Announcements

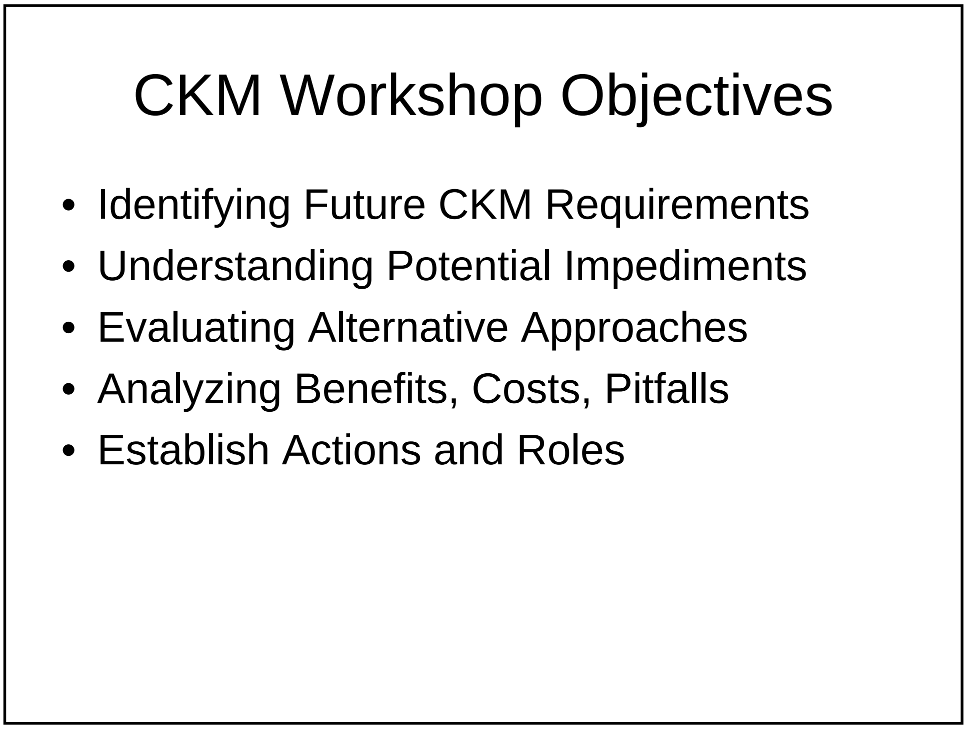
- Emergency Exits: Rear & Front-Side Doors
- Restrooms: Across from cafeteria;
  - Also in Corridor to Red Auditorium
- Cafeteria: Lunch available 1:00 – 2:00
- Morning Break: Refreshments in Cafeteria
- Afternoon Break: Cafeteria Closed

Key Management Project Context

- Cyberspace Security Policy Review: 2009
- Role of Key Management in Cybersecurity
- Challenges and Requirements
- Way Forward

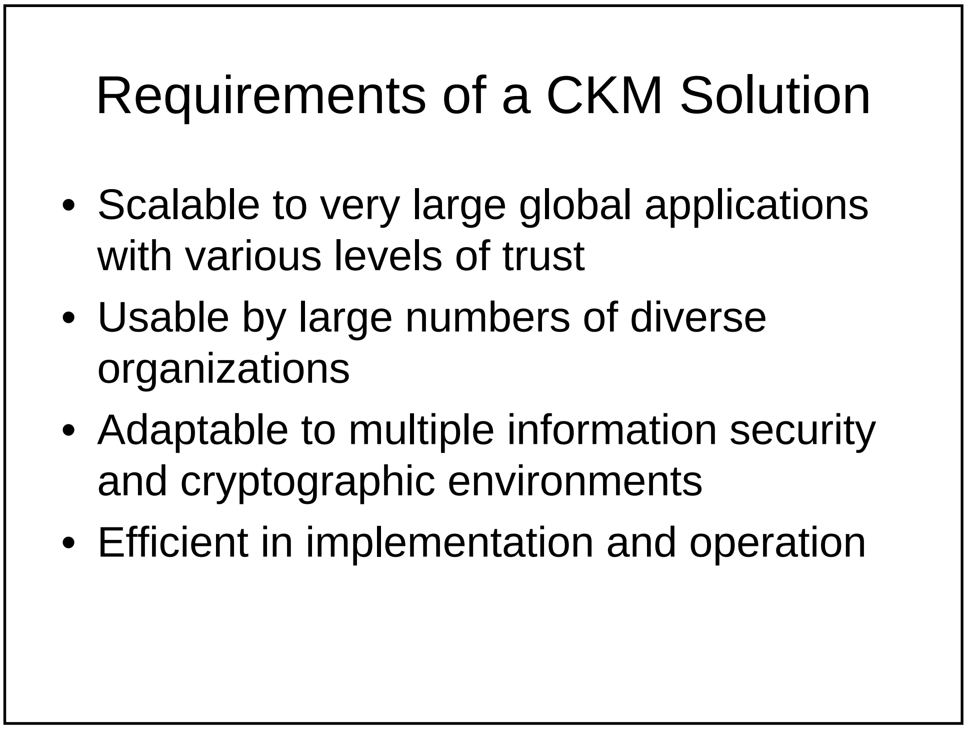
Cyberspace Policy Review Highlights

- Architecture of the Nation’s digital infrastructure is not secure or resilient
- Nation must develop policies and technology required to mitigate risks
- Security objectives must be defined for the next-generation infrastructure
- Cybersecurity Policy requires standards regarding secure operations in Cyberspace



CKM Workshop Objectives

- Identifying Future CKM Requirements
- Understanding Potential Impediments
- Evaluating Alternative Approaches
- Analyzing Benefits, Costs, Pitfalls
- Establish Actions and Roles



Requirements of a CKM Solution

- Scalable to very large global applications with various levels of trust
- Usable by large numbers of diverse organizations
- Adaptable to multiple information security and cryptographic environments
- Efficient in implementation and operation

Potential CKM Impediments

- Diverse National/Organizational Requirements
- Intellectual Property Interests among Vendors, Services
- Incompatibility among Available Technologies
- Lack of User-Acceptable Standards
- Technical Problems Associated With Revocation and Replacement
- Data at Rest Discovery Requirements

Players/Roles in CKM Solutions

- NIST
- Other Federal Agencies
- Executive and Legislative
- Industry
- Academia
- Other

Actions in CKM Solutions

- Development
- Analysis
- Testing
- Qualification
- Procurement
- Operation & Maintenance

Roles and Actions

- Identify the Key Players in a CKM Program
- Establish Roles and Partnerships
- Specify Appropriate Actions for Players
- Coordinate Actions to Produce Solutions
- Demonstrate and Test Solutions in Applications
- Develop and Promulgate Standards for Solutions

Monday Morning Agenda

- Keynote: Admiral Mike McConnell, BAH
- Keynote: Dr. George Strawn, NSF
- 10:15 – Key Management Today
- 11:15 – Break
- 11:30 – Key Management: Lessons Learned
- 12:00 – Future Key Management Methods
- 12:30 – 2010 Transitions
- 13:00 – Lunch Break