Frequently Asked Questions:

What Can I Be Doing Now?

Make sure your AD Group Policy Objects follow NIH naming practices.

Active Directory (AD) group policy is a feature that provides centralized management and configuration of computers and users in an AD environment. Group Policy Objects (GPOs) must have unique names. Naming rules are the following:

- GPOs should have the IC prefix followed by a space followed by a unique name related to the function of the GPO, for example, "CIT Vista Standards".
- Use letters a–z and A–Z and numerals 0–9. Note, because AD DNS is not case-sensitive, do not use upper and lower letter case to differentiate for the owner or purpose of a computer.
- You can use spaces, but no special characters.

For more information on naming, see: AD Attribute Data Content and Management: Best Community Practice

Transition your IC's GPOs to the NIH.GOV domain.

You can contact the "CIT AD Migration Team" and request that a blank GPO be created within NIH for each GPO that you will be moving up. Then, export your child domain GPO settings and import them into the new NIH GPOs. Test them thoroughly to make sure they work as expected. Typical problems in this area are references to the child domain that will have to be edited for the NIH domain. Note that FDCC policies must be linked to the original FDCC policies.

Analyze your applications for service account dependencies so that you know what accounts affect which applications.

Those accounts will eventually be migrated to NIH, so early analysis and identification will go a long way to smoothing the transition to using NIH resource/service accounts.

Make sure you have implemented an IC-wide policy to create all new accounts, groups, or computer objects in NIH.GOV.

This policy has been in place NIH-wide since April 23, 2008. All new accounts, groups, or computer objects should be created within the NIH domain, not within your child domain. You should change your desktop/server build processes so that ALL new computers are joined to the NIH domain rather than your child domain.

If you need to create any of these objects with your child domain, NIH Office of the Chief Information Security Officer (CISO) is developing a process of exception that you will apply for.

Use a GPO to set the primary DNS suffix to be the child domain DNS Zone.

NIH AD has already been configured to use the child domain DNS Zones (all ICs have been added to allowed suffixes at nih.gov). Enforcing DNS suffixes on servers and workstations can be done with a GPO. There is a setting called "Primary DNS Suffix" located in the Computer Configuration/Administrative Templates/Network/DNS Client portion of any GPO whose computer configuration settings are enabled. Desktops can then be set, when added, to default to IC.nih.gov.

Analyze your systems for DNS and convert your desktop and server computers to use NIH Dynamic DNS (DDNS).

It is important to ensure that the DNS on your desktop and server computers is configured to point to NIH DDNS. You can use DHCP to configure the DNS on client machines, and you will have to manually check your servers that have static IP addresses to make sure they are pointing to the NIH DDNS.

Clean up unused and obsolete objects in AD, especially user, group, and computer accounts.