Criteria

- Security
  - Confidence
  - Resistant to attack
  - Manage threats effectively
  - Attribution/zone data?
  - WHOIS problem?
  - Physical Security
  - Data integrity
    - Submission/registration
  - DNSSEC
    - Recursive resolver
    - DNSSEC taxonomy
    - Hard to determine health of DNS based on unknown but exploited holes in DNS
    - Need of service level of DNS (dashboard)
- From whose perspective???
  - Different issues, depending on point of view
  - (+) Registrant <--> Registrar (1)
  - (+) Registrar <--> Registrar AND Registry <--> Registrant (2)
  - (+) Registry <--> DNS (3)
  - (+) DNS <--> End-user (4)
  - (+) Picture
- Action items
  - Ask Mark to clarify the "DNSSEC" part of that group's work
  - Scott -- expand on:
    - WHOIS problem?
    - Threats and defenses
      - Operational criteria
        - Roles and responsibilities
        - Physical/procedural/process
        - 3rd party suppliers of services/SLA's
      - Institutional confidence
      - Accountability and transparency
- Criteria
  - Infrastructure (Mikey's suggestion for topic-header)
    - Hardware
    - Software
    - Capacity
    - Transit
    - Connection (minimums?)
      - Bandwidth
      - Connectivity
      - Latency
      - Resilience?
  - Timely response
- Stability
  - Uptime
    - Reachability
      - At multiple ports
      - Unintended
      - Officially intentional
      - Malicious
    - Note -- WW CGI.hR, SIMET
  - Changes can be implemented with a predictable impact on services
  - Acceptable performance for all actors
  - DNS is (by definition) an End-to-End service -- not just the protocol between client and server, but has boundaries that go far beyond that
  - Availability
    - Availability of data/system
    - Availability of DNS as a service
      - Secondary servers
  - Data integrity
    - Integrity of data
      - Authenticity
      - Trustworthy
    - Types of data
      - Configuration
        - Accuracy (e.g. errors/typos in names/IPs/etc.
        - Correctness/accuracy
      - Scope -- not just registry data, registrars AND registries
  - Process integrity
    - Scope -- includes policy, political, protocol
      - Action: expand/clarify
    - Institutional confidence
    - Accountability and transparency
    - Availability to end user
      - "reachability"
      - Action -- Don B -- figure out a substitute for the word "availability"
    - Procedures
      - Roles and responsibilities
      - Physical/procedural/process
    - Incidence response
      - Threat warning and recommendations of mitigation based on the warning
    - Expertise
      - DNS
      - Security
      - Networking
      - Skill
        - Design
        - Operation
    - Healthy DNS needs good incident management and good network operations
    - Diversity
      - Operator (people, location, funds, experience)
    - Protocol integrity
  - System integrity
    - Consistency
    - Infrastructure (brand, spec, location)
    - 3rd party suppliers of services/SLA's
    - Works and continues to work in a highly predictable way