ANS X9.82: Random Number Generation
• Work began about 1998;

• Main contributors/editors from NIST, NSA, and CSE

• Material later incorporated and revised into the SP 800-90 series – in order to include test and evaluation methods
Four Part Standard

• Part 1: Overview and Basic Principles (2006; R2013)
• Part 2: Entropy Sources ((2011)/2015)
• Part 4: Random Bit Generator Constructions (2011; R2017)
Part 1: Overview and Basic Principles

• Original content:
  o Overview: secure RBGs, functional model, RBG types of RBGs
  o Security Properties
  o Annexes

• Current status

(No SP 800-90 counterpart)
Part 3: Deterministic Random Bit Generators

• Original content:
  - Similar to the current SP 800-90A
  - Specifies HMAC_DRBG, CTR_DRBG, Dual_EC_DRBG)
  - Annexes

• Current status: To be revised to adopt SP 800-90A
Part 2: Entropy Sources

• Original content:
  o Similar to SP 800-90B
  o Does not include validation tests

• Current status: Revision in progress to adopt SP 800-90B
Part 4: RBG Constructions

• Original content:
  o Similar to the first two drafts of SP 800-90C
  o Annexes

• Current status: Revise to adopt SP 800-90C
Questions?
Thanks!