- Criteria
  - Metrics
    - Uptime
      - Reachability
        - At multiple ports
        - Unintended
        - Officially intentional
        - Malicious
        - Note -- WW CGI.hR, SIMET
    - Infrastructure (Mikey's suggestion for topic-header)
      - Hardware
      - Software
      - Connection
        - Bandwidth
        - Connectivity
        - Latency
        - Resilience?
    - Content (Mikey's suggestion for topic-header)
      - Configuration
      - Data integrity
        - Transit
        - Submission/registration
  - Enablers
    - Diversity
      - Operator (people, location, funds, experience)
      - Infrastructure (brand, spec, location)
    - Skill
      - Design
      - Operation
      - DNS
      - Security
      - Networking
    - Expertise
    - Technology
      - DNSSEC
        - Recursive resolver
        - DNSSEC taxonomy
        - Hard to determine health of DNS based on unknown but exploited holes in DNS
        - Healthy DNS needs good incident management and good network operations
        - Threat warning and recommendations of mitigation based on the warning
        - Need of service level of DNS (dashboard)
    - Procedures
  - Threats and defenses
    - Operational criteria
      - Roles and responsibilities
      - Physical/procedural/process
      - 3rd party suppliers of services/SLA's
    - Institutional confidence
    - Accountability and transparency
  - 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

- Summary
  - From whose perspective???
    - Registrant
      - (1)
      - Registrar
      - (2)
      - Registry
      - (3)
      - DNS
      - (4)
      - End user
    - (2)
    - Different issues, depending on point of view
      - (1) Availability - n/a
        - Availability of DNS as a service
          - Secondary servers
        - Data consistency
        - DNS data accuracy -- 100%
        - Data integrity
        - Process integrity
        - System integrity
      - (2) Availability - 90%
        - DNS data accuracy -- 100%
        - Data integrity
        - Process integrity
        - System integrity
      - (3) Availability --
        - DNS data accuracy -- 100%
        - Data integrity
        - Process integrity
        - System integrity
      - (4) Availability -- 100%
        - DNS data accuracy -- 100%
        - Data integrity
        - Process integrity
        - System integrity
  - Criteria
    - Availability
      - Availability of data/system
    - Capacity
    - Accuracy (e.g. errors/typos in names/IPs/etc.
      - Correctness/accuracy
    - Security
      - Integrity of data
        - Authenticity
        - Trustworthy
      - Data consistency
      - Confidence
      - Resistant to attack
      - Manage threats effectively
      - Attribution/zone data?
      - WHOIS problem?
    - Stable
      - Works and continues to work in a highly predictable way
      - Changes can be implemented with a predictable impact on services
      - Consistency
      - 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
    - Timely response
  - Physical Security