SHA-1: Practical Security Implications of Continued Use

- Where is SHA-1 widely deployed today? What are the security implications of current hash attacks on these applications? Which applications are threatened by collision attacks and which applications are not?
- Is it practical to continue using SHA-1 for the next five years? Under what circumstances would an immediate shift away from SHA-1 be required?
- What are the benefits and costs of shifting to another algorithm in the next few years? What should be done to help ensure a transition?