UNITED STATES

GEOLOGICAL SURVEY

Active Directory Standard Operating Procedures

Version 1.3

February 16, 2005

Document Contacts:

ADIPT
Project Manager

Table of Contents

REVISION HISTORY

Date	Version	Description	Author(s)
04/13/2004	0.0	Initial Draft	Scott Brondel, SAIC
07/27/2004	0.1	Revised draft	Nelson Williams, USGS
11/04/2004	0.2	Added back-up policy and revised the draft	Nelson Williams, USGS
12/10/2004	0.3	Incorporated review comments from ADIPT	Nelson Williams, USGS
02/08/2005	1.0	Incorporated comments from regional review teams	Nelson Williams, USGS
02/11/2005	1.1	Modifications to several sections and several minor edits	Gail Kalen and Nicole Bogeajis, USGS
02/14/2005	1.2	Made major changes to backup policies	Nelson Williams, USGS
02/16/2005	1.3	Inclusion of graphic, additional modification to backup policies, and baseline of document	Scott Brondel, SAIC, Sam Martinez, USGS, and Nelson Williams, USGS

INTRODUCTION

The transition from hundreds of locally managed Active Directory (AD), NT, and Novell domains to a single, centrally managed AD domain in the U.S. Geological Survey (USGS) is bringing about significant changes in the duties of Information Technology (IT) personnel. Instead of each local domain being managed as a separate entity, a team, consisting of only a few USGS AD Domain Administrators, is responsible for tasks affecting the entire Bureau's domain. However, many tasks affecting science centers, districts, and field offices will remain the responsibility of the local IT personnel through the use of delegation.

The USGS employs many skilled and dedicated IT professionals working both in the field and on special projects in regional and national centers. Their expertise will be leveraged to implement and operate the Bureau's domain. In addition, they will continue to serve the USGS as experts in many IT and information management (IM) roles, which are not directly tied to the Bureau's AD domain.

Purpose

This document describes the standard operating procedures for USGS Domain Administrators, and local IT personnel. It also delineates the responsibilities of each group of administrators. Finally, it includes a detailed description of how backups are to be performed, logged, and verified.

Scope

The duties and responsibilities in this document are limited to IT personnel in the USGS. The specific role of the Department of Interior (DOI) Enterprise Administrator won't be described beyond defining the role in general terms.

Although operating procedures related to AD administration are the foundation of this document, duties and responsibilities described are not limited to the operation of the Bureau's AD domain.

This document should be considered as a USGS-specific supplement to Microsoft's AD Product Operating Guide, which is considered industry best practices. The Microsoft Product Operating Guide is available on-line at – http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/adpog/adpog1.mspx.

Although this document has been base lined, it should still be considered a living, breathing document as the project progresses. Therefore, it may be modified, as necessary. However, any change(s) must go through Change Management for approval before change(s) are applied to this document.

Definitions, Acronyms, and Abbreviations

AD	Active Directory
ADIPT	Active Directory Integrated Project Team
CCB	Configuration Control Board
CIU	Computing Infrastructure Unit
CTO	Chief Technology Officer
DC	Domain Controller
DOI	Department of Interior
GIO	Geographic Information Officer
IM	Information Management
IT	Information Technology
ITSOT	Information Technology Security Operations Team
LAN	Local Area Network
OLA	Operational Level Agreement
OU	Organizational Unit
PDC	Primary Domain Controller
RAID	Redundant Array of Independent Disks
RID	Relative Identifier
SA	System Administrator
SLA	Service Level Agreement
USGS	United States Geological Survey
WAN	Wide Area Network

LEVELS OF SYSTEM ADMINISTRATION

In discussing the Bureau's AD domain, there are four levels of system administration to be considered –

1. **Enterprise Administrator** – A manager who sets basic policies for all member domains, at the Departmental level. The USGS AD domain is part of the Department of Interior (DOI) AD forest, and hence is a member domain. The role and responsibilities of the Enterprise Administrator won't be described further in this document.

2. **Domain Administrators** – A team responsible for managing the Bureau's AD domain. This team may be a collection of USGS employees, or a group of contractors managed by one USGS employee. This group of administrators will be under the auspices of the Geographic Information Officer's (GIO) Computing Infrastructure Unit (CIU).

3. **Organizational Unit (OU) Administrators** – Individuals responsible for managing a logical grouping of computers, either at a science center, field office, or program office. These responsibilities are delegated by the Domain Administrators, in order to ensure the efficient and effective administration of IT resources. In most cases, current USGS System Administrators (SA) will be designated as the OU Administrators.

4. **Local Administrators** – A person, or persons, with administrative access to one or more individual member servers, workstations, and/or laptops at a given location. This role may, or may not be performed by the same person(s) as the local OU Administrator(s).

DOMAIN MANAGEMENT

Delegation in an Active Directory Environment

The delegation of administrative tasks is a necessity in a Windows 2003 enterprise environment. It is common to delegate authority not only to members of the IT group but to human resources personnel and various managers for tasks related to their duties. Delegation distributes the administrative workload without granting sweeping privileges to all users. This is an expression of the security concept of "principle of least privilege," that is, granting only the permissions necessary for performance of specific tasks.

Through various means, AD allows delegation of rights to groups or individuals for a prescribed degree of control over a limited set of objects. The only prerequisite is that the appropriate delegation elements (users, groups, Group Policy objects, files, directories, and so forth) must be in place before delegation can be performed. In the USGS AD environment, a default Organization Unit (OU) structure has been created that will provide OU Administrators with the permissions to perform their job functions without the need for full Domain Administrator rights and without having to rely on Domain Administrators to manage local resources.

Default OU Structure and Permissions

To illustrate the OU structure, a Water Resources District Office in the fictional location of Anytown, Missouri is used throughout this section as an example.

Prior to the Bureau's AD deployment, Anytown had a single Windows NT 4 domain, with 60 users and 90 client computers (workstations, servers, and laptops). In the USGS AD, Anytown's local resources exist in an OU named "AnytownMO-W", which sits beneath a top-level regional OU (in this example, it would be CR for Central Region). The OU name identifies the location of the site, as well as the discipline responsible for managing the local resources. The AD naming conventions can be found in the USGS Active Directory Naming Standards document.

The following steps will be performed by a Domain Administrator in preparation for Anytown's migration –

1. The "AnytownMO-W" OU and the "AnytownMO-W Full Admins" OU will be created beneath the "CR" OU
2. Inside the "AnytownMO-W Full Admins" OU, an "AnytownMO-W Delegators" OU and an "AnytownMO-W Admins" OU will be created
3. The groups "AnytownMO-W Full Admins" and "AnytownMO-W Delegation Group" will be created in the "AnytownMO-W Full Admins" OU
4. The "AnytownMO-W Full Admins" group will be given Full Control rights on –
    a. the "AnytownMO-W" OU and all child objects,
    b. the "AnytownMO-W Delegators" OU and all child objects, and
    c. the "AnytownMO-W Delegation Group" security group.
5. The "AnytownMO-W Delegation Group" security group will be given Full Control rights on the "AnytownMO-W Delegators" OU and all child objects

The purpose of this structure is to create three tiers of OU management. Members of the "AnytownMO-W Full Admins" group have total administrative control on the "AnytownMO-W" OU and the "AnytownMO-W Delegators" OU. The members of this group will perform functions similar to a Domain Administrator in an NT 4.0 domain. The "AnytownMO-W Full Admins" group is also added to the "OU Admins" group maintained by the Bureau's Domain Administrators. The "OU Admins" group is member of the "Group Policy Creator Owners" group. Thus, members of the "AnytownMO-W Full Admins" group can create and link new Group Policies.

Security groups can be created inside the "AnytownMO-W Admins" OU in order to delegate certain explicit duties in AD. The following are a few examples of such groups –

- An "AnytownMO-W Password Admins" group to allow Help Desk personnel to reset the passwords of users in the "AnytownMO-W" OU
- An "AnytownMO-W Account Unlockers" group to allow Help Desk personnel to unlock user accounts
- An "AnytownMO-W Workstation Installers" group to allow selected staff members create and delete computer accounts in the "AnytownMO-W" OU as new workstations are configured and installed.

The "AnytownMO-W Delegators" OU, along with its associated group, can be a difficult concept to grasp, but it will be useful in managing local resources. As illustrated above, the "AnytownMO-W Delegation Group" gets Full Control on all objects in the "AnytownMO-W Delegators" OU. This means that members of the delegation group have authority to set the membership of any administrator groups created in the "AnytownMO-W Admins" OU. Section chiefs, unit supervisors, etc., could be added to the “AnytownMO-W Delegation Group”, and they, in turn, can have granular control over which employees perform various functions.

Because the "AnytownMO-W Delegation Group" is NOT a part of the "AnytownMO-W Delegators" OU, members cannot add users into the group. If desired, the group could be moved into this OU, thus allowing its members to identify additional users.

The “AnytownMO-W Full Admins” group doesn’t have Full Control rights over the “AnytownMO-W Full Admins” OU. This means that members of the "AnytownMO-W Full Admins” group cannot change the membership of the group. Membership of Full Admins groups will be controlled by Bureau’s Domain Administrators, in order to ensure that members of the group have an appropriate base skill level for management of and AD domain or OU.

Figure 1 depicts a simplified example of OU structure in the Bureau’s AD domain, as described above. This example illustrates how the Bureau AD domain, gs.doi.net, will be divided into regions. Within each region, OUs will be created for each location. In addition, an OU for full administrators will be created for each location.

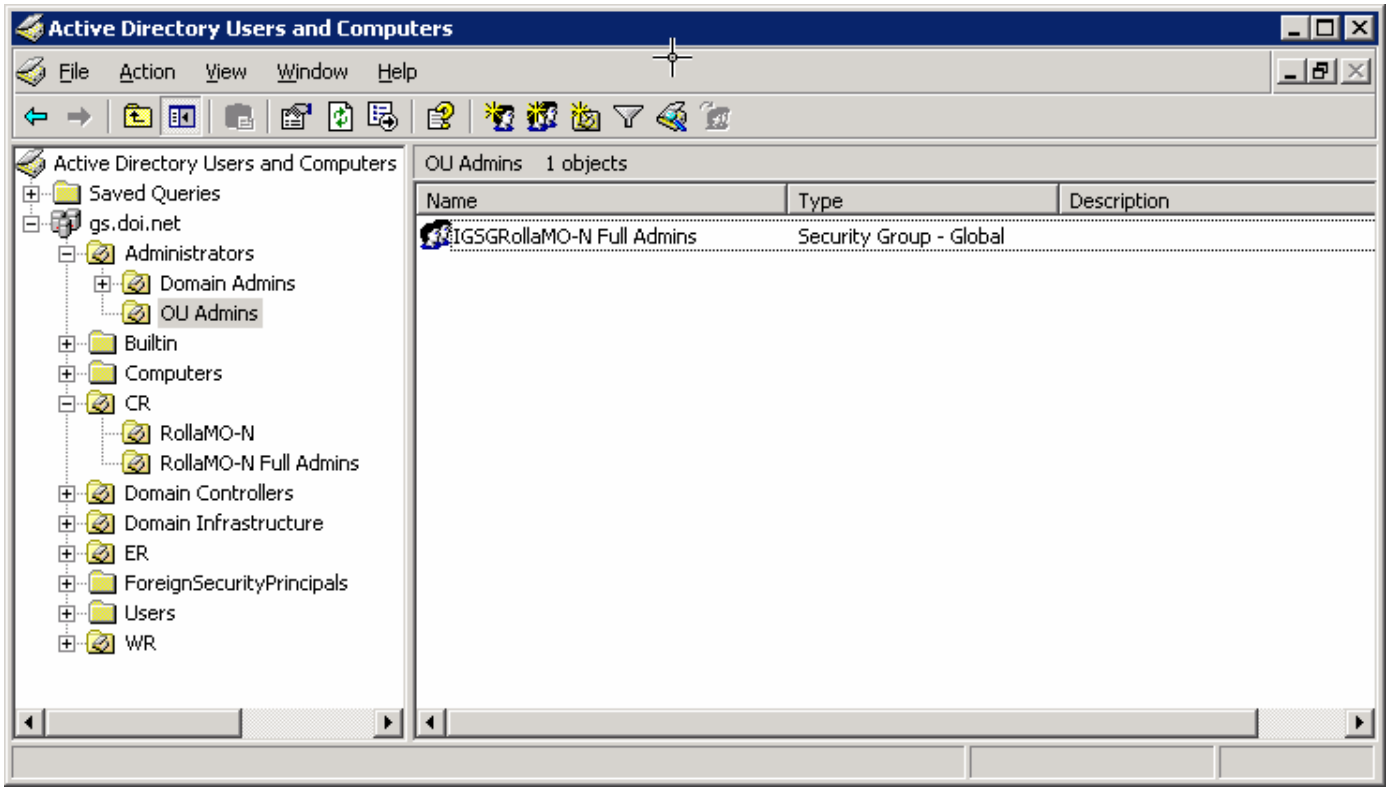

Figure 1—Screen capture showing an example of USGS AD structure.

DUTIES AND RESPONSIBILITIES

The intent of this section is to define the major responsibilities of the three classes of administrators – Domain, OU, and Local – working within the USGS domain, and to delineate among their respective duties. However, the duties and responsibilities of the Bureau's Domain Administrators and OU Administrators are intertwined. In order to successfully implement, manage, and maintain an efficient and effective AD domain, these two groups of administrators have to develop a positive, interdependent working relationship. Well established lines of communication are essential; and Operational Level Agreements (OLA) and Service Level Agreements (SLA), supported by USGS management, will be critical.

No administrator is allowed to include their personal, general office-use user ID in an administrator group for the domain or OU privileges. In lieu of using their general ID to perform administrative tasks on a system, OU, or the Bureau domain, AD administrators at all levels should use one of the following three options –

1. Use the "Run as…" option for executing utilities
2. Map network drives as the administrator in cases where the Windows Explorer is needed, or
3. Log in using the administrator ID for the domain, OU, or client computer, as appropriate

Domain Administrators

The Bureau's Domain Administrators are responsible for the day-to-day operations of the AD domain. The team is made up of six to ten full-time employees and/or contractors. There will be at least two Domain Administrators located in each regional office. Additional Domain Administrators may, or may not be located in regional offices. Whether they are contractors or USGS employees, they will report directly to the Bureau AD Project Manager. The Project Manager will serve as a member of the Computing Infrastructure Unit (CIU), which is a part of the Geographic Information Office (GIO) organizational structure. The Chief Technology Officer (CTO) will exercise responsibility for the overall direction of AD, while deferring day-to-day operational issues to the Project Manager, or to appropriate regional personnel.

The main AD-related duties of the Bureau's Domain Administrators can be divided into five categories – communication, configuration, monitoring, security, and routine maintenance.

Communication

- Train OU Administrators, local administrators, and Help Desk staff, as needed
- Test proficiency level of potential OU Administrators, as requested. Once requirements are met, elevate appropriate IT personnel to OU Administrator status
- Stay current with DOI Enterprise AD directions and policies. Provide feedback to CIU Chief and Chief Technology Officer (CTO), as appropriate
- Update intranet website with notices, status reports, and other useful information
- Advise OU Administrators of critical issues via e-mail, when necessary
- Report critical failures, or other serious issues, to the Bureau's Chief of the CIU and the CTO

- Report security incursions, following Bureau procedures, to the Information Technology Security Operations Team (ITSOT)
- Assist local sites with contingency planning and other required, AD-related documentation
- Assist local sites with transition planning and implementation
- Listen to, act upon, and appreciate input from OU Administrators regarding the operation and performance of the Bureau's AD domain
- Resolve issues and record results when problems are reported by the Help Desk

Configuration

- Manage domain account policies and other domain-level group policies
- Thoroughly test proposed changes in a non-production environment before implementation in the Bureau's production AD domain
- Coordinate, communicate to OU Administrators, and adapt to schema changes made by Enterprise Administrators
- Develop and provide baseline images for domain controllers
- Review and implement group policy changes submitted by OU Administrators using the Bureau funded NetIQ tools
- Coordinate all configuration changes with the Configuration Control Board (CCB)

Monitoring

- Check the event logs of AD Domain Controllers (DCs)
- Utilize Microsoft Operations Manager (MOM) to simplify monitoring of the state of the Bureau's domain
- Monitor AD database replication between sites
- Monitor WINS replication
- Closely monitor all AD DCs for security, usage, or hardware problems
- Check Performance Monitor, Network Monitor, Uptime/Downtime reports, and third-party tools for standard baselines
- Audit AD network for unauthorized changes and security problems
- Periodically evaluate software used for enterprise monitoring and administration
- Monitor performance and plan for needed capacity, budgeting for future modifications
- Replace monitoring and alerting tools (third party), as necessary

Security

- Develop risk assessments, contingency plans, continuity of operations plans, and complete certification and accreditation documents, as required by DOI mandates
- Ensure that anti-virus software is functioning properly and virus definitions on DCs are updating as expected
- Maintain Software Management System (SMS) server(s) for Bureau-level patch management of DCs
- Make appropriate entries to the Command Center Management Tool
- Backup AD Domain Controllers and verify functionality of backups
- Develop and maintain AD disaster recovery procedures. Implement AD disaster recovery, when necessary

Routine Maintenance

- Reboot AD Domain Controllers, as necessary. All reboots are cleared with the Configuration Control Board (CCB) and are logged
- Manage the Lotus-to-AD interface through Microsoft Metadirectory Services (MMS)
- Apply operating system patches, including service packs, on AD Domain Controllers
- Correct issues identified from reviews of event logs and other monitoring activities
- Maintain software and hardware contracts for all AD Domain Controllers and supporting hardware

OU Administrators

OU Administrators will be trained and certified from among the Bureau's pool of IT support personnel. Generally, the candidates will be science center, field, or project office system administrators. OU Administrators are, in many ways, the first line of defense for the Bureau's IT issues. They are assigned to perform IT administration functions in field offices, science centers, and project offices throughout the country, in U.S. Territories, and in some cases, in foreign countries. Members of this group are characterized by their ability to adapt to both changing Bureau IT policies and local conditions. Please note that, some of their most important contributions will be to field and project offices, and could include everything from development of local IT budgets to the maintenance of local power equipment. However, the Bureau will also depend on them to resolve, when possible, operational issues experienced by computer users. Problems which cannot be resolved locally should be referred to Domain Administrators by OU Administrators via the Bureau Help Desk.

For the purposes of this document, the duties of the OU Administrators are being divided into two groups -- OU Management Duties and Non-AD Duties.

OU Management Duties

The local OU Administrators are responsible for performing many duties in the Bureau's AD domain that are similar in nature to the job functions of an average SA in a locally-managed domain. The major differences are in adapting to policy changes made

at the Bureau or Departmental levels, and in communicating issues or coordinating work with appropriate parties at the Bureau level.

- Serve as the local point-of-contact for the USGS Domain Administrators to help troubleshoot potential AD DC problems
- Ensure the physical security of local DCs
- Log all hardware maintenance performed on AD Domain Controllers, if this happens at the local site
- Monitor member servers and workstations for intrusion or possible compromise. Notify appropriate contacts, as per Bureau policy, when incidents occur
- Configure, install, and maintain all local member servers and client workstations, using Bureau-standard baseline system images. The baseline images are merely a suggested starting point for member system configuration
- Propose group policy additions, modifications, and deletions to the Domain Administrators, for any group policy
- Check event logs on every member server. Resolve issues, as necessary
- Create new directories, shares, security groups, temporary and specialized user accounts, and group policies. Disable/delete specialized accounts, archive old profiles and workspaces, and remove old shares, as required
- Perform backups for member servers, workstations, and laptops, in accordance with Bureau and local IT policy. Periodically test the viability of back-ups by doing test restorations
- Provide AD training for end users
- Perform local disaster recovery for member servers and clients
- Ensure that all appropriate services are running on local servers
- Ensure that all local systems have up-to-date anti-virus definitions and recommended operating system patches
- Report AD-operational issues to Domain Administrators and the CIU via the Help Desk
- Monitor the Bureau's AD domain news items and status messages via the Intranet
- Maintain Software Update Service (SUS)/Windows Update Service (WUS) server(s) for local member servers, workstations, and laptops

Non-AD Duties

Not all OU Administrators will perform all of the duties listed in this section. However, these responsibilities are typical of the contributions made by the Bureau's many field-level SAs --

- Configure, maintain, and monitor the Local Area Network (LAN)
- Check local router and firewall logs. Manage local software and hardware firewalls in cooperation with the Bureau's ITSOT

- Check for free space on all local servers, for file pollution and quotas
- Run the *defrag* and *chkdsk* utilities on all local drives
- Keep service packs (and/or) hotfixes current on local member servers and workstations, as per agency policy
- Provide general IT training for end users
- Install software for users
- Verify that all third-party software in use is properly licensed
- Manage all local print queues
- Maintain all local applications
- Maintain local permissions and file systems
- Clear out rogue local profiles
- Clean local servers, check for .tmp files, and other file pollution
- Implement any new local policy, permission, logon script, or scheduled script modifications
- Check Performance Monitor, Network Monitor, Uptime/Downtime reports, and third party tools for standard baselines
- Reboot local servers as needed
- Remote access coordination for local users, including Virtual Private Network (VPN)
- Keep up-to-date on IT news regarding USGS networks
- Hands-on problem resolution and support
- IP management and Host (Domain Name Service (DNS)) registration
- Local e-mail support
- Represent local office at meetings or conferences
- Certification and Accreditation of local systems
- Documentation of local configurations
- Develop local IT budgets
- Supervise local IT staff, including webmasters, database administrators, etc.
- Manage enterprise class Unix servers for mission-critical databases

- Configure Windows XP workstations and laptops to interface with specialized scientific equipment, including paper-tape readers, magnetic media readers, laboratory analysis equipment, and remote sensing (field) equipment
- Coordinate service, upgrades, and programming of additional communications and environmental equipment
- Maintain on-site and off-site back-ups
- Prepare, maintain, and disseminate continuity of operations and contingency plans for local operations
- Maintain local generators and back-up power equipment, as required by local conditions
- Perform technical reviews of project proposals
- Support local report production
- Manage and maintain local peripherals, including printers and plotters. This will include coordination of service, upgrades, stocking media, and the like
- Hands-on and phone support of remote users in field offices serviced by district offices or science centers
- Procurement of new IT equipment and related supplies

Local Administrators

Although the group of local administrators will primarily be laptop users with administrative access only on their own laptops, there will be some other users with administrative access on workstations and servers. Non-laptop local administrators will include users in very small field offices with less than five users. The group may also include selected scientists running specialized software for modeling or other simulations of environmental conditions.

Delegation of local administrative authority should be granted by the appropriate OU administrator. The OU administrator will be expected to follow DOI and USGS guidelines and policies when making these determinations. Local Administrators will be responsible for informing the appropriate OU Administrators when operational issues arise.

Local Administrators will be responsible for –

- Applying updates and security patches
- Updating local virus definitions for unmanaged systems
- Ensuring that backups of laptops are performed periodically
- Installing applications
- Ensuring that all local, Bureau, and Departmental policies and procedures are followed before laptop computers are reconnected to the Internet

BACKUP PROCEDURES

This section will describe back-up procedures for DCs in general terms. It doesn't include details about specific hardware and software used to backup DCs because these may change with technology several times during the lifespan of the Bureau's AD domain. This section applies almost exclusively to Domain Administrators; OU Administrators won't have permission to backup DCs, because DOI is strictly limiting membership in the Backup Operators group.

The Domain Administrators are responsible for performing all backup procedures. They are also responsible for documenting and verifying the integrity of backups. All backups are performed during off-peak hours, in order to minimize disruption to and degradation of operations. These hours will be clearly posted on an intranet page devoted to the operational status of the Bureau's domain, and maintained by the Domain Administrators.

The AD database is replicated periodically among all DCs. This typically occurs every 15 minutes. The periodic replication provides AD database redundancy. Given normal network connectivity, Domain Administrators will have the capability of building and promoting new DCs on any member server without the use of backups.

There are three special AD operation master roles – Relative Identifier (RID) Master, Primary Domain Controller (PDC) Emulator, and Infrastructure Master – unique in the GS.DOI.Net domain, which must be managed differently with regards to backups. Tasks related to each of these master roles can be performed on one or more domain controllers. These controllers need not be assigned to a specific geographical location. Once established, master role services can easily be transferred from one DC to another. The DCs performing master role functions are the only DCs which require regular backups.

Domain Administrators may choose to backup additional DCs at their discretion, or at the request of OU Administrators. Any additional DCs to be backed up will be backed up using collocated member servers. This is because DOI won't allow OU Administrators to install any software or hardware on the DCs. The reason for considering backups of additional DCs is to create a local copy of a domain controller for use in disaster recovery. These local backups could cut recovery time by a day, or more, because with them, shipment of a disk image or disk drive may be unnecessary. OU Administrators won't be able to perform a restore using such a DC backup without assistance from the Domain Administrators.

Each DC will utilize a Redundant Array of Independent Disks (RAID) in order to reduce downtime and safeguard against the loss of data due to hardware failures. In addition, as stated above, the Bureau's DCs periodically and automatically replicate with each other over the Wide Area Network (WAN), thus providing another layer of protection against possible operational failures. The procedures described in this document are intended to facilitate the creation of backups in order to protect the DCs from possible inadvertent misconfiguration, accidental deletion of files, and unauthorized access which may result in the damage to files or data. It sets general schedules and quality assurance methods for Domain Administrators, and thereby sets a level of expectation for OU Administrators and users.

Full Backups

Complete backups will be done of DCs once per week. The full backups will include all disk partitions on each regional DC.

Each full back-up will be marked with a letter of the alphabet in order to uniquely identify it. If more than one tape, disk, or other removable storage medium is required for a full backup, then they will each be labeled with a sequence number. For example, if two tapes are required for a full backup cycle, and backup "M" is being performed, then the tapes will be labeled "M1" and "M2".

Once 26 backups have been completed, using media sets A through Z, an archive set is created, media set "A" is reused, and the cycle begins again. Hence, twice per year, two sets of full backups are created in a single week – the regular weekly backup and the archive copy. Because of the recycling of tapes, regular full backups are available for 26 weeks.

Differential Backups

A backup of all files modified since the last full backup will be created each weeknight, Monday through Friday. These are known as "differential backups." Differential backups are created instead of incremental backups in order to simplify restores. With this method, only the latest full and the latest differential backup are needed to restore a DC.

Each differential backup will be clearly labeled with the day of the week. For example, a differential backup created on Thursday will be labeled "Thursday". These media will be overwritten each week. Domain Administrators will be particularly diligent in checking the integrity of these media, replacing them as necessary.

Archives

Periodically archives of the system logs are created. Domain Administrators will determine archival frequency.

Archives of log files are kept indefinitely and are never recycled. If the backup/archive hardware is changed such that a different medium is used, then the old log archives will be converted to the new medium.

Disk Images

A copy of the most current disk image for a Bureau AD DC located in each regional office will be kept in that office on a non-volatile medium, such as a CD, DVD, or portable computer. At the end of each full-backup cycle, once every six months, the standard disk image will be checked to make certain it is current. If the disk image has been significantly updated, a new image will be created.

Disk images may be used to help sites recover from catastrophic failure, in lieu of sending them a replacement domain controller. An image could be loaded on a machine in the affected office(s) allowing a return to operational functionality.

Quality Assurance

Documentation of backups will be critical to the security of the overall Bureau AD domain. Each backup must be documented in hard copy form in two separate backup log books. One log book will be kept on-site with the backup media. The other will kept in a secured off-site location.

As media are recycled, the corresponding log sheets can be discarded. Hence, a log book will contain 26 pages for full backups (A-Z), five pages for differential back-ups.

The backup log sheets will include the media label, the date of the backup, and the signature and printed name of the person who performed and verified its successful completion.

Off-Site Storage

The most recent full backup should always be available on-site. The two previous full backups should be kept off-site. When a week-old full backup is transported to the off-site location, then the older of the two full backups off-site will be moved back to the on-site facility.

The off-site location must be a secure, climate controlled facility. Examples include, but are not limited to – 1) A local bank vault or safe deposit box; 2) A contract media storage facility; or 3) Another federal agency. The off-site location must be at

least one mile from the DC, although at least five miles of separation between locations are recommended. The intent is to reduce the likelihood that a major event, such as fire, earthquake, or tornado, will severely damage both sites.

Backup log sheets should be marked to indicate whether a media set are located on-site or off-site. They should also include dates the media were moved to one location or another. Finally, the logs should include the names of responsible parties for moving media to-and-from off-site locations, such that a chain-of-custody report can be generated.

Disposal

If the backup media become damaged through repeated use, they are to be physically destroyed prior to disposal. There must be a reasonable certainty that no data can be retrieved from these media. Compact disks should be shredded, micro-waved, or scratched. Similarly, tapes should be demagnetized and the cassettes destroyed with a hammer, drill, or other device.

THEFT OR COMPROMISE OF A DOMAIN CONTROLLER

If a DC, or its disk drives, is stolen, or a DC is compromised, there are a number of steps to be taken by the OU Administrator and by the Domain Administrators to prevent or limit disruption of the mission of the Bureau. This section describes these steps, in order, and provides contact appropriate information.

Theft

If a DC is stolen, the appropriate OU Administrator, or their designated back-up, must immediately contact three groups –

1. The Bureau Help Desk. The Help Desk can be contacted at (703) 648-7300, or via e-mail at GS Help Desk.
2. The Bureau's Information Technology System Operations Team (ITSOT). Contact should be made with ITSOT by filing an incident report via their web pages at – https://itsot.usgs.gov/ir_app/index.html
3. Local Law Enforcement. Contact information for local law enforcement officials should be located in your office's Continuity of Operations Plan. Save copies of their reports such that they can be sent to ITSOT.

In the case of DC theft, Domain Administrators, working with ITSOT, should issue an alert to all OU Administrators describing the situation and the actions being taken. A baseline of a Tier 1 DC should be archived. Domain Administrators will make sure that all users are forced to change their passwords on their next login. Finally, Domain Administrators will change any administrative account passwords as soon as possible.

If users report that they cannot log into the system following the incident, the corresponding OU Administrator must report this to ITSOT immediately. Once reported, the passwords for these users may be reset.

Compromise

If an OU or Domain Administrator has reason to believe that a DC has been compromised, they should immediately contact ITSOT and the Bureau Help Desk. Contact information is provided above.

If an OU Administrator reports a possible DC compromise, the Help Desk will notify the Domain Administrators. The Domain Administrators will then work with the appropriate OU Administrator and ITSOT to evaluate the situation, before filing a report and recommending action to the Project Manager and the Chief, CIU.

CATASTROPHIC NETWORK LOSS

Network connectivity can be lost for a number of reasons, including router failure, line cuts, or court decisions to remove DOI or individual Bureaus from the Internet. Loss of connectivity becomes catastrophic if it interferes with normal operations in an office, or offices, for more than four business hours.

If a catastrophic network failure occurs at a site which has a DC, then the failure shouldn't dramatically interfere with normal operations. In these cases, the appropriate OU Administrator should report the network outage to the Bureau Help Desk, and state clearly that a DC is present at the site. The matter will be referred to the GEONET Team for resolution, and electronic notification will be sent to the Domain Administrators apprising them of the situation.

If a DC is not present at the site, the OU administrator should report the network outage to the Bureau Help Desk, and state clearly that a DC is not present at the site. The matter will be referred to both the GEONET Team and the Domain Administrators. The GEONET Team will be charged with resolving the networking problem and providing the Domain Administrators with a reasonable estimate of how long the network outage may last.

In the case of sites with no DCs losing connectivity, the Domain Administrators will contact the appropriate OU Administrator(s) to explore possible temporary problem resolution. Domain Administrators may chose to –

1. Ship or deliver a back-up DC to the affected site
2. Ship or deliver a current disk image of a DC to a site which has available and compatible hardware
3. Ship or deliver a hard drive containing the system and data partitions of a DC
4. Request that a nearby OU administrator deliver a DC, or allow them to deliver a disk image or local back-up of a DC, provided the affected site has available and compatible hardware
5. Provide instructions for using dial-up lines to do user authentication for the affected site
6. Other

SUMMARY

There are four major levels of administration to be considered in the Bureau's AD domain. Using these standard operating procedures, the responsibilities for each level are delineated. Their work can be coordinated for the overall efficient and continuous operation of the domain.

The operating procedures described in this document are to be considered as Bureau-specific additions to, or clarifications of, the AD Product Operating Guide provided by Microsoft.

APPENDIX A

(Sample backup log sheets to be added)