Systems

- Certificate Management System
- Certificate System
- Delegated Third Party System
- Issuing System
- Root CA System
- Security Support System

System

- One or more pieces of equipment or software that stores, transforms, or communicates data.

CA Infrastructure

- Collectively the infrastructure used by the CA or Delegated Third Party which qualifies as a:
  - Certificate Management System;
  - Certificate System;
  - Delegated Third Party System;
  - Issuing System;
  - Root CA System (Air-Gapped and otherwise); or
  - Security Support System.

Certificate Management System

- A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate System

- A system used by a CA or Delegated Third Party to access, process, or manage data or provide services related to:
  - identity validation;
  - identity authentication;
  - account registration;
  - certificate application;
  - certificate approval;
  - certificate issuance;
  - certificate revocation;
  - authoritative certificate status; or
  - key escrow.

Delegated Third Party System

- Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.

Issuing System

- A system used to sign certificates or validity status information.

Root CA System

- A system used to:
  - generate a Key Pair whose Private Key is or will be a Root CA Private Key;
  - store a Root CA Private Key; or
  - create digital signatures using a Root CA Private Key.

Security Support System

- A system or set of systems supporting the security of the CA Infrastructure, which minimally includes:
  - authentication;
  - network boundary control;
  - audit logging;
  - audit log reduction and analysis;
  - vulnerability scanning;
  - physical intrusion detection;
  - host-based intrusion detection; and
  - network-based intrusion detection.

What are we talking about?

- Stuff used specifically to interact with certificates
  - Certificate Management System
  - Certificate System
    - Delegated Third Party System
  - Issuing System
  - Root CA System
- Stuff used to keep everything else secure
  - Security Support System

NS-003: CA Infrastructure

- A definition for “CA Infrastructure” has been added. There are 7+ types of “systems” defined in the NCSSRs, but their use is inconsistent and unclear in some cases. For example, Security Support System is defined as a system that does 8 different things, but the 8 things this system does are each described within the requirements themselves, making somewhat of a circular definition as well as creating an unnecessary defined term, since it’s only used in the context of describing what it is.
- “CA Infrastructure” merely defines a term to encapsulate the collective set of systems elsewhere defined. The use of CA Infrastructure throughout this draft to replace a vast majority of the individual “systems” previously used is intended to:
  - 1. Simplify the assessment of the NCSSR’s applicability. Most requirements apply to the CA’s Infrastructure as a whole, with specific applicability to aspects of that infrastructure defined and described in-line; and
  - 2. Draw out any areas where requirements are applied in an overly broad way, so that improvements can be made to the requirement phrasing itself to clarify the intended scope of applicability
- It’s plausible (and desirable, assuming agreement with the above) that we’ll be able to remove some or most of the definitions of separate systems within the CA’s infrastructure as their use becomes obviated by this consolidation of terminology.

NS-003: Security Support System

- This definition has been reformatted to a numbered list.
- This is a definition that seems better suited as part of the core requirements, rather than a separately defined term. We should be able to obviate the need for it because of the presence of dedicated sections outlining these requirements, for example:

  - authentication; <In section 2 of this draft ballot>
  - network boundary control; <In section 1 of this draft ballot>
  - audit logging; <In section 3 of this draft ballot>
  - audit log reduction and analysis; <In section 3 of this draft ballot>
  - vulnerability scanning; <I think included in draft ballot addressing updates to section 4>
  - physical intrusion detection; <I think included in draft ballot addressing updates to section 4>
  - host-based intrusion detection; and <I think included in draft ballot addressing updates to section 4>
  - network-based intrusion detection. <I think included in draft ballot addressing updates to section 4>

What should we do?

- Remove Security Support System
  - Not used in the text itself
  - The functions these systems perform have requirements described throughout the document
- Remove Certificate Management System
  - Not used in the text itself
  - Duplicative of Certificate System

What should we do? Continued

- Remove Signing System
  - Not used in the text itself
  - Duplicative of Certificate System
- Remove Delegated Third Party System
  - Not used in the text itself
  - Duplicative of Certificate System (which includes Delegated Third Party directly)

Result

- 2 Systems Remain:
  - Certificate System
  - Root CA System
- Requirements remain for the functions previously defined systems perform