X9.82 (RNGs)

Elaine Barker
National Institute of Standards and Technology
ebarker@nist.gov
301-975-2911

ges

- five parts:
  - Pa view and Basic Principles
  - P RBGs Based on Hash Functions
  - Part RBGs Based on Block Ciphers
  - Part 4: DRBGs Based on Hard Problems
  - Part 5: NRBGs

[illegible] (contd.)

- [illegible], symbols and [illegible] in the appropriate part

[illegible] Overview and Basic [illegible]ples

- [illegible]on
  - [illegible]ional Model - needs to be re[illegible] with the text
  - [illegible]curity requirements
  - RBG functional requirements
- Deterministic RBGs
  - As before; what goes here vs. what goes in Parts 2-4?
  - Added section on the error state (7.2.6)

[illegible] (contd.)

- [illegible] RBGs
  - [illegible] here vs. what goes in Parts 5?
- [illegible]
  - Hybrid [illegible]Gs
  - Using Multiple RBGs
  - Producing RNs from Random Bits
  - Implementation Issues (general)
  - Testing (general)

[illegible] DRBGs

- [illegible]rt
- DRB[illegible]ssions - currently same as Pa[illegible]
- Types of DRBGs
- Approved DRBGs
  - Error state has been indicated