

3.0 NAMING AND DIT STRUCTURE

This section discusses naming and registration recommendations for the Federal Government X.500 name space. The Federal Government name space is defined as those entries in the DIT that are directly subordinate to the U.S. Government in the global DIT. Specific policy is recommended for the naming and registration of first level organizationalUnits, and general guidance is offered for naming and the DIT structure below this first level (L3). An example DIT for the top level of the Government Directory is shown in Exhibit 3-1.

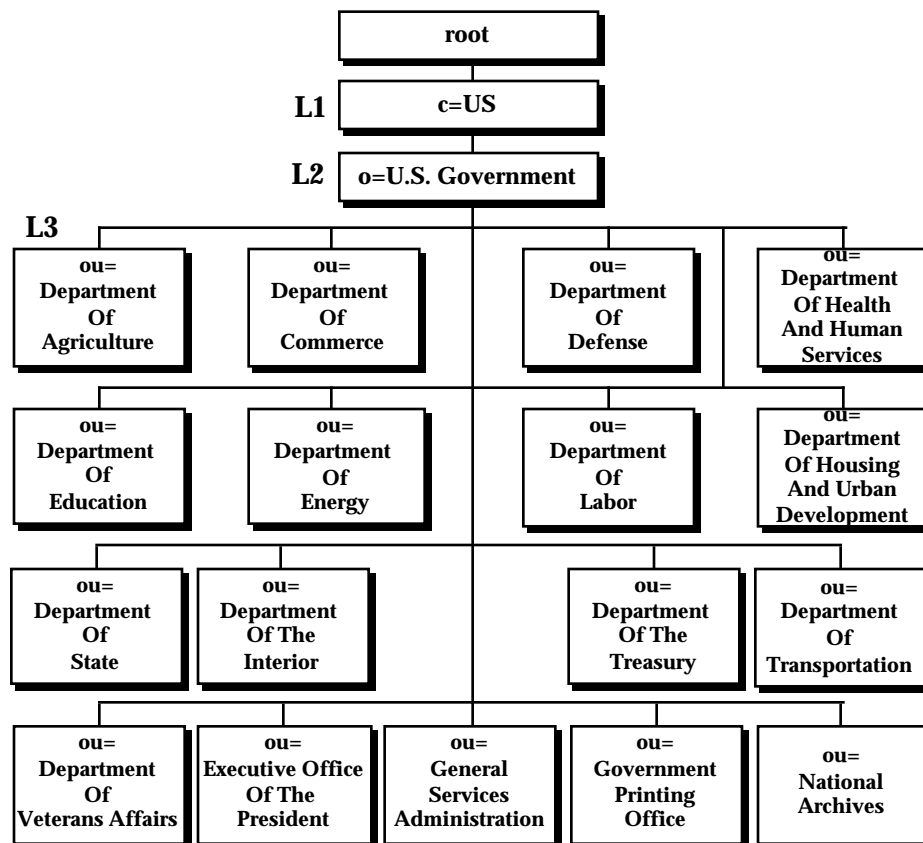


Exhibit 3-1
Federal Government Top Level DIT

3.1. First Level Organizational Units - Registration Policy

The U.S. Government is registered as an organization (O=) object class in the Global DIT. Agencies and departments are registered as organizationalUnit (OU=) object classes immediately beneath the O=U.S. Government entry in the Global DIT. It is recommended that the source for the registration of agencies and departments be the Federal Government Manual. This publication cites first level agencies and departments (organizationalUnits) in each branch of the Federal Government. First level organizationalUnits are those that are not subsumed hierarchically under any other organizationalUnit. Each agency/department to be entered into the Government Electronic Directory shall be registered by the Federal Government Registration Authority (FGRA). In addition, the FGRA will accept a first level OU registration from any organization which appears in the Federal Information Processing Standard Publication (FIPS PUB) 95-1, Codes for the Identification of Federal and Federally Assisted Organizations. FIPS PUB 95-1 defines a standard four digit numeric identifier, based on the Department of Transportation's coding system used to distinguish Federal organizations in the budgetary process. The first two digits identify the agency/department, the third and fourth digits define the level of the organization within the agency/department. Codes ending in "00" represent first level organizations. The organizations listed in FIPS Pub 95-1 belong to the following groups:

- Legislative Branch
- Judicial Branch
- Executive Office and Departments (and their associated organizations)
- Other Independent Federal and Quasi-Federal Organizations (and associated organizations)
- Independent Federal-State and Interstate Organizations
- International Organizations.

If the requesting organization may be subsumed under one of the "00" organizations, the FGRA will inform the "parent" organization and the requesting organization of the conflict. The FGRA will then mediate any concerns that may exist between the parties. In all cases, the requesting organization may be aliased at the 1st

OU level while having their data subordinate to the first level organization as listed in Federal Government Manual.

3.1.1 First Level organizationalUnits - Naming Policy

It is recommended that the name for the registered entity be that name recorded in the Federal Government Manual and listed in Appendix A. The syntax for that name can be :

Department of (name of agency)
Department of the (name of agency)

At the time of registration, one or more alternative names may be designated. For example, the Department of Transportation could designate the following alternative names:

organizationalUnitName = Transportation
organizationalUnitName = DOT.

Any number of organizationalUnitNames may be entered for the registered entity to aid in directory searches; however, only one of the specified names can appear as the relative distinguished name (RDN). The RDN is the name that will be presented to identify the OU to the user as a result of browsing or searching the directory. For example, the Department of Transportation directory entry may have the following names entered into the directory entry:

organizationalUnitName = Department of Transportation (specified RDN)
organizationalUnitName = Transportation
organizationalUnitName = DOT.

Any search conducted using part or all of the above names will bring up the directory entry listed as the "Department of Transportation".

3.1.2 First Level organizationalUnits - Exceptions

Any first level OU as designated in the Federal Government Manual may voluntarily designate other first level OUs as subordinate to them for the purposes of X.500 naming and registration. For example, the Department of Defense may subsume the Departments of the Navy, Army, and Air Force. This will be acceptable under the following conditions:

1. A memorandum of understanding (MOU) is submitted to the FGRA stating agreement by all agencies involved.
2. The subsumed agencies agree to withdraw registration at the first level OUs.

Any first level OU designated in the Federal Government Manual may voluntarily designate any OU subsumed to them as a first level OU for the purposes of X.500 registration and naming. For example, the Department of Transportation may voluntarily designate the Internal Revenue Service as a peer first level OU, even though that guidance may be contrary to the guidance in the Federal Government Manual. This will be acceptable under the following conditions:

1. An MOU must be submitted to the FGRA that states agreement by all agencies involved.
2. The “spun off” OU shall agree to appoint a Senior Registration Official (SRO) for X.500 naming and registration.
3. The “spun off” OU shall agree to submit their registration as a 1st level OU and follow the policies and procedures for SROs at the 1st level OU.

3.1.3 Responsibilities of First Level organizationalUnits

Under a Delegation of Authority for X.500 naming and registration from ANSI, and in turn, from NIST, the FGRA will delegate authority to organizations that register as first level OUs. This authority delegates the following responsibilities:

1. Establishment of a Directory Registration Official (DRO) to administer the X.500 naming and registration policies for the agency. Specifically, the DRO must maintain a register of RDNs for the OU for the purposes of uniqueness.

The DRO may appoint an agent, such as GSA, who will actually perform the duties associated with the delegation of authority. For example, the International Whaling Commission may wish to be listed in the Government Electronic Directory, but does not wish to become an Administrative Directory Management Domain (ADDMD) operator. In this case, they could appoint GSA as their agent.

2. Ensure that each object in the subtree below the first level OU is unique and unambiguous.
- 3 . Management of the ADDMD for the organizationalUnit. Specifically, management must include the five functional areas of systems management:
 - Configuration - Software and hardware modularity to facilitate component modification with minimal impact to directory operations.
 - Fault - The directory will employ an auditing capability that can identify operational problems, detect security breaches, and provide diagnostics to support restoration of directory services.
 - Performance - The directory will be configured to optimize performance, which will be measured by the time required for servicing user queries.
 - Security - The directory will provide access control mechanisms for protecting information at the attribute level.
 - Accounting - The directory will be a self-supporting service providing usage-sensitive billing to recovering operational costs.

In addition, the DRO becomes the authoritative source for data contained in the DIB, ensuring that it is accurate.

3.2 Second Level and Below organizationalUnits

Authority for naming and registration will be delegated from the E-Mail PMO to all first level OUs. Each first level OU will be responsible for the formation and maintenance of a structure that best defines their organization within the guidelines and recommendations discussed below.

3.2.1 Directory Distinguished Names

Directory Distinguished Names (DN) are assigned to each directory entry to provide a map between user-friendly names and entry values. Entries in an X.500 directory are related to each other using a hierarchical structure termed the DIT. The recommended DIT for the Federal Government is shown in Exhibit 3-2.

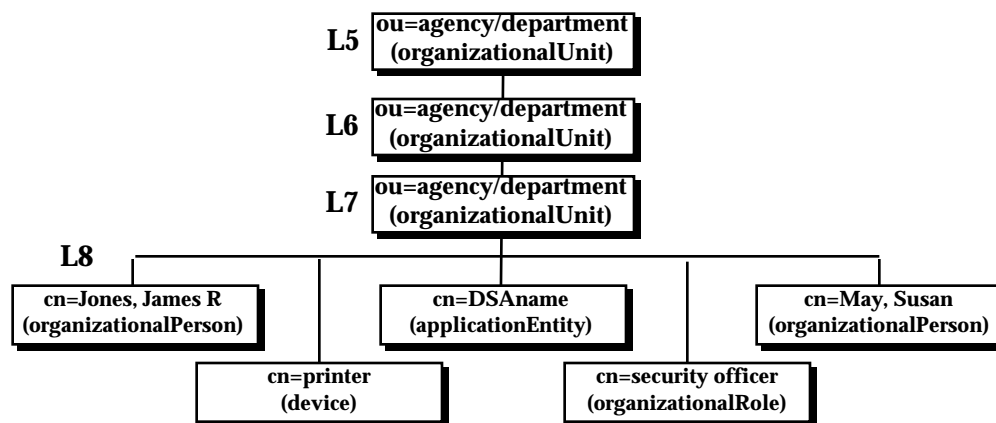


Exhibit 3-2
Organizational Subtree

Each entry in the DIT is uniquely identified by its DN. The DN of a given object is defined as being the sequence of the RDNs of the entry that represent the object and those of all of its superior entries in descending order. Each entry has a unique RDN, which is an attribute value that forms the DN of the entry. Agency/department DROs are responsible for the registration of `organizationalUnitNames` below the OU level (second level OUs). Individuals (`organizationalPersons`) are listed under the OU subtree for the agency/department, as are devices and `applicationEntities`.

3.2.2 Aliasing

For any given entry in the Directory, an alias entry may be used. Aliases may be placed at any level of the DIT in order to facilitate searching in a smaller subset of the tree. An alias entry only contains a RDN and the DN of the object entry it references. An alias entry has no subordinates and is therefore always a leaf entry. The object entry pointed to by the alias entry contains the actual data requested. The conversion of an alias name to an object name is termed dereferencing. Exhibit 3-3 provides an example of the use of an alias `organizationalUnit` for the National Aeronautics and Space Administration (NASA) which is listed as an alias entry beneath the `O=U.S. Government` entry. NASA is currently registered as an organization beneath the country entry for the United States (`C=US`).

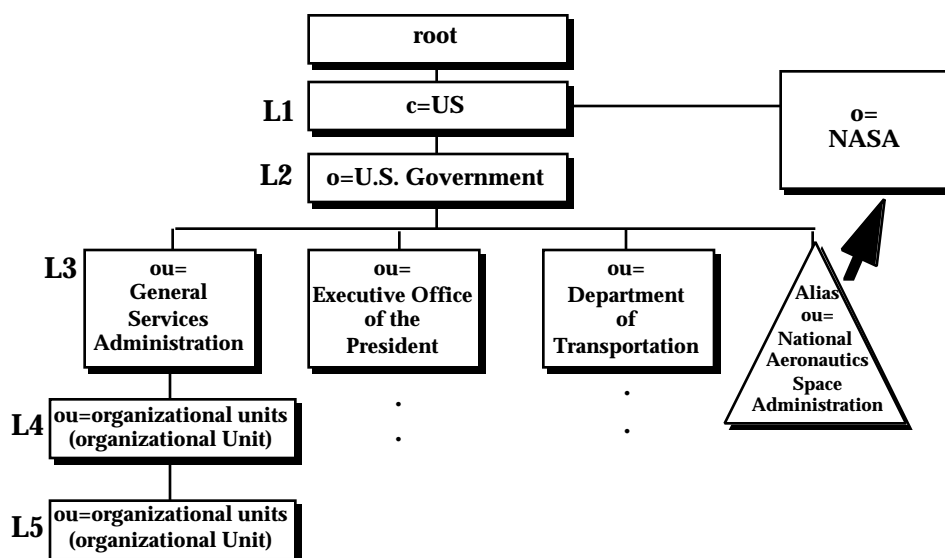


Exhibit 3-3
Alias First Level OU

Government Electronic Directory alias object classes are listed in Section 5.

3.2.3 Basic Recommendations

An RDN must be unambiguous for each object defined. The DN for each object will be unique in most cases if the RDN is defined properly and is unambiguous. The DIT design should be a compromise between depth and width, yet maintain uniqueness of objects. Documenting the entire organizational structure for the agency is generally not necessary to ensure uniqueness, and is not recommended. A maximum of eight levels of the DIT is recommended. The DIT design should reflect the most efficient method of organizing information for directory user.

As determined by the Agency, organizationalUnits or localities may be used at the second level and below. A locality may be used as an organizationalUnit at the second level (and below) if the first level OU is geographically dispersed throughout the U.S. Either an object class of locality or organizationalUnit may be used to designate the location depending upon the capability of the DUA (e.g., is it intelligent enough to determine that the input should be used to match to a locality or organizationalUnit value), as is demonstrated in Exhibit 3-4. This would also add a level to the DIT for an OU that is geographically dispersed, but would likely result in reduced search times.

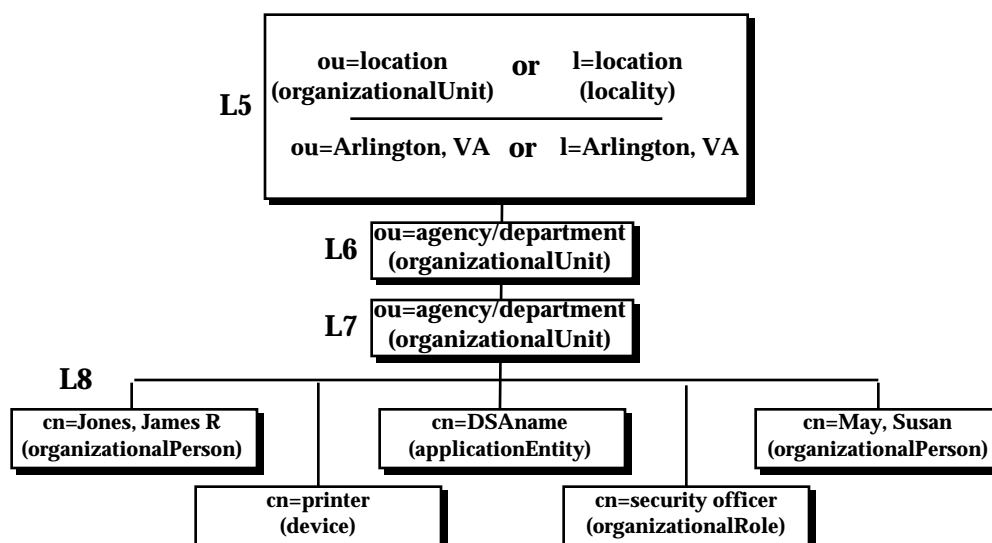


Exhibit 3-4
Organizational Subtree With Optional Locality

3.2.4 Naming Convention - `organizationalUnit`

The `organizationalUnitName` should be a user-friendly name for an organization within the Federal Government. It is not case-sensitive and the size is limited to 64 characters. The name must be kept as brief as possible, but still be recognizable.

3.2.5 Naming Convention - `locality`

The `localityName` should be a user-friendly name for the location as defined in its constitutional charter, articles of incorporation, or as generally recognized by a superior governmental entity (e.g., State of Virginia, Fairfax County, Fairfax City).

3.2.6 Naming Convention - `organizationalPerson`

Federal Government person entries should be listed in the agency/departments `organizationalUnit` name space, allowing for a `locality` to be designated in the organizational subtree in the Agency DIT for the purposes of uniqueness and unambiguity. The following guidelines are recommended for establishing `commonNames` for organizational persons (CN=organizational person's name). If possible, the name should comprise "LASTNAME, FIRSTNAME". The use of a middle initial (I) will occur only when required to form a unique name. As a general rule, `commonNames` will be formed from entries found in the organization's Personnel Records. In the future, names may be produced directly from information contained within the Personnel System. Each Agency should generate their names and resolve duplicates via the simple rules listed below.

Simple Rules:

1. Form the `commonName` by taking the "LASTNAME, FIRSTNAME". If the listing contains an initial and middle name, then use the listed middle name as FIRSTNAME. For example;

C. Everet Koop becomes Koop, Everet

2. If the formed name is one requiring resolution through the use of a middle initial, append the middle initial forming LASTNAME, FIRSTNAME I. For example:

Mary A. Johnson becomes Johnson, Mary A

NOTE: No period is used with the initial.

3. A list of chosen names should be submitted to the registration authority for a final check on uniqueness. If the `commonName` is, for some reason, offensive to the user, provisions are available to alter the FIRSTNAME (I). This will be handled on a case-by-case basis with the Agency registration authority.

Additional Construction Rules:

1. If the last name contains a space, such as Van Duzer, remove the space forming VanDuzer. For example:

John Van Duzer becomes VanDuzer, John

2. If the last name contains a “.” with or without a space, such as St. Denis, remove the “.” and space forming StDenis. For example:

Julie St. John becomes StJohn, Julie

3. If the last name contains a generation qualifier, such as Jr, Sr, or III, concatenate the given name and the generation qualifier to form a single word. For example:

Tom Nicholson, Jr. becomes Nicholson, TomJr

4. The use of an apostrophe or hyphen in the last name is permissible. For example:

Hillary Rodham-Clinton becomes Rodham-Clinton, Hillary

5. If the person's first and middle name are demanded, such as Mary Sue, then form the FIRSTNAME as MarySue. For example:

Mary Beth Johnson becomes Johnson, MaryBeth

6. If the middle initial is used to resolve duplicates, use a single character initial without the period. The middle initial will be used for all known duplicate “LASTNAME, FIRSTNAME” combinations to minimize future serialization of the middle initial when duplicate “LASTNAME, FIRSTNAME I” combinations occur. For example:

Mary A. Johnson becomes Johnson, Mary A
Mary M. Johnson becomes Johnson, Mary M
Mary D. Johnson becomes Johnson, Mary D

7. If two known duplicate “LASTNAME, FIRSTNAME I” combinations occur, one name will be formed without the middle initial (usually the second occurrence if they are not both discovered at the same time) to minimize serialization of the middle initial. For example:

Mary A. Johnson becomes Johnson, Mary A (1st occurrence)
Mary A. Johnson becomes Johnson, Mary (2nd occurrence)

8. If more than two known duplicate “LASTNAME, FIRSTNAME I” combinations occur, the first instance will be “LASTNAME, FIRSTNAME” (usually the second if they are not both discovered at the same time), the second will be “LASTNAME, FIRSTNAME I”, the third will be “LASTNAME, FIRSTNAME I1”, etc. For example:

Mary A. Johnson becomes Johnson, Mary A (1st occurrence)
Mary A. Johnson becomes Johnson, Mary (2nd occurrence)
Mary A. Johnson becomes Johnson, Mary A1 (3rd occurrence)

9. If the first name and middle name are initials, then use the two listed initials as FIRSTNAME, omitting the “.” and space. For example:

C. Wyatt becomes Wyatt, KC

3.2.6.1 User Friendly Names

Each person should also list other `commonNames` that they are known by, including nicknames. An alternate name allows for multiple values to produce a successful result when searching for an item in the Directory. For any given RDN in the Directory, multiple alternate values of the `commonName` may be included for the entry and the same structure/format must be used. For example, CN=Smith, James Q may be the RDN of an individual in the Directory. The entry may also contain other values such as CN=Smith, Jim and CN=Smith, James. In a search based on `commonName`, the entry is retrieved if any of the three common names is entered in a search request.

3.3 Non-Operational DITs

When DN's are required for test purposes, it is recommended that the RDN be appended with the symbol, (p), designating the RDN as provisional. This would be done in order to distinguish the DIT below as being used for test rather than operational purposes. Provisional DITs are temporary and should indicate in the registration when they will no longer be needed. A provisional subtree for GSA might be registered as:

OU = General Services Administration (p)

3.4 Government Contractors

Contractors that may be in the employ of the Federal Government and do not appear elsewhere in the global directory may have entries in the Government Electronic Directory. The contractor entry should be placed below the first level OU at any OU level where appropriate. The RDN for the OU should be the name of the contractor. For example, Booz-Allen & Hamilton as a contractor for the GSA would have an RDN under the GSA subtree in the DIT.

OU = Booz-Allen & Hamilton

Contractor subtrees can be aliased at the first level OU in the DIT pointing to an entry in the contractor name if one existed, or to an entry in the Federal Government DIT.