



USGS

Active Directory Project

Business Requirements Document

Version 1.2

January 18, 2003

Paul Exter



Table of Contents

EXECUTIVE SUMMARY	2
REVISION HISTORY	3
INTRODUCTION.....	4
Document Overview	4
Audience	5
THE PROBLEM	6
PROJECT ASSUMPTIONS	8
PROJECT RISKS	9
SCOPE.....	10
BUSINESS REQUIREMENTS	11
FUNCTIONAL REQUIREMENTS	12
Scalability/Performance Requirements.....	12
Collaboration Requirements	12
Availability/Fault Tolerance Requirements	12
Centralized Manageability Requirements.....	12
Security Requirements	13
Networking Services Requirements.....	13
Interoperability/Migration Requirements	13
Reporting Requirements.....	14
Desktop Requirements.....	14
SIGN-OFF AGREEMENT	ERROR! BOOKMARK NOT DEFINED.



EXECUTIVE SUMMARY

The USGS serves the Nation as an independent fact-finding agency that collects, monitors, analyzes, and provides scientific understanding about natural resource conditions, issues, and problems. The value of the USGS to the Nation rests on its ability to carry out studies on a national scale and to sustain long-term monitoring and assessment of natural resources. The USGS provides impartial science that serves the needs of our changing world. The diversity of scientific expertise enables the USGS to carry out large-scale, multi-disciplinary investigations that build the base of knowledge about the Earth. In turn, decision makers at all levels of government--and citizens in all walks of life--have the information tools they need to address pressing societal issues.

The 10,000 scientists, technicians and support staff of the USGS are located in nearly 400 offices in every State and in several foreign countries. With a budget of more than \$1 billion dollars a year, the USGS leverages its resources and expertise in partnership with more than 2,000 agencies of State, local and tribal government, the academic community, other Federal allies, non-governmental organizations, and the private sector. Field investigations, direct observations of natural science processes and phenomena, and monitoring and data collection at the local scale are the scientific hallmarks of the USGS.

Currently, the USGS strains under the pressure of the Department to meet requirements and mitigate certain deficiencies noted by external parties. In an attempt to correct some Information Technology (IT) configurations, the USGS wishes to initiate a project to design and deploy a Microsoft Active Directory structure within the entire organization. Benefits achieved include *enhanced* security, simpler administration, extended interoperability, streamlined end-user signon, and the potential for reduced total cost of ownership (TCO).

This document will serve as a building set of business requirements. Politics, budgets, and business functions influence business requirements. Conflicting business requirements must then be prioritized. For example, a security requirement may be at odds with performance and application requirement. Once prioritized, these business requirements then spawn design functional requirements. Functional requirements have impacts and implications. Many times functional requirements will be altered when applied against existing circumstances. It's important to document the critical business requirements so actual implementations don't undermine those factors.

This paper documents the problem, assumptions, risks, scope, business requirements, and functional requirements of this project. A business case should build upon these items and guide the selection of suitable alternatives from which architectural designs are created.

As an overview, the principal business requirements and their significance are highlighted below:

- The project will demonstrate compliance with specific requirements originating from OMB Circular A-130 and mandates from the Department. In addition, it will demonstrate corrective action to the courts to assist in preventing future interruptions to agency operations.
- Enhanced security and a reduction in total cost of ownership will be achieved. One directory service will be used for user authentication across USGS. Only authorized users will be able to log onto workstations and access local/network resources. This architecture promotes:
 - The ability for USGS staff to authenticate into the network at any USGS facility.
 - Authorized access to USGS information when staff is conducting work at home or in travel status.
 - Easier access to common information and enhanced cross-discipline collaboration efforts.
- The ability to collect quality IT asset/infrastructure information for decision-making by policy makers and senior managers. The USGS will benefit from quicker, more accurate and more consistent reporting capabilities.



REVISION HISTORY

Paul Exter	1/20/03	Document Creation	▪ V 1.0
Paul Exter	2/02/03	Revised after January Core Meeting	▪ V 1.1
Paul Exter	2/11/03	ITAC Presentation	▪ V 1.2
			▪
			•
			•
			•



INTRODUCTION

In mid-August 2002, following an extensive Information Technology (IT) Management Reform Study conducted by Science Applications International Corporation (SAIC), DOI's Information Technology Management Council (ITMC) directed that planning be initiated for deployment of Microsoft Active Directory (AD) as Interior's enterprise directory service. That effort was bolstered on September 13, 2002, when Interior established Microsoft Windows server and desktop operating systems, the Microsoft Office suite of desktop applications, and Microsoft Systems Management Server (SMS) asset management software as DOI-wide standards. DOI has stated the Active Directory project will be complete by December 2004.

Since that time several bureaus have struggled with the concept of a DOI-Wide Active Directory. Upon hearing those concerns, and coupled with the current network design, the Department has taken a step back in its initial statement of a DOI-Wide Active Directory by December 2004.

The current direction from DOI is the following:

- Bureaus with an existing forest will act independently and not be merged at this time. A DOI business case will determine the final AD design. In the meantime most industry opinion suggests that a single forest will offer the best alternative, so current efforts will support this structure.
- Standards should be developed with a single forest in mind, and future work should comply with these standards.
- The business requirements document serves as a critical cornerstone for the business case.
- Funding for this project is limited, and implementation costs will be shared between the department and the bureaus.
- The executive sponsor for the AD Core Team is now John Branan.
- Recommended changes from the initial direction include:
 - Emphasize the business case for determining the final AD design,
 - Allow for the creation of a clean separate DOI forest as a *pilot* project,
 - Allow DOI Office of Secretary to be included in the *pilot*,
 - Allow the DOI network to complete before Bureaus join,
 - Specify that if the business case determines a single forest model is best, then existing forests will integrate into the DOI forest when "prune & graph" migration tools become available (anticipated within 2-4 years).

This leaves the USGS with a 2-3 year window to migrate from its current infrastructure to a centralized Active Directory structure. It allows proper planning to be accomplished and factors considered.

Document Overview

This document identifies problems inherent in USGS's existing IT infrastructure (when compared to a Active Directory migration) and describes the enterprise business requirements that will be targeted by Active Directory deployment across USGS.



Audience

The intended audience is USGS managerial and technical personnel. This document assumes the reader is familiar with basic information architecture concepts as well as information technology terms and acronyms, particularly those pertaining to directory services. It also assumes the audience is familiar with the requirements from the Department.



THE PROBLEM

The USGS faces an elevated level of scrutiny and a need to markedly improve IT security as a result of high profile legal proceedings. These requirements compel the USGS to promptly address existing IT infrastructure and data management problems without the luxury of extensive planning.

At current, the direction the USGS is taking to solidify its networks and systems may be in conflict with the need to deploy Active Directory. There are many ways to deploy Active Directory. The decisions made while designing a suitable approach to Active Directory deployment must be based on a clear understanding of agency business needs and strategic direction.

In order for the USGS to meet the Departments goal of a central Active Directory structure by 2005-2006, the USGS must address the following:

- The USGS currently has no support structure for a central Active Directory,
- Adequate testing and planning has not been preformed,
- Asset and discovery phases have not been completed,
- Secure configurations have not been outlined,
- Existing network projects are in conflict with the ability of Active Directory to communicate successfully,
- Existing name resolution does not separate internal from external,
- Existing security procedures prohibit Active Directory from functioning efficiently.

The USGS needs to embark on a comprehensive Active Directory Project plan, complete with the following:

♦ **Program Definition and Direction** - to establish Active Directory mission and objective
(Requires direction from the GIO)

- Complete Gap Analysis
- Create an Active Directory Integrated Project Team
- Modify / Create Business Case documents
- Create Goals, Vision, Objectives, high level Project Plan
- Acquire Funding, and Resources (Limited to Discovery and validation of AD)
- Risk Assessment
- Develop Project Timelines, Scope, etc

♦ **Program Development** -to develop efficient deployment plans

- Asset Information and critical areas needing attention
- USGS Discovery



- Continue testing / pilot environments
 - Documentation, standards, naming conventions, etc
 - Network design, DNS Infrastructure
 - Security Certification
 - Site Design, Backup Procedures ♦ *Program Oversight, Assurance, Implementation* -to coordinate accurate and timely implementation
 - Implementation –Phased
 - Revises budget Proposal
 - Training
 - Life-Cycle plans, Security plans, Firewall
 - Disaster Recovery, Contingency Plan
 - Enterprise Administration / Oversight, Administration support
 - Change Management control
 - Tactical and transition/migration plan ♦ *Program Oversight, Assurance, Implementation* -to coordinate accurate and timely implementation
 - Implementation –Phased Plan
 - Training
 - Life-Cycle plans, Security plans, Firewall
 - Disaster Recovery, Contingency Plan
 - Enterprise Administration / Oversight, Administration support
 - Change Management control
 - Tactical and transition/migration plan
-



PROJECT ASSUMPTIONS

To maximize chances for success of the USGS ployment project, justifiable assumptions must be documented and accepted. The assumptions must be validated and target dates should be established for elements not currently in place. If assumptions prove incorrect as the project proceeds, successful goal completion may be in jeopardy.

- Adequate funds and resources will be provided for this project. Project success is dependent upon adequate resources.
 - Microsoft Active Directory is the official directory service for the Department and USGS.
 - The USGS will have a physical network with connectivity to all endpoints and non-conflicting IP addresses for the operation of Active Directory. Connectivity across offices and firewalls is needed.
 - The physical network and AD design will be sufficiently integrated to ensure reliable directory services.
 - The AD design must be flexible enough to respond to Department mandates such as PKI.
 - Adequate AD Change Management processes will be developed and implemented.
 - Policies, standards and practices will be developed to provide a consistent security model.
 - This project will integrate with other key efforts such as the Network Security Project and the USGS DNS design.
 - Business and functional requirements will not significantly change during the design, development, and implementation of Active Directory.
 - Enough communication occurs between USGS AD Team members and bureau IT infrastructure managers to assure that the AD deployment is consistently implemented across the bureau.
 - Those responsible for administering the AD infrastructure will possess adequate knowledge, skills, and abilities to manage the directory service.
-



PROJECT RISKS

The following items are risks to successful Active Directory implementation within the USGS:

- Failure to validate the assumptions. If the assumptions are not valid, they need to be revised early in the project in order to avoid a subsequent high cost of correction. Each assumption is critical. For instance, if sufficient resources and funding aren't available, the project will fail.
 - Differing readiness levels exist with current USGS IT projects. If readiness levels aren't sufficiently considered and a limiting architecture design is chosen, failure to meet the deadlines may occur. Differing levels may conflict in overall design.
 - Conflicting priorities may drain momentum and resources from this project in the future.
 - Certain proposed network and directory services designs allow security threats to be isolated within individual offices. Configuring AD through series of firewall configurations could be problematic.
 - A comprehensive project plan is missing from this project. The scale of this project requires planning.
-



SCOPE

This project is highly susceptible to scope creep since it's being conducted in parallel with aspects of other USGS initiatives. As a preventive measure the following items have been identified as "within scope" or "out of scope":

Within scope:

- Windows Active Directory implementation for the entire USGS and ultimately the Department of the Interior
- Design and deployment of a department-wide internal DNS
- The establishment of a standardized, secure, desktop template for bureau implementation
- The design, deployment, and production environment of Microsoft Operations Manager (MOM) on all Active Directory dependent devices such as domain controllers

Out of scope:

- USGS intranet, the USGS telecommunication staff is charged with the implementation and maintenance of the physical network.
 - The reorganization of bureau IT staff into a USGS-wide IT organization with the goal of a more centralized Active Directory administration
 - The design, deployment, and operation of an SMS environment for inventory and audit. It is recommended this be identified as a separate project.
-



BUSINESS REQUIREMENTS

The following requirements for the Windows Active Directory implementation have been identified as they relate to USGS business goals and objectives:

- The project will facilitate compliance with requirements identified in OMB Circular A-130.
 - USGS staff will be able to authenticate into the network at any USGS facility.
 - One directory will exist for user authentication.
 - Only authorized users will be able to log onto workstations and access local/network resources. All authorized users will be uniquely identified. User credentials will not be shared between users.
 - The project will enhance the sharing of information across organizational, discipline and geographic boundaries by promoting:
 - Authorized access to USGS business information available for support work when staff is outside of the office environment (e.g. work at home or during travel).
 - Easier access to common information and facilitating cross-discipline collaboration efforts.
 - A common set of business rules related to authentication and access control services will be developed and maintained.
 - The project will facilitate the collection of quality information for decision-making by policy makers and senior managers.
 - The Active Directory implementation will provide a fundamental building block for the enterprise architecture. The Windows Active Directory design should be architected to minimize the bureau cost of deployment and the Total Cost of Ownership.
 - The project must be implemented with minimal impact to USGS existing production servers and business applications. All business critical applications must remain operational.
 - Adequate consideration for individual discipline readiness levels will be taken into account to ensure Active Directory is fully implemented within the USGS.
 - The final outcome will result in a secure and cost-effective solution, which promotes reliability and availability to the end user.
-



FUNCTIONAL REQUIREMENTS

USGS previously identified business requirements for Windows Active Directory, which yielded the following functional requirements:

Scalability/Performance Requirements

The USGS Active Directory project identified the following Windows Active Directory scalability and performance requirements:

- The Windows Active Directory architecture will be flexible to allow USGS to scale for approximately 20% growth with respect to the number of users without significantly impacting performance.
- The Windows Active Directory sites will be designed to minimize the replication and logon traffic across USGS WAN links.
- The Windows Active Directory architecture will be designed to ensure that users at branch offices with significant staff size and network-reliant resources attempt to authenticate from an Active Directory server local to the site. Authentication across WAN connections will be conducted only if the local server is unavailable.
- The Windows Active Directory design and implementation strategy will support possible reorganization to the DOI Active Directory by 2006-7.

Collaboration Requirements

The USGS Active Directory team has identified the following Windows Active Directory collaboration requirements:

- The USGS Active Directory architecture will be designed to ensure that USGS network users have the ability to authenticate and gain access to critical network resources at any USGS location.
- The USGS Active Directory design will support the sharing of data between all disciplines within the internal USGS network.
- The USGS Active Directory design will support the current USGS and future DOI implementation of video conferencing, chalk boarding, instant messaging, and other collaborative tools.

Availability/Fault Tolerance Requirements

The USGS Active Directory team identified the following Active Directory fault tolerance and availability requirements:

- Users at USGS office locations with significant staff size and network-reliant resources will authenticate to the Active Directory without relying on the availability of WAN links. Smaller offices may require this capability depending upon mission criticality or the lack of link reliability.
- Because Active Directory is very dependent on the DNS service, the design will ensure that larger USGS office locations with significant staff size and network-reliant resources maintain local servers capable of querying a local DNS server even if the WAN links are unavailable.
- A Windows Active Directory disaster recovery process must be established and tested to ensure domain controller system recovery in case of failure.

Centralized Manageability Requirements

The USGS Active Directory team identified the following Active Directory centralized management requirements:

- The Windows Active Directory design will provide the capability for enterprise management in a delegated administrative model.



- The Active Directory project will establish a USGS enterprise administrative group that will have the ability to audit all enterprise components. In addition, this USGS enterprise administrative group will have complete transparent access to bureau audit logs to facilitate responses to data calls and ensure compliance with directed security practices.
- USGS will utilize Terminal Services in Windows 2000 Server for remote administration duties.
- Active Directory services and devices will be managed and monitored with Microsoft Operations Manager (MOM).
- User provisioning will be supported for new hires. Resources would be digitally assigned to staff as they move throughout an organization. At the appropriate time the resources are systematically, uniformly, securely, and automatically removed.
- The USGS enterprise administrative group will only implement those directives as issued and sanctioned by the Change Advisory Board (CAB). The CAB will consist of representation from every discipline office. Formal change management procedures will be developed to support smooth enterprise operations. The CAB is also responsible for Active Directory lifecycle plans.

Security Requirements

The USGS Active Directory team identified the following Active Directory security requirements:

- The USGS Active Directory will provide a centralized directory for authentication on all Windows devices. Lightweight Directory Access Protocol (LDAP) or other protocols should be leveraged for authentication on non-Windows devices.
- The Active Directory design will provide the ability to apply granular security permissions to objects to limit the assignment of Domain Administrator rights to only a few users. Any security changes to group objects such as the Enterprise Administrators or Schema Administrators group will be audited. Security officers will have adequate permissions to read these audit logs.
- As USGS becomes a more centrally managed environment, the Active Directory architecture will provide the ability to delegate security control easily to objects or containers when necessary.
- The AD design will separate the “trusted” active directory DNS from the DNS for devices that are accessible via an Internet DMZ.
- The USGS network will need to evolve to support Active Directory.

Networking Services Requirements

The USGS Active Directory team identified the following networking services requirements:

- Because USGS will still maintain down-level clients and software applications that will require NetBIOS name resolution, WINS must be implemented or migrated to the new Windows infrastructure.
- USGS will utilize the Dynamic DNS (DDNS) features present in Windows 2000 to eliminate the manual input of records into the DNS databases.

Interoperability/Migration Requirements

The USGS Active Directory team identified the following Active Directory interoperability/migration requirements:

- Upon deployment the Windows Active Directory servers must interoperate with the existing Windows NT 4.0 member servers and potentially other network operating systems in the USGS enterprise.
 - The Windows Active Directory design will utilize established USGS and DOI naming standards for Active Directory objects.
-



Reporting Requirements

- The USGS Active Directory design will support the auditing of access to all USGS network/enterprise resources.
- Bureau Active Directory administrators must be able to provide transparent, complete, consistent, and timely audit reports to USGS administration.

Desktop Requirements

The USGS Active Directory team identified the following Active Directory desktop requirements:

- The USGS Active Directory design will maintain a secure Windows operating environment by using Kerberos 5 authentication support; which requires at a minimum the Windows 2000 desktop operating system.
 - The desktop design will identify a standardized minimum-security configuration that will be used by all disciplines. Offices will coordinate the migration of their desktops to this standard in order to ensure compliance by December 2004.
-