

USGS Windows Active Directory Project

Management Summary

Calendar Year 2004 promises to bring technology changes to USGS of unprecedented scope and scale. It will mark the first year of a profound transition from literally hundreds of distributed and highly disparate local computing environments to an integrated Bureau-wide infrastructure with a consistent technical architecture and common software tools.

Enterprise Directory Services

The fundamental building block of an *enterprise* infrastructure is a common **directory service**—a centralized and standardized *trusted* system that automates network management of user data, security controls, and distributed resources. An enterprise directory provides a single point of access for administering user accounts, clients, servers, and applications and reduces costs by eliminating duplication of effort. In a findings and determination directive signed in September 2002, the Department of the Interior (DOI) Assistant Secretary for Policy, Management and Budget designated Microsoft Windows **Active Directory** (AD) as the department's enterprise directory service. Thus, USGS participation in this Department-wide initiative is not optional; it is mandatory and it must be accomplished within an extremely compressed timeframe.

Security Benefits

Whether measured by the recently released Congressional scorecards in which DOI received an *F*, or by the weaknesses identified in IT Security Audits, DOI's reputation for compliance with Federal information security requirements and industry best practices is poor. Moreover, continued non-compliance with security standards is no longer limited to mere embarrassment or to intermittent inconveniences (as when DOI's Internet connections were severed by court order). OMB now threatens serious measures such as withholding of funds and imposition of increasingly burdensome certification and reporting requirements, unless DOI achieves substantial improvements this year.

The need to establish acceptable levels of information **security** is thus **the primary business driver** behind the initiative to implement AD. Fortunately, in addition to bringing DOI into regulatory compliance, an enhanced and modernized security platform will yield many benefits to USGS. Among the most important of these benefits will be a *common view* from the perspective of scientific end users. Because a single directory service will be used for user authentication across USGS, users will have fewer accounts and passwords to remember, and they will be required to log-in less frequently as they move from application to application. The ability of USGS staff to sign-on to an enterprise-level security manager at any USGS facility will promote flexibility and portability, especially when working at home or on travel.

Cost Savings

Even if there were no Department-wide directive to deploy central directory services, the aging USGS computing infrastructure needs rapid modernization. For example, current local area networks using the Microsoft NT 4.0 Operating System are no longer supported by Microsoft. Similarly, Novell technologies in use at many USGS locations are fast becoming obsolete. COTS (current off the shelf) software vendors offer software for Windows 2000 and Windows XP, but not for older operating systems widely used at USGS (e.g., Windows 95 and Windows 98). Therefore, the time has come to upgrade the USGS environment whether or not department-wide change is mandated.

Given that a general modernization is needed, the deployment of a standardized infrastructure based on AD affords important opportunities to reduce and contain costs through:

- Efficiencies in administration, support, and collaboration,
- Lower software costs under the department's Enterprise Licensing Agreement,
- Reductions in the total number of servers required, and
- Simplification of the Certification and Accreditation (C&A) process.

The last of these factors—a more efficient C&A process—represents an estimated savings of 500 man hours in local system administrator resources. This savings is due to the fact that the certification of an infrastructure that is consistently deployed under a central design model is far less costly than that of an infrastructure with more than three hundred distributed sites, each with differing security models and specifications. Furthermore, improved reliability, accessibility, manageability, and interoperability will all contribute to reductions in the total cost of ownership (TCO).

Other Benefits

The USGS Windows AD project is an important step toward developing a modern and extensible computing infrastructure to enable scientific processing, to ensure flexibility in responding to future requirements, to reduce administrative cycle times, and to provide new features and functionalities.

The central directory infrastructure will make it much easier to deploy new software, to distribute patches to fix bugs and vulnerabilities, to deliver rapid-response support, and to collect and analyze an IT asset inventory for decision support.¹ Centralized management utilities, troubleshooting tools, software management tools, and support for self-healing applications all make it simpler for administrators to deploy and manage servers as well as desktop and laptop computers. Exploiting the advantages of a common AD, administrators and IT resources in the USGS will be working together, not

¹ It should be noted that OMB has mandated that the Department build and maintain a comprehensive inventory of IT software and hardware assets this fiscal year.

independently. As a result, senior USGS IT managers will have dashboard views on the entire organization's IT lifecycle, security level, and health.²

A central directory service is also essential to the Bureau's participation in future Department-wide and government-wide initiatives. For example, pursuant to the E-Gov initiative in the President's Management Agenda, enterprise directory services will be an important building block for establishing Federal Identity Credentialing (FIC) and controlling access to DOI facilities. AD will also be integral to building a secure public key infrastructure (PKI) framework for improving controls over sensitive systems and for supporting digital signatures as required by the Paperwork Elimination Act. In addition, it parallels the Federal Enterprise Architecture program, and the Secretary of Interior's Program of Conservation through Collaboration, Cooperation, and Coordination, listed under Interior's Strategic Plan.

USGS Active Directory (AD) Project

To design an AD configuration that is consistent with the mission, structure, and culture of the USGS, a cross-disciplinary project team representing all regions and disciplines has been assembled. This team is working closely with Microsoft Consulting Services as well as other DOI bureaus and the Department to design the USGS infrastructure and to develop viable security templates, administrative procedures, and operational solutions. The project team expects to complete a detailed Active Directory design by the end of March, 2004. Thereafter, in the second quarter of 2004, a series of proof-of-concept pilot installations will be tested at selected USGS locations, beginning with Reston. Following successful testing, a complete implementation plan for the USGS will be published and an aggressive rollout and migration effort will begin. Preliminary plans call for the full migration of all USGS offices by the end of Fiscal Year 2005.

Effects of Change

The Windows AD Project presages important changes to the organizational, cultural, technical, and procedural aspects of the USGS. Until now, each office has operated independently of the others to support individual network and information services. Operational management of these diverse technological resources is the responsibility of distributed local and regional USGS offices. As a result, the environment is difficult to manage, and lack of interoperability is a significant problem. In formulating the USGS plan for deploying AD, the USGS team has given high priority to retaining as much local flexibility as is feasible by ensuring that local systems administrators retain sufficient authorities to perform their jobs effectively. Still, it is only fair to concede that some loss of autonomy will be felt and there will be resistance to changes of the breadth and magnitude brought on by this project.

² IT dashboards aggregate information and content onto a single screen to provide users with timely, actionable information to help them manage their overall corporate investment.