USGS FY04 Information Technology Implementation Plan

DRAFT

Contents

Document Description

The FY04 Information Technology Implementation Plan is an annual, tactical plan that describes bureau-wide Information Technology projects that will be implemented over the next 12 months.

Background

Throughout FY03, a number of bureau-wide IT projects were initiated which had a significant impact on field IT resources (System and Network Administrators, IT Security Staff, Lotus Administrators, etc.) Examples include numerous data calls, server security patching, NWIS Certification and Accreditation, DMZ deployment, the separation of Public and Private Data, Required Security Training, FTP consolidation, and the implementation of Enterprise Security Manager. All of these initiatives competed for the same local IT support resources. In the absence of prioritization, integration, communication, and planning, field support staffs were frequently confused, frustrated and ultimately over-worked to comply with short-term deadlines.

Purpose

The primary purpose of this document is to provide USGS personnel (Regional Executives, Science Center Chiefs, System and Network Administrators, Scientists, etc.) with information that describes the cross-bureau projects that are anticipated by USGS IT Managers. Through a partnership in planning, necessary for the drafting of this document, Bureau IT managers have identified, prioritized and integrated projects that span the Office of Information Technology, the Bureau IT Security Manager, the Regional Geographic Information Officers, USGS Disciplines and the Department of Interior. The Plan provides the identification and prioritization of IT projects, illustrates dependencies between projects, identifies the anticipated schedule and provides estimates of the commitment of resources required at the local science center level.

External Information Technology Influences

There are many external drivers influencing Information Technology initiatives in the USGS. These include the President's Management Agenda, the E-Government Initiative, Federal IT reform, legal challenges, oversight agency audits (GAO, OMB, DOI IG) and the Department of Interior.

Federal Information Technology Reform is a movement in Government to ensure the appropriate management of Information Technology resources and the maximization of their efficiency and benefits in achieving the Agencies mission. Laws passed include:

The Federal Information Technology Reform Act of 1996 (Clinger-Cohen Act),
The Government Information Security Reform Act (GISRA),
The Federal Information Security Management Act (FISMA),
The E-Government Act of 2002, and
The Homeland Security Act of 2002.

In conjunction with ongoing Federal IT reform, the Department of Interior (DOI) issued Secretarial Order 3244, "Standardization of Information Technology Functions and Establishment of Funding Authorities", on

November 25, 2002. This order is the impetus behind far-reaching IT management standardization across the Department. A significant portion of that strategy was documented in the DOI IT Transformation Strategy, which includes the following:

Evolving toward a common IT environment and infrastructure across all bureaus.
Standardizing on industry standard and "well accepted" technologies.
Executing integrated projects to upgrade the infrastructure, i.e. Active Directory, email messaging, smart cards, etc.
Enhancing the security of all DOI IT infrastructures.

Enhancing and securing IT infrastructure is also a critical component of the President's Management Agenda (as part of E-government) and is of central importance to Homeland Security. As a result of this government-wide emphasis, as well as recent Indian trust data security issues, OMB and the Department continue to emphasize IT infrastructure consolidation, enhancement and security as the highest IT-related.

Recent DOI guidance includes the DOI 5-Year IT Transformation Strategy (June 2003), the DOI Security Staffing Study Draft (Nov. 2003), and Enterprise Services Center Concept of Operations Draft (Nov. 2003).

The FY04 IT Agenda

In FY04 the Bureau will continue to participate in the DOI-wide implementation of more secure, standardized and consolidated approaches for critical IT infrastructure components. We work toward improving internal communication processes among the IT community, and we will execute projects aimed at improving our contributions to science and the mission of the USGS.

The projects described in this document are driven in large part by the external influences described above. However, they are also driven by the internal goals of the USGS to maximize the effectiveness and efficiency of our IT infrastructure. Information technology is a major USGS investment and a key enabler in the performance of the USGS mission. It therefore warrants the effective and adequate management of its architecture and resources.

How to Use This Document

The list of projects is split into two sections: 1.) PROJECTS WITH DIRECT IMPACT ON THE FIELD, and 2.) PROJECTS TO BE AWARE OF. The latter section lists projects requiring little to no resources from local science centers. The document index provides a list of all projects as well as the page number on which to find a description of the project. Each project is listed in the same format and includes the identification of each manager and contact information, project background, actions required in FY04, the anticipated level of effort required, and the expected project schedule. Questions on individual projects should be directed to the project manager listed in the project's description.

An Evolving Landscape

Given the number of external influences, changing priorities and limited resources, it is likely that changes to individual projects as well as the overall agenda will be necessary. In order to accommodate these changes, the FY04 IT Plan will be updated on a regular basis throughout the year.

PROJECTS WITH DIRECT IMPACT ON THE FIELD

Project: IT Asset Inventory

Project Manager: Larry McIrvin, CTO Office, *lmcirvin@usgs.gov*, 703 648 4664

Background:
A detailed IT Asset Inventory is required to support a number of IT management requirements including Circular A-130 C&A, vulnerability awareness and configuration management.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required:
The level of effort to inventory and enter this data will vary from office to office based on the complexity of the local IT environment. However, it is estimated that the average office will require 3-5 days to conduct the inventory and 2-3 days to enter or verify the information.

Linkages & Dependencies to Other Projects: ITSOT, BITSM and Help Desk

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.): Not yet determined, depends on decision to use COTS or custom database.

Estimated Project Cost and Probable Source of Funds:

- Labor Costs: $300,000 for custom database developed by a contractor
- Training Costs
- Equipment Costs: $10,000 hardware, $300,000 for COTS software including installation.
- Source of Funds

Benefit to USGS Mission:
Provide accurate up to date inventory of IT Assets and allow quick, easy and accurate reports as needed.

Schedule: The Project will start in the 2nd quarter of FY04.

FY 04 Action and Tasks:
During FY04, the Information Technology Office (ITO) will develop a web-accessible database for storing IT Asset Inventory information. As much inventory data as possible will be collected by automated procedures. Field system and network administrators will be asked to input data not automatically collected and verify automatically collected data in this database on a quarterly basis. It is expected that this database will dramatically reduce the number of data calls sent to the field. Additionally, the database will provide local inventory support to field IT staffs.

Project: Evaluation of Public Data and Content

Project Manager: Tim A. Brown, ITSOT Team, Web Site: ???

Background: When publishing any data on behalf of the USGS, it is necessary to evaluate that data for its appropriateness for public consumption. Of specific concern is Privacy data, Proprietary data, of sensitive data such as For Official Use Only, or information that could be used to compromise USGS security controls.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: The level of effort to evaluate publicly accessible data will vary from office to office based on the amount of public data provided by the local office. However, it is estimated that the average office will require 3-5 days to conduct the appropriateness evaluation.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: The evaluation can be conducted at the convenience of the local office, but should be completed by the second quarter of FY04.

FY 04 Action and Tasks: In FY04 the CTO will ask all offices to evaluate their publicly assessable data for appropriateness.

Project: IT Security Operations Team (ITSOT) Firewall Team & DMZ Implementation & Re--addressing of Public IP

Project Manager: Timothy A. Brown, Interim ITSOT Firewall Team Lead

Background:
The mission of the ITSOT firewall team is to ensure the security of the network perimeter.

Firewall technology will be used to protect the local area networks from the wide area network and the Internet by enforcing a 'deny all except as specifically authorized' security policy. This security policy will be applied independently to both the internal protected (private) and demilitarized zone (DMZ) networks at all USGS locations. The deployed firewalls will be fully stateful and consistent with recommendations specified in the DOI Perimeter Security Plan and NIST 800-41. The operation of stateful analysis at each science center provides enhanced security through containment; whereby an infected system cannot be used to attack systems at other locations.

The ITSOT Firewall Program is designed to:

- Improve the overall security of the USGS Wide-Area Network
- Manage the firewalls in a consistent manner and in accordance with the DOI Perimeter Security plan
- Centralize the configuration and administration of network security devices under the USGS CTO with direction from the BITSM
- Control costs of network security
- Assure high quality standards in the administration of network security devices

The Department has directed all Bureaus to move (physically or logically) public web and FTP servers to a DMZ network in order to separate the public servers from internal systems. The separation of public services is underway with the deployment of a DMZ architecture. As part of the DMZ strategy, the Bureau also is reducing exposure to the Internet by consolidating public services, if feasible, to regional locations. For cases where a business case is presented to show that consolidation to a regional location is not possible, the Bureau ITSOT and Geonet teams will build DMZ networks at the local site.

Mandates/External Drivers (DOI Federal Regulations, Etc.): DOI Network Perimeter Security Standard

Level of Effort Required:
The level of effort required is dependent on the security practices of the respective science center. At sites that have complicated IT environments, including the multiple-use of some servers, the amount of effort to separate systems will be substantial. In addition, at sites that have servers providing public information and internal services that include information not intended for public distribution, resources will be needed to acquire additional equipment and software. The acquisition and deployment of equipment and software is necessary to effectively separate the functions into private (internal) and public (DMZ) resources.

Linkages & Dependencies to Other Projects:
The completion of this project is dependant on the dissemination of Department and Bureau policies in order to obtain cooperation from administrators of affected information and network-security resources.

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):
The USGS Security Working Group must ensure that Department and Bureau policies are disseminated and understood. A process for receiving and evaluating science center business cases must be developed. The "field" science centers must have the alternatives explained. Where needed, the ITSOT and Geonet teams will build the networks and configure the necessary firewalls. When the ITSOT is staffed with permanent team members, the centralization of firewall management will be expanded. At sites large enough to have a dedicated firewall administrator, the firewall configurations will be subjected to peer review. At sites with firewalls not under ITSOT management and without dedicated firewall administrators, the local management will be asked to allow the ITSOT to mange, or replace, the firewalls.

Estimated Project Cost and Probable Source of Funds:

- Labor Costs: 3 FTE (permanent)
- Training Costs: Netscreen Training – $7500 (3 slots @ $2500)
- Equipment Costs:
  Rough order of Magnitude estimates:
  Initial purchases: 100k (HW – Netcontinuum proxy servers, appliance firewalls); 50k (SW and licensing)
  Recapitalization: 250k
- Source of Funds: CTO Network Security Project Account

Benefit to USGS Mission:
Completion of the firewall and DMZ implementations allows the USGS to continue serving information to external customers. The USGS must meet DOI mandates in order to maintain connection to the Internet. The enhanced security provided by the firewalls and DMZs allows USGS to ensure the confidentiality, integrity and availability of network-connected information resources. The use of a separate Internet Protocol (IP) address range for public systems will allow enhanced filtering to be implemented at the Internet gateways.

Schedule:
The dissemination of Bureau and Department policy should occur immediately. The process for receiving and evaluating business cases also must be developed immediately. The ITSOT and GeoNet teams will work to deploy the DMZ networks on a case-by-case basis. Much of the needed network infrastructure (OSPF routing, IP address assignments, etc.) was implemented in July and August of 2003 when DMZ networks were built for the Water Resources Discipline. The schedule deadline for separation of public and private systems is March 31, 2004.

FY 04 Action and Tasks:
The USGS Security Working Group must ensure that Department and Bureau policies are disseminated and understood. A process for receiving and evaluating science center business cases must be developed. The "field" science centers must have the alternatives explained. Where needed, the ITSOT and Geonet teams will build the networks and configure the necessary firewalls. When the ITSOT is staffed with permanent team members, the centralization of firewall management will be expanded. At sites large enough to have a dedicated firewall administrator, the firewall configurations will be subjected to peer review. At sites with firewalls not under ITSOT management and without dedicated firewall administrators, the local management will be asked to allow the ITSOT to mange, or replace, the firewalls.

Project: Bureau Active Directory

Project Manager: Paul Exter, CTO Office, Web Site: *www.usgs.ad.gov*

Background: 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. In continuing their enterprise architecture, DOI is requiring all Bureaus of Interior to centrally manage their IT investment and configurations via Microsoft Active Directory.

DOI has stated that the AD project will be completed by December 2004 and Bureaus will be expected to migrate to a DOI Active Directory by September 2005. These configurations are consistent with DOI Enterprise Architecture.

For USGS, information technology resources have been traditionally managed at the office level. In meeting DOI architecture goals it is increasingly important USGS strive to manage certain network and IT resources uniformly, in a cost effective manner, across the entire Bureau. 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 sign on, and the potential for reduced total cost of ownership (TCO).

In addition to DOI initiatives, the USGS must also consider the replacement for the NT 4.0 server operating system and the Microsoft domain model that will lose support by Microsoft in December 2003.

To this end, the USGS wishes Active Directory to replace the current disparate directory services used across the Bureau, significantly improving the security of information and the ability to share information Bureau-wide. An Active Directory configuration will also align the USGS with the strategic goals of the Department and its own Operations Mission. These configurations will be consistent with our ongoing mission to improve and decrease costs related to Information Technology.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: This is a large effort for the USGS involving a cross-bureau core team that consists of System and Network Administrators, and representatives from each region. A core AD team will be created to design, develop and implement the USGS AD backbone. After the backbone is deployed, AD will be deployed to every USGS office under a single deployment plan developed by the core AD Team. During AD deployment it is expected that local office system and network administrators will be required to dedicate their full time to the AD implementation. The length of time required to deploy AD will vary from office to office based on size.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: The AD effort will be a continuous schedule. Planning will begin in December 2003 and continue through February 2004. Implementation is currently scheduled for March 2004 through December 2005.

The AD effort will be a continuous schedule. Planning will begin in December 2003 and continue through February 2004. Implementation is currently scheduled for March 2004 through December 2005.

FY 04 Action and Tasks: The CTO will develop a comprehensive project plan for Active Directory planning and implementation for the USGS.

Project: Baseline Security for Desktop Hardening

Project Manager: Brenda Flanagan (CR-GIO) and Linda Peng (CTO), Web Site: *http://wdst.cr.usgs.gov*

Background: Recent inspections of U.S. Geological Survey (USGS) workstations concluded that the majority of the workstations and laptop computers do not comply with the security standards established by the National Institute of Standards and Technology (NIST), the Department of Interior (DOI), and the Office of Management and Budget (OMB).

To ensure the USGS workstations comply with the security measures, DOI and contracted agencies are conducting audits on a regular basis. These audits can be performed in person or by remote scanning technologies to determine whether a given workstation is secure. If security vulnerabilities are discovered, the offending workstation and related devices will be shut down until the workstation complies with the documented standards.

All workstations and laptops that connect to the USGS must be secured, in order to protect USGS information from unauthorized access. Since over 80% of these devices are currently using a Windows-based platform, this project is focused on those devices. Macintosh and Unix platform-based devices will be addressed by separate but coordinated projects.

To proactively help the USGS comply with the mandated security standards, a team was formed in March 2003. The Windows Desktop Security Team (WDST) consists of system administrator (SA) representatives from all the disciplines who will implement and maintain a minimum USGS baseline security standard. Standards and procedures developed by the WDST, where appropriate, will be implemented throughout the organization.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: An inventory will be performed on each workstation and laptop to identify the hardware configuration and OS level to determine the course of action the SA needs to take with that system. Depending on the information gathered, the system will require some or all of these to be performed: hardware replacement, an OS upgrade to Windows XP Pro, the application of the baseline security template, and the

configuration of automated security measures to continue the maintenance, e.g. Antivirus software updates and Windows critical patches.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: In late March 2003, a pilot was started in the National Center in Reston, VA. The pilot is expected to complete in December 31, 2003. Rollouts in the regional offices will be in phases. Project completion is December 31, 2004.

FY 04 Action and Tasks: In FY04, the CTO will develop a project plan for Windows Desktop Hardening and start the implementation process in the regional offices.

Project: Symantec Anti-Virus Services and Software Update Services (SUS) Implementation

Project Manager: Paul Exter and Garry Neverdon, Office of Information Technology

Background:

All workstations and laptops that connect to the U.S. Geological Survey (USGS) must have anti-virus software installed and configured, in order to protect USGS information from threat. The USGS maintains an enterprise software agreement for anti-virus control with Symantec Corporation. Virus update signatures are typically released at a rate of once per week. These updates must be applied to all USGS Windows-based computers with urgency, in order to maintain an adequate level of host-based security. At present there is no consistent procedure for applying updates to computers. Offices are charged with configuring and deploying technologies and configurations to update virus definitions. The USGS would like to streamline virus updates, reporting and deployment to a consistent process for all offices and locations, thereby maintaining an adequate security level for all networked systems.

The objective is to consistently update and report on all Windows workstations, servers and laptops accessing the USGS network from vulnerability in the following manner:

- Install a managed top layer Symantec Anti-Virus (SAV) design for each Regional location, including messaging, gateway and ftp/http traffic
- Implement second layer designs at each major science center
- Use Symantec Event Center to consolidate reporting across all servers
- Establish support for Regional servers, software distribution and vulnerability notification
- Establish a method of communication to offices when threats are released
- Establish a mechanism for consolidated reporting to the CTO on systems infected

In addition to antivirus, the Microsoft Corporation releases critical security updates in reaction to security vulnerabilities discovered in all versions of the Windows operating system and Internet Explorer at an average of one per week. These updates must be applied to all USGS Windows-based computers with urgency, in order to maintain an adequate level of host-based security. At present there is no consistent procedure for applying updates to computers. Offices are charged with configuring and deploying many technologies and configurations to patch systems. The USGS would like to streamline patch management to a consistent process for all offices and locations, thereby maintaining an adequate security level for all networked systems.
The objective is to consistently secure all Windows workstations, servers and laptops accessing the USGS network from vulnerability in the following manner:

- Install a managed top layer Software Update Service (SUS) design for each Regional location
- Implement a child layer design at each office requiring the need for local servers
- Establish support for Regional servers and vulnerability notification
- Establish a method of communication to offices prior to patch release
- Establish a test network prior to patch release
- Establish a mechanism for consolidated reporting

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required (Impact on Customers or Field Offices):

- **Equipment –** Nine (9) servers (redundancy) in three Regional locations. Six servers, 2 in each region, for SUS and one in each region for Symantec Event Manager (60k), SUS (free). Three servers are currently in production, therefore there are six for acquisition which may exist within the Regions.
- **Staffing –** It is recommended each Region support and maintain each server with concurrence from WTST and ITSOT. Each office will secure and maintain local servers. Each Regional security FTE will be responsible for virus and system update, release, reporting and dissemination. It is estimated that this team approach will spend an average of 2-to-4 person hours per day (½ FTE), total, to perform the necessary duties on the central USGS SAV and SUS servers (check logs, process updates, generate reports and maintain the servers themselves), assuming a rate of one update per week. Additionally support will be needed at the gateway, messaging and ftp locations. These rates will vary depending and no estimate is available.
- **Training –** Training is required for Regional SAV administration, Event Manager Installation and administration and local Parent server administration. The Regional team will need representation from each Region (Brody, Schachte, Van Dreser) that will coordinate regional information dissemination and implementation. In addition, the team will need a directional email from the GIO on the standardization of SAV parent servers in each Region, so that Event Manager reporting configured to include local offices. For SUS, system administration knowledge is required and the Regional SUS team (Flanagan, McHendrie, ER POC) will coordinate regional information dissemination and implementation. In addition, the team will need a directional email from the GIO on the standardization of SUS and the need for each location with local servers to configure central updates of MS vulnerabilities.

Linkages & Dependencies to Other Projects: None.

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.): See level of effort above.

Estimated Project Cost and Probable Source of Funds:

3 teams (one in each region equaling ½ FTE each) and 6
$50,000.00 (FTE) per Region = $150,000.00 total per year. This cost may be reduced due to current FTE participation.

Hardware cost = $9000.00 for remaining 6 servers, and $27,000.00 replacement cost for every 5 years thereafter.

Benefit to USGS Mission:

Completion of this project will allow USGS to enhance compliancy with federal regulations.

Schedule:
All phases will be completed by May 31, 2004

- Phase 1: Create a USGS-wide Regional team to establish secure SAV and SUS configurations for all Windows workstations, servers and laptops and formalize as policy.

- Phase 2: Pilot in the Central Region and Headquarters
- Phase 3: Rollout in Western Region
- Phase 4: Rollout in the Eastern Region
- Phase 5: Project Closeout and maintenance

FY 04 Action and Tasks:

The primary scope of this project is to update virus definitions and to secure all Windows workstations, servers and laptops from vulnerabilities that access the USGS network in order to support the minimum USGS security standard. The CTO will develop a comprehensive project plan for SAV and SUS implementation utilizing resources from the Windows Technical Support Team (WTST), and the Information Technology Security Operations Team (ITSOT). This effort will be coordinated with the Regional Security Managers.

Project: Command Center

Project Manager: BITSM Staff

Background:

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required:

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule:

FY 04 Action and Tasks:

Project: Enterprise Security Manager

Project Manager: Mike McNally, BITSM Staff

Background: Efforts to secure our IT Assets are driven by Laws, Policies and mandates. There are two important sources of requirements that are driving the IT Security efforts today. The first, called OMB Circular A-130, which is a policy, has been around for some time. The Federal Information Security Management Act or FISMA is the second.

FISMA amends the Paperwork Reduction Act and requires the head of each agency to develop and maintain an inventory of major information systems operated by or under the control of the agency. The BITSM works with the Bureau managers in determining which systems are to be included in the inventory. At this time there are 13 systems in the USGS inventory. Each system on the inventory is required to move to full accreditation.

In order to fulfill Federal Requirements in evaluating the implementation of effective security controls on computer systems, the product from Symantec Corporation called Enterprise Security Manager will be used.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required:

BITM Staff: The BITSM office will involve two personnel about 6 months full time in order to achieve full implementation.

Regional Security: The amount of time for a Regional Security Manager/Officer to assist in developing the standard policy will require about 40-60 hours of time. To review and develop an interpretive report for a large report on one computer is about 3 hours, on a clean system about 5 minutes.

System Administrator: It takes less than one hour of total time to prep and install an agent on a single computer system.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule:

Finish standard operating procedures by December 30, 2004
Finish testing of the product (test plan already developed) to be completed by January 15, 2004
Develop an interpretative report January 15, 2004
Conduct a formal risk assessment to be completed by January 1, 2004
Open up access to Systems Administrators by February 17, 2004
Develop/revisit the standard policy checks to be used in evaluating a computer system by ESM to be completed by March 1, 2004

Complete ESM implementation methodology by March 1, 2004
Deploy agent on outstanding computer systems (estimate is about 100 computers) by May 1, 2004
Integrate with the DOI Command Center by April 1, 2004

FY 04 Action and Tasks: During fiscal year 2003 three managers and 200 agent licenses were purchased. At this time of writing (November 19, 2003), 160 agents have been deployed on two managers. An additional manager is also operational that provides a test environment. To date we have used ESM in certifying and accrediting three major applications. During fiscal year 2004 we will:

Complete a system inventory in cooperation with the BITSM. This will get us a total count of systems to deploy agents on.
Finish testing of the product (test plan already developed)
Develop an interpretative report
Conduct a formal risk assessment
Finish standard operating procedures
Develop/revisit the standard policy checks to be used in evaluating a computer system by ESM
Open up access to Systems Administrators
Complete ESM implementation methodology
Deploy agent on outstanding computer systems (estimate is about 100 computers)
Integrate with the DOI Command Center

Project: IT Security Operations Team (ITSOT) - Consolidation of Public FTP Servers

Project Manager: Jessica Alvarez, Eastern Region GIO Office

Background:
In the summer of 2002, when a data call of public services revealed the USGS had over 300 distributed public ftp servers, it became apparent that the Bureau needed to initiate an effort to consolidate and centrally manage these services. This project intends to slow down further proliferation of public FTP servers and reduce the number of Internet facing servers by consolidating the majority of distributed ftp servers onto one solution that can be centrally managed. The goals of this project complement DOI's efforts to redesign the network and reduce the number POPs, both efforts that originate from the need to improve security.

Mandates/External Drivers (DOI Federal Regulations, Etc.):
As part of DOI's efforts to improve security of IT systems, on July 19, 2002, DOI mandated that anonymous ftp services be disabled at all Bureaus. A follow up memo sent on October 9, 2002, mandated that all ftp and web servers be located in DMZs and that points of presence to the Internet be reduced. To comply with these mandates the CTO's office is establishing centralized ftp services.

Level of Effort Required:
The level of effort to migrate existing ftp servers will vary for science centers based on the complexity of the local IT environment. Some sites may not be able to migrate if the sites utilize "home grown" applications that interact with the local ftp server or if adopting the Bureau FTP solution would reduce performance. The FTP team will attempt to accommodate the needs of each site by working with the sites on a case-by-case basis. After the migration instructions are finalized, the average site should be able to migrate to the Bureau FTP solution within a day. As a result of the USGS efforts to improve security, the number of ftp servers has been steadily declining from the original findings in 2002. It is estimated that approximately 200 sites will need to be migrated or set up to use the reverse ftp proxy.

Linkages & Dependencies to Other Projects:
To avoid duplication of effort and because the functions performed by these projects will prove beneficial to the ftp consolidation effort, the FTP team is maintaining linkages with the: Enterprise Web Infrastructure (NatWeb) Team, ITSOT's Firewall Team and Vulnerability Scanning Team.

Priority: To be determined by the CTO and RGIO staff.

Resources Required (Manpower, Equipment, Software, Etc.):
Two servers with Disk Arrays have been purchased. One will only be accessible to USGS hosts, the other will reside in one of the Bureau managed DMZs available for public interaction. A lead Linux administrator will be needed for approximately 1000 hours. Five hundred hours of a Windows and Solaris administrator will also be needed to assist with testing, development of procedures and migration. ITSOT members will serve as consultants to identify ftp servers, approve the design ideas, review project documentation and maintain the project's web page.

Estimated Project Cost and Probable Source of Funds:

- Labor Costs, $100K- Project Manager (600 hrs) from April 2003 to June 2004, Linux Administrator (1000 hrs) from Oct. 2003 to July 2003, Windows/Solaris administrator (500 hrs) from June 2003 to July 2004.
- Training Costs, $0
- Equipment Costs, $30K- Two servers and miscellaneous software licenses.
- Source of Funds- CTO Office

Benefit to USGS Mission: Improvement of the USGS's security posture, standardization of procedures used to exchange data with partners, overall reduction of servers within the USGS.

Schedule:
By the end of the third quarter, FY04, the number of publicly accessible anonymous ftp servers within the USGS should be drastically reduced. At this point, the project will end and ITSOT will continue to maintain and support servers until the CTO's office decides to assign this task to an alternate team.

FY 04 Action and Tasks:
The central ftp servers were purchased and configured during the fourth quarter of FY03. During the first quarter of FY04 the FTP Project will be initiating the migration of distributed ftp servers to the central servers, identifying sites whose business case does not allow them to migrate, and setting up a reverse proxy for sites who have a need to maintain their local ftp server. The effort to centralize ftp servers will reduce the number of publicly accessible servers and reduce the need for distributed DMZs within the USGS.

Project: IT Security Operations Team (ITSOT) – Vulnerability Scanning Team

Project Manager: Brian Schachte, Eastern Region GIO Office

Background:
The Department of Interior, Network Perimeter Security Standard, mandates that bureaus implement a network vulnerability testing process.

In response to this requirement the U.S. Geological Survey (USGS), Information Technology Security Operations Team (ITSOT), under the direction of Bureau Information Technology Security Manager (BITSM), will perform vulnerability assessments of local area networks on a monthly basis.

Mandates/External Drivers (DOI Federal Regulations, Etc.):
The following excerpt is from the DOI document:

Each bureau must create a network vulnerability testing process and a patch management process for hosts and devices that are exposed to the Internet. The same processes should be applied to internal bureau systems that have higher risk levels than typical workstations connected to the wide area network. (For example, law enforcement systems, financial systems, etc.)

Bureaus will conduct network vulnerability tests to ensure that Internet facing devices do not have exposed vulnerabilities. Systems must be routinely scanned with a vulnerability scanner such as Nessus. The SANS/FBI Top 20 list must be used as a base line for the tests. After significant improvement is made reducing these vulnerabilities, additional vulnerability tests must be added to the test procedures.

Internal network perimeters should also be tested. Scanning can be conducted from a central location in the bureau wide area network to simulate access of a typical workstation connected to the wide area network. The same general procedures for testing Internet facing devices can be used.

Testing must be done at least monthly and reports must be sent to the system administrators and BITSM for remediation. System administrators are responsible for the remediation any discovered vulnerabilities as soon as possible. The bureau's network assurance testing procedures must include the following at a minimum:

- Monthly vulnerability scans of Internet facing devices
- Notification to system administrators that the scans will occur
- Summary reports for the BITSM and system administrator including
    - IP address of device
    - Vulnerability discovered
    - Risk Level of Vulnerability
    - Status of vulnerability (recurring, new, etc.)
- Workflow to allow system administrators to track vulnerabilities and mark false positives
- Monthly report to the DITSM (Department IT Security Manager) showing vulnerability trends. The reports must use a consistent format to allow monthly comparisons of the network security posture.

In addition, on December 22, 2003, the DOI released a policy expanding the scope of vulnerability assessments to include internal, local area networks.

Additional External Mandates and Requirements

Federal Information Security Management Act (FISMA), Section 3544, Federal agency responsibilities, Paragraph 2, Subparagraph A states the head of each agency shall "ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems".

Department of the Interior **Departmental Manual, 375 DM 19, Section 19.9, Standards, Requirements and Procedures** requires each information technology system have a contingency plan based on current vulnerability assessments.

Vulnerability assessments are a required part of the Certification and Accreditation process as described in the **DOI Security Test and Evaluation (ST&E) Guide, Version 1.0.**

Responsibilities

Project management and assessments will be performed by, or under the direction of, the Regional Information Technology Security Mangers (RITSM). The assessments are designed to identify systems potentially vulnerable to the SANS Top 20 Internet Security Vulnerabilities. The ITSOT will be employing several assessment tools including ISS Network Scanner and Nessus. The scans attempt to gather information through normal and specially crafted requests to Internet services. No attempts to compromise, gain access or intentionally cause a denial of service to a system will be made. Since the SANS Top 20 is a dynamic list representing current threats scan policies will be reviewed and, if necessary, updated each month.

Reports, containing the following information, will be made available to the Security Points of Contact (SPOC).

- Summary of high, medium and low threat level vulnerabilities discovered
- Detailed summary of the vulnerability detected on each host
- Recommended corrective actions

To update policies, perform scans, produce and disseminate results, and report summary results to the BITSM requires a minimum of three employees and can range from 40-60 hours per month. As process become more automated the time requirements will decrease.

SPOCs will be responsible for distributing results to the appropriate system administrators and the oversight of corrective measures. At this time it is not necessary for the SPOCs to report actions taken or false-positives. Level of effort could range from 4-16 hours depending on the size and complexity of the local area network.

System Administrators will be responsible for implementing corrective actions. Level of effort could range from 1-40 hours depending on the number of systems and level of technical support for each local area network.

The BITSM will be responsible for compiling summary reports and submitting results to the DOI. The summary reports will contain the following information:

- Number of hosts in the wide area network

- Number of hosts with high risk vulnerabilities
- List of open ports with corresponding number of hosts (top 20 ports)
- Trend reports for each of the above items

Level of Effort Required: The level of effort required is dependent on the security practices of the respective science center. Science centers that have institutionalized IT security practices will have little additional work. Science centers with complex IT environments may have to devote a substantial amount of resources to remediate deficiencies. Science centers with deficient IT security practices will have to devote a substantial amount of resources to remediate deficiencies.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Labor	3 employees GS12 pay level 40-60 hours per month	$19,200-$28,800 annually
Training	3 employees	$6,000
Software Maintenance	ISS Internet Scanner 10,000 node license	$20,000 annually
Source of Funds	CTO account supporting Information Technology Security Operations Team program.	
Total		$45,200 - $54,800

Benefit to USGS Mission:
Performing regularly scheduled vulnerability assessments is an industry best practice for determining the Bureau's security posture and identifying vulnerabilities capable of impacting the confidentiality, availability and integrity of Bureau computing and data assets.

Schedule: Testing and preliminary scans were completed during the second quarter of FY04. Additional functionality to automate processes, implement control console and expand coverage will be performed during the third quarter of FY04.

FY 04 Action and Tasks: The project will continue to meet requirements mandated by Federal and Departmental mandates by performing regularly scheduled network and computer vulnerability assessments.

Project: Enterprise Web (Separation of Public and Private Content, Moving of Public Servers into DMZs, Reducing the number of publicly available Web servers using Reverse Proxy, Collocation of Content and Consolidation of Web Servers (NatWeb), and C&A of Web Servers)

Project Manager: Lorna Schmid, 703.648.6834
439 National Center Reston, VA
Internal Web Site: *http://natweb.usgs.gov*

Background:

Moving of Public Servers into DMZs

The USGS National Web Server System, or NatWeb, is a long-term managed Web hosting service provided to USGS Web server administrators as part of an effort that will reduce the number of publicly available Web servers and collocate content. Originally, funding was provided by three sources - GIO, Water, and ADT (Title VIII); this year funding will be from the GIO Office.

Migrating USGS content to this infrastructure is helping USGS reduce the number of public Web servers, reduce security related workload for content owners and reduce traffic on internal networks. NatWeb provides security at the highest level and data and information management at the lowest appropriate level. Migrating USGS content to this infrastructure is helping USGS reduce the number of public Web servers, reduce security related workload for content owners and reduce traffic on internal networks. Development of the NatWeb infrastructure was led by Water Resources to enhance delivery of real-time water data and to meet additional USGS Web content delivery needs through the GIO Office. Integration of the real-time water data including emergency backup processing and replicated Web hosting within the NatWeb infrastructure was completed September 30, 2003.

As of March 31, 2004, all public access to USGS Web information will need to be provided through a DMZ in order to meet DOI requirements. DOI has authorized USGS to maintain 4 long-term DMZ environments (Denver, Menlo Park, Reston, and Sioux Falls) any additional DMZs will require waivers by DOI. The NatWeb system is hosted from a DMZ environment and is in the final stages of C&A. Therefore, Web sites that are moved to the NatWeb system will meet C&A requirements because the original host system can be retired or repurposed.

Collocation of Content and Consolidation of Web Servers (NatWeb)

The collocation strategy that the GIO has embraced through the NatWeb project was established by the Gartner Group for use by large, distributed organizations that desire to optimize a distributed Web infrastructure. It includes the following four steps:

1. Collocate
2. Consolidate redundancies in content
3. Evaluate and develop a long term-strategy for managing and serving content; develop plan
4. Migrate

This collocation strategy is also in line with the Departmental directive to reduce the number of publicly available Web servers, to insure that all public access is to servers located in DMZs and with the newly reformed DOI Web Council's activities related to evaluating and improving the DOI Web presence.

Reverse Proxy
The NatWeb team is coordinating with the Bureau IT Security Operations Team (ITSOT) on a strategy of using reverse proxy to further reduce the number of publicly available Web servers. This strategy will allow USGS to focus the C&A effort for 2004 on those publicly available systems not using reverse proxy and on developing a plan for obtaining C&A for all those systems behind the firewall by 2005.

In December the NatWeb system activated its first reverse proxy service for the *Nonindigenous Aquatic Species* Web site. The NatWeb team is coordinating with the Bureau IT Security Operations Team (ITSOT) on a strategy of using reverse proxy to further reduce the number of publicly available Web servers. Additionally, we are working with the GIO Enterprise GIS Program and have tested reverse proxy of Arc-IMS sites and anticipate activation of Arc-IMS sites to begin soon.

What is reverse proxy?
A Google search provides the following Web definition: "A proxy server that appears to the client as if it is an origin server. This is useful to hide the real origin server from the client for security reasons." Using the NatWeb systems we can reverse proxy information hosted on systems running inside our firewalls and close off public access to those systems. Although this does not remove the long-term requirement for C&A of those systems, it should allow USGS to remove those systems from the high priority list requiring C&A by July 2004.

Separation of Public and Private Content
Finally, there is a requirement to separate public and private content on publicly available servers. The NIST Special Publication 800-44 Guidelines on Securing Public Web Servers Section 6 (page 38) identifies content that should never be stored on a publicly available server even if there are logical access controls set. Additionally, Section 6.4 contains a "Securing Web Content Checklist." This information will be used to develop a strategy to comply with this requirement.

<u>Mandates/External Drivers (DOI Federal Regulations, Etc.):</u>

Federal Information Security Management Act (FISMA)

OMB Circular A-130

DOI IT Security Instructional Memorandums and Bulletins
http://internal.usgs.gov/gio/security/doi_instructional_memos.html

Network Hardening
DOI Network Perimeter Security Standard
USGS Network Perimeter Security Standard based on the DOI Network Security Standard

NIST Guideline 800-44 Guidelines on Security Public Web Servers
http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf

USGS Network Perimeter Security Matrix (Dec 8, 2003)

Office of Management and Budget Circular A-130, “Management of Federal Information Resources”, Appendix III, “Security of Federal Automated Information Resources.”	Establishes a minimum set of controls to be included in Federal IT security programs.
Computer Security Act of 1987	This statute set the stage for protecting systems by codifying the requirement for Government-wide IT security planning and training.
Paperwork Reduction Act of 1995	The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996	This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and recodified the Computer Security Act of 1987.
Presidential Decision Directive 63, “Protecting America’s Critical Infrastructures.”	This directive specifies agency responsibilities for protecting the nation’s infrastructure; assessing vulnerabilities of public and private sectors; and eliminating vulnerabilities.
Presidential Decision Directive 67, “Enduring Constitutional Government and Continuity of Government.”	Relates to ensuring constitutional government, continuity of operations (COOP) planning, and continuity of government (COG) operations
OMB Memorandum 99-05, Instructions on Complying with President's memorandum of May 14, 1998, “Privacy and Personal Information in Federal Records.”	This memorandum provides instructions to agencies on how to comply with the President's Memorandum of May 14, 1998 on "Privacy and Personal Information in Federal Records."
OMB Memorandum 99-18, “Privacy Policies on Federal Web Sites.”	This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so.
OMB Memorandum 00-13, “Privacy Policies and Data Collection on Federal Web Sites.”	The purpose of this memorandum is a reminder that each agency is required by law and policy to establish clear privacy policies for its Web activities and to comply with those policies.
General Accounting Office “Federal Information System Control Audit Manual” (FISCAM)**.**	The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
NIST Special Publication 800-14, “Generally Accepted Principles and Practices for Security Information Technology Systems.”	This publication guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.
NIST Special Publication 800-18, “Guide for Developing Security Plans for Information Technology Systems.”	This publication details the specific controls that should be documented in a security plan.
Federal Information Processing Standards**.**	This document contains legislative and executive mandates for improving the utilization and management of computers and IT systems in the Federal Government.

Level of Effort Required:

Web site administrators and content providers in the USGS need to comply with the DOI directive that all publicly accessible systems to be moved into DMZs is March 31, 2003. All science centers are expected to comply with the directives outlined by that date. The NatWeb system provides USGS cost centers with a Bureau supported infrastructure to meet these requirements by migrating content into the NatWeb system using the Migration Procedures found at http://natweb.usgs.gov/migration/ or for those sites serving content not compatible with the NatWeb infrastructure implementation of reverse proxy through the NatWeb system. It is

not recommended that multiple reverse proxy systems be established to reduce the number of servers that have to be managed to securely provide this service. The reverse proxy service will allow USGS to continue to serve Web content to the public while the proxied servers will be behind firewalls and not directly accessible to the public.

Compared to the level of effort required to obtain C&A using NatWeb and Reverse Proxy is minimal.

Linkages & Dependencies to Other Projects:
The Project Manager has been assigned as a CTO Liason to the Enterprise Web Program and will be coordinating on the described tasks.

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

- Labor Costs
- Training Costs
- Equipment Costs
- Source of Funds

Description	FY 04 Amount (in thousands) (FY03 in parenthesis)	
Salaries	n/a	
Awards	6.2	(2.9)
Travel	24.0	(34.5)
FedEx & Shipping	0.6	(0.6)
Communications	4.7	(3.8)
Training	8.0	(3.5)
Contractual Services	327.5	(260.0)
System Maintenance		
Module support		
Contractor support		
Monitoring costs		
Software recovery		
Nat'l Center (mail – personnel)		
Equipment Procurements	255.0	(381.0)
Total	626.0	(683.4)

Source of Funds:
Good Question… ;-)

Hedy said that EWeb would fund NatWeb this year to the same level as last minus salaries, that would be $122K. I have made that request in budget discussions.
I have ~$110K remaining of Title VIII which is slated for the backups for NatWeb (included in request above). We were waiting for the DOI contract to come through to finalize that procurement.

Benefit to USGS Mission:

- Meets IT Security requirements. OMB Certification and Accreditation was expected by the end of FY03 and is waiting on the required Security, Testing & Evaluation process by the BITSM office; it is anticipated that this will be complete by the end of the second quarter. All documentation is complete and the system is working under an Interim Authority to Operate.
- Meets contingency requirements for data access through a replicated and geographically distributed system located at the high bandwidth Internet access points.
- Content can be managed from anywhere using locally available content management tools. This is due to NatWeb's use of a sophisticated, platform independent enterprise file system.
- Continual monitoring and notification of NatWeb performance and health.
- Cumulative or single site usage statistics detailing access to USGS Web sites and information are automatically generated.
- Faster access to USGS Web pages and files.
- Reduced internal network load since public traffic stops at the Internet gateways.

Schedule:

- NatWeb operations and migrations of virtual hosts into the system are ongoing.
- System performance monitoring for early identification and mitigation of potential bottlenecks or performance issues is ongoing. This includes internal monitoring and notification and external monitoring by Keynote Systems, Inc. (Details available on the NatWeb Web site)
- OMB Certification and Accreditation was expected by the end of FY03 and is waiting on the required Security, Testing & Evaluation process by the BITSM office; it is anticipated that this will be complete by the end of the second quarter.

FY 04 Action and Tasks:

1. NatWeb operations
    a. DD technology replacement
        i. Technology review in process with the assistance of the Network Services Support team (Rob Weitzel and Max Hechter), including:
            1. F5
            2. CISCO technology
            3. Akamai First Point
    b. Develop formal service level agreements
    c. Continue improvement of procedures for operation and administration of the *www.usgs.gov* system. This includes documenting procedures.
    d. Reverse Proxy implementation.
        i. Continue work with the ITSOT including additional prototype activity with reverse proxy through the NatWeb systems.
        ii. January 2004 conduct test of NetContinuum technology in Menlo Park, CA. If successful these boxes provide reverse proxy service and additional security enhancements that would allow USGS to place all Web servers inside network firewalls and remove them from public access.
        iii. Systems being served by reverse proxy are no longer publicly available and can reside behind the USGS firewalls.
        iv. Following testing and coordination with ITSOT and Enterprise GIS Program staff reverse proxy is running for one host currently with anticipated activation of Arc-IMS sites soon.

v. This implementation and others will be monitored for performance.

e. Upgrade the usage statistics log analysis server (natalog.er.usgs.gov).
    i. This server process all the usage statistics and generates Web access to the data for each individual virtual host and also a Consolidated statistical analysis which shows cumulative access.
    ii. With the implementation of reverse proxy this server will be even more busy since cumulative usage statistics will become available for all proxied sites.
f. Implement consistent backup strategy at all NatWeb modules
    i. Currently backup files are transferred across the network to a single module and backed up there. This is an inefficient procedure that needs to be rectified.

2. Continued Migration of Virtual Hosts into the NatWeb system using the migration instructions from the NatWeb site.
3. Evaluate expanding NatWeb functionality to support additional Internet applications such as Oracle Arc-IMS, Microsoft IIS, etc.
    a. Establishment of a technical advisory group would enhance NatWeb operations and level of service for USGS customers.
    b. The technical advisory group, which would include Internet application experts and NatWeb user's, could formalize requirements for additional services and potentially serve on working groups to develop strategies and solutions as deemed appropriate by the CTO and the GIOLT.
4. Coordinate with E-Web Program on Certification and Accreditation
    a. Finalize NatWeb C&A
    b. Co-develop strategy for non-NatWeb hosts (this strategy will take into account reverse proxy service)
5. Develop Working Capital Fund plan

Project: Narrowband Radio Transition

Project Manager: Skip Dutrow, Office of CTO/TIU

Background: In 1994 Congress passed legislation mandating a 10 year transition starting on Jan 1, 1995 of radio equipment within the Government radio spectrum band of 162Mhz to 173Mhz (VHF), and the 406Mhz to 420Mhz Band (UHF), to reduce or narrowband, channel bandwidth from 25Khz b to 12.5Khz to make available more radio spectrum for Government use. Mandated completion for VHF target date is Jan 1, 2005. Although UHF is mandated to be complete by Jan 1, 2008 UHF narrowband radios are available, and with the small quantity USGS has in inventory, UHF had been included to be completed with the transition target for VHF. With advancements in digital radio technology, and the enhanced capabilities digital offers, DOI has mandated that all of the replacement handheld, mobile, aircraft and repeater radios will be digital.

Mandates/External Drivers (DOI Federal Regulations, Etc.):
The National Telecommunications and Information Administration (NTIA) narrowband mandate requires all federal agencies operating LMR wireless systems be more efficient with their spectrum resources by using narrower channel widths. Specifically, Public Law 102-538, the NTIA Organization Act of 1992, requires NTIA to promote spectrum-efficient and cost-effective use of radio spectrum (Title 47, U.S.C. 903 [d][1]). A progress report was sent to the Congress in 1995 that identified several specific actions to enhance spectrum efficiency, including the requirements known as the "narrowband mandate", to convert federal LMR systems operation in the VHF and UHF bands from wideband 25 kilohertz (kHz) channel bandwidth to narrowband 12.5 kHz bandwidth systems. The NTIA's Manual of Regulations regulates Federal Government spectrum use for Federal Radio Frequency Management (Section 4.3.7a), which establishes the following timelines:

-All federal agencies operating LMR systems in the very high frequency (VHF) band (162-174 megahertz [MHz]) must convert by January 1, 2005.
-All federal agencies operating LMR systems in the ultra high frequency (UHF) band (406.1-420 MHz) bands must convert by January 1, 2008.

DOI Departmental Bulletin, IRM BULLETIN NO. 1996-003, signed: March 4, 1996, mandated that all DOI Bureaus will use the APCO25 standards for narrowband radios and that all narrowband radios will use digital technology.

Level of Effort Required: The level of effort is high. The average office will require 1 to 3 days to review inventory, place requisitions and replace the affected equipment when received. All USGS Disciplines are involved. The affected radio spectrum impacts almost entirely all of the radios used for the protection of the public, property, USGS personnel, and USGS mission operations. Replacement of radios is a one for one replacement of the affected current radio inventory. Replaced wideband radios cannot be surplused and must be destroyed.

Discipline Radio Officers:

Geography (NMD)	Alan Davidson	703-648-4686
Biological Resources (BRD)	Wayne Wiltz	337-266-8687
Geology (GD)	Robert McClearn	650-329-4716
Water Resources (WRD)	Paul Tippett	228-688-1565

Linkages & Dependencies to Other Projects: None.

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):
Principal manpower resources require the five discipline radio officers located in Menlo Park, CA; Bay St Louis, LA; Lafayette, LA; and Reston, VA. FTE Services would be necessary for approximately 60 working days each, intermittent during the calendar year, or until completion of the project. Discipline centers and field offices resources are estimated to require 1-3 days each of an FTE. Approximately 160 offices are involved.

Equipment required will be purchased off an existing DOI/BLM contract mandated by DOI to use for all purchases of handheld, mobile and repeater radios. Custom radios not available off the BLM contract will be purchased through GSA schedule contracts.

No software is required for this project.

Estimated Project Cost and Probable Source of Funds:

Labor Costs:
Discipline Radio Officers

Government FTE	5 employees	60 day duration	$100K Salary

Field Offices Personnel, Approximately 160 Offices

Government FTE	160	1 to 3 Days	$50K Salary

Training Costs: None

Equipment Costs:
The total estimated costs to replace existing radios with Narrowband Digital Radios are $6.1M.

Source of Funds:
Funding from 1996 to 2002, in the amount of $0.6M, was from Discipline Projects Funding.

Funding for 2003, in the amount of $1.5M, was from Discipline Capital Funds.

Funding for 2004, in the amount of $3.9M, is from requested and approved additional budget funding, also known as a pass back, specifically for the narrowband project.

Benefit to USGS Mission: Meets mandate as required by Public Law 102-538. Meets the NTIA's timelines for implementing narrowbanding as stated in the Manual of Regulations, which regulates Federal Government spectrum use for Federal Radio Frequency Management (Section 4.3.7a).

Schedule: Completion of project is targeted for the end of this calendar year Dec31, 2004.

FY 04 Action and Tasks: Project to date is currently about 30% complete. Working with the USGS disciplines, radio officers and management, the remaining radios to be transitioned have been targeted for completion by end of 2004. All affected equipment has been identified through inventory checks. What remains is for the responsible offices and centers to place requisitions through their discipline radio officers for the equipment to be replaced, forwarded to Reston HQ's for compilation and processing, equipment totals forwarded to BLM for negotiation of discounts and placement of the orders with vendors by contracts when negotiated vendor

discounts are complete. New narrowband radios are delivered from the vendors directly to the offices having the affected equipment.

Project: Windows Technical Support (formally NT TAC)

Project Manager: Garry Neverdon (http://nttac.usgs.gov)

Background: The New Technologies Technical Advisory Committee (NT TAC) was established to provide continued and future testing and development of new technologies in Windows computer systems. NT TAC provides technical support and resources for well-integrated, secure, and stable deployment of new Windows technology computing systems within a mixed USGS computing environment.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: Remote office effort required for this project would include following the standards provided by the "Windows Technical Support Team" for maintenance, management and configuration of Windows operating systems.

Linkages & Dependencies to Other Projects: N/A

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Required Human Resources: 10 members - Six (6) members would be from WRD.

Labor Costs - Field Support Re-allocations (includes limited COTS support)	$120,000
Awards	$ 10,000
Travel	$ 50,000
Training Costs	$ 50,000
Equipment Costs - Shipping	$ 2,000
HW/SW Purchase	$ 50,000
Communications	$ 2,000
Total Cost	$284,000

Source of Funds – CTO/CI

Benefit to USGS Mission:

- Provide configuration standards for Microsoft Windows operating systems and associated applications.
- High level of Windows technical support via email.

Schedule: NT TAC is currently operational and this project is an ongoing effort to insure Windows operating systems are supported and conform to a standard configuration, which includes security settings. Project plan is underway to rename and restructure the group with other discipline members under the new name "Windows Technical Support Team".

FY 04 Action and Tasks: During FY04, the CTO will reorganize NT TAC by expanding the group to include multi-discipline members and increase the level of support to manage Windows operating systems for the bureau, as well as, rename the group "Windows Technical Support Team". The new Windows Technical Support Team will follow NIST and DOI standards for configuring and securing Windows operating systems.

This group will change from a committee giving advice to a Team that will create standards and procedures for Windows operating systems, which would:

- Verify and test operating systems and all discipline applications/databases identified by each discipline as mission essential on every supported platform, which is currently Windows 2000 and Windows XP.
- Provide technical support and direction for secure, standardized deployment of all new Windows technology computing systems and associated software within a mixed USGS computing environment.
- Provide technical support and direction for PC and server software installation and management (Windows 2000 and 2003) tasks or applications (IIS, MS Office, SUS, MOM, SMS, etc.).
- Standardize desktop, laptop and server security settings as identified by NIST, BITSM and DOI, as well as, overall security for associated applications.
- Provide backup solutions for small office environments and individual systems with tools such as Ultrabac.

Project: Certification and Accreditation (C&A)

Project Manager: Maryjon McAvery

Background: Ensure A-130 compliance for the CTO computing infrastructure, achieving and maintaining certification and accreditation of bureau-wide computing infrastructure. Develop and maintain foundational documents related to the computing infrastructure, including security plans, risk analyses, asset valuation, Interim Authority To Operate (IATO) and Plan Of Action and Milestones (POAM) status reports, and disaster recovery/continuity of operations plans.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: Offices will be required to provide information associated with identified CTO computing infrastructure, which will include ALL general purpose, nonscientific computing components. Several days may be required to address all of the required Office information.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: This project will be on-going in order to provide infrastructure reporting on the status of the USGS computing infrastructure, as it applies to the actions above, to DOI and the Office of Management and Budget.

FY 04 Action and Tasks: This project will insure that the CTO computing infrastructure meets A-130 compliance. The following actions are required:

- Asset inventory
- Asset Valuation
- Risk Assessment
- Business Impact Assessment
- Security Plan
- Disaster/Contingency Plan
- Management Control Review
- Security, Test and Evaluation
- Certification and Accreditation

Project: Enterprise Software Support Clearinghouse

Project Manager: Tom Wood/Paul Exter

Background: A USGS Enterprise Software Support (ESS) team will provide cost-effective computing applications and a single point of contact for USGS sponsored software that meets the needs of administration and science. The software support program will provide services in two major areas:

1. Point of contact for enterprise software licenses, cost recovery, configuration management, distribution, and training, etc.
2. Virtual user help desk for enterprise software support.

Mandates/External Drivers (DOI Federal Regulations, Etc.): DOI software contracts

Level of Effort Required: System administrators throughout USGS will interact with the software support program once it is functional. SAs will be expected to install new releases of software for their users and to keep track of and report on licensing usage in their area of responsibility. SAs will be called upon in some cases to assist in testing software installations.

Linkages & Dependencies to Other Projects: The virtual help desk is directly linked to the USGS Help Desk system project.

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.): The activities of the software support clearinghouse will use existing budgeted resources of the ITO staff as well as limited Windows TAC and field software support personnel.

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission: The benefit of this project is primarily the cost savings associated with centralized support management (licensing, configuration management, simplified install instructions for the field SAs, etc.), as well as the benefit of assisting USGS scientists and support personnel with using the software most effectively.

Schedule: Discussions are underway. Implementation is expected by 2nd-3rd quarter of FY04.

FY 04 Action: The FY 04 activity will focus on developing a strategy for providing the suite of services in the two major areas, and implementing the strategy. The suite of services will include:

- Provide a "virtual" help desk for all questions related to software acquisition, usage, installation, etc., in conjunction with the USGS Help Desk.
- Configuration management of software in conjunction with Windows TAC.
- Software distribution management.
- Software Cost Recovery management.
- Software training information clearinghouse.
- Determine, with collaboration, software that should be acquired on a bureau level.

- Coordinate bureau purchases with DOI and other bureaus.
- Provide a single point of contact for license information and software inventory.

Project: Enterprise Network Services (ESN) Design and Implementation

Project Manager: Elaine Stout, OIT/Telecom Infrastructure, Web Site: internal tracking of all major TIU projects at:

Background: The Department of Interior has committed to a "single network" -- the Enterprise Network Service [ESN] – to be used by all DOI bureaus and which will complement or replace individual bureau network backbones and drastically decrease the number of Internet connection points throughout DOI. The deployment of the ESN, Phase One for FY04 have been cited as 1) DOI Intranet (replacement for the current VPX), 2) reduction from 33 to 3 ISP services, 3) DOI managed Network Operations and Security Center. The deployment of the Department Internet access is planned for 3rd quarter CY 04, and since USGS has the most complex network infrastructure, USGS has been asked to assist the Department CIO with planning, model deployment and design, and deploying the ESN assisting the Department CIO for planning, and perhaps reuse of existing facilities. Two major meetings involving USGS senior technical staff and DOI senior technical and program management staff have occurred in FY04.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: In July 2003, the primary USGS ESN Design team was selected; these individuals, several from the field, are the key network technical staff at USGS. If USGS becomes the technical-arm for DOI (as was discussed at the 11/19-20/2003 meetings), staffing will stretched even more severely than currently. Resources are even further constrained with network staff moving to other areas. With the ESN, the bureau will need to maintain its existing infrastructure while transitioning to a new infrastructure. At minimum, two highly technical network FTE or contractors our required to facilitate the support for the Department and the transition.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: Decisions on what and how-much of the USGS network infrastructure could (and should) be reused in the ESN. This decision needs to be made no later than late January 2004.

FY 04 Action and Tasks: During FY04, the Department is committed to ordering and installing very-high speed Internet access at 3 or 4 locations. Over time, bureaus will connect to these locations and then drop their existing bureau service. Discussions indicate that NPS, NBC and OSec to connect in FY04. The USGS needs to decide if it should make its current Sprint service as part of a possible "reuse" in conjunction with other existing UUNet service. In late-January 2004, a major ESN meeting will be held in Washington to discuss the ESN model, the planned funding, and deployment schedule for VPX replacement and Internet access.

Project: Enterprise Remote-Access VPN Service

Project Manager: Rob Weitzel, Telecommunications Specialist OIT/Telecommunications Infrastructure Unit Reston, Va. Phone (V) (703) 648-7013 (email) *mailto:rweitzel@usgs.gov*

Background:

Over the past several years the USGS has been running several adhoc VPN & remote-access services including the defunct Cisco AS5200 services, the AT&T managed remote-access and VPN services with portals in both Menlo Park and Reston, and most recently the Cisco based 5000 VPN concentrators deployed in Menlo Park, Reston, Denver, Sioux Falls, Anchorage, and the Cisco 3005 concentrators deployed in Flagstaff and Menlo Park.

There are several drivers forcing the USGS to re-evaluate new VPN technologies. The first driver is Cisco's support for the current 5000 VPN concentrator deployment. On February 24, 2002 Cisco announced the EOS or end-of-sale for the 5000 series concentrators and associated client software. The EOS means Cisco will not support further feature development for the 5000 concentrators. Cisco is advising their clients to invest future VPN monies towards product solutions that provide more robust feature sets and support including the Cisco 7200 series routers, modules for the 65XX series switches, and the Cisco 3000 series concentrators. The second driver is security. Security is a high profile driver that is forcing many programs to act. VPN services allow authorized users access to the USGS intranet resources. Consolidation of VPN access helps isolate access into the USGS network and mitigate security risks posed by such access rights. Developing a centrally managed enterprise while working hand in hand with the BITSM & ITSOT to ensure policy is met can attain mitigation of security risks. The last driver is both a money and resource issue. The USGS currently has limited resources to design, deploy, and manage day-to-day enterprise services. To date the majority of enterprise resources were procured and deployed using local funding despite several attempts to obtain enterprise funding via the GIOLT.

The USGS would like to initiate a fact-finding mission to determine the VPN requirements for VPN access to USGS intranet resources. The end product would be a consolidated VPN service, which supports USGS intranet access for employees and other authorized users. This product will meet all departmental and bureau security mandates by reducing the number of entry points into the USGS internal infrastructure. A determination will also be made on whether the services will be supported by the USGS, contractor managed, or possibly a hybrid of both USGS employees, and contractors.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Timeline

Last Software Releases

The final Cisco VPN 5000 Series feature release for enterprise organizations will be v5.2.23. The final feature release for service providers will be v6.0.21. Both final software releases will be available in March 2002. The final Cisco VPN 5000 Client feature release will be v5.2, also available in March 2002. The final client release will include the following client platforms: Windows 95/98/Me, Windows NT, Windows 2000/XP, Mac OS 8 and 9, Mac OS X (3DES only), Linux (Kernel 2.2.x and 2.4.x only), SPARC Solaris 32/64 bit, and Intel Solaris. Cisco will continue to offer patch and maintenance releases as necessary. No new feature enhancement requests for the final releases will be addressed.
Support of Hardware and Software

Cisco will provide maintenance support to customers who have existing service contracts with Cisco in accordance with the dates specified in Table 1 below.

Table 1: Key Dates

Milestone	Effective Date
End of hardware maintenance (engineering)	February 19, 2002
End-of-sales announcement	February 25, 2002
Last day to order product	August 26, 2002
Last day of trade-in program	August 26, 2002
End of production	October 28, 2002
Discontinue contract renewal	August 26, 2004
End of software maintenance (engineering)	August 26, 2005
End of software support	August 26, 2005
End of support and product obsolescence	August 27, 2007

Level of Effort Required:

This will be a phased project. The first phase would be to implement a replacement platform for the existing deployment. This will involve requirements analysis, and may require a data call to acquire those requirements. There are pending BITSM policy on VPN services. An initial deployment might require specified sites to install & house VPN related equipment. VPN clients would potentially be forced to change their procedures & processes and software to adapt to any new VPN service.

Linkages & Dependencies to Other Projects: There may possibly be links to ESN as DOI is looking into the feasibility of integrating VPN services via the ESN.

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.): TBD

Estimated Project Cost and Probable Source of Funds:

- Labor Costs - TBD
- Training Costs - TBD
- Equipment Costs - TBD
- Source of Funds - TBD

Benefit to USGS Mission:

- To provide an enterprise level VPN service to allow USGS employees, contractors and collaborators selected access to authorized USGS resources.
- To adhere to both departmental & bureau security mandates
- To reduce the number of backdoor entry portals into USGS resources thus mitigating potential data loss, theft, loss of time and money associated with improperly managed VPN systems.
- To consolidate VPN services and make better use of USGS resources and money

- To provide a higher level of service & functionality

Schedule:

Including but not limited to the following:

PHASE ONE: Preliminary study (Proposal) & gathering of requirements

PHASE TWO: Conceptual Design (Planning)

PHASE THREE: Detailed Design (Management)

PHASE FOUR: Implement VPN Services (Closeout)

FY 04 Action and Tasks:

Goals for FY 04 include, but are not limited to;

- Requirements analysis & proposal
- Conceptual design & prototype/proof of concept
- Detail design/migration & management strategy
- Implementation

PROJECTS TO BE AWARE OF

Project: Information Technology Office (ITO) Communications

Project Manager: Terry Reinitz

Background: The ITO Communications Project is a long-term effort to manage internal and external communications in a manner consistent with GIO Communications processes. The Information Technology Office (ITO), operating under the Chief Technology Officer (CTO), supports the management of information technology networks and systems in telecommunications, computing, and enterprise application management. The office supports information technology operations across the USGS and works closely with the Department of the Interior's Office of the Chief Information Officer.

Within the Office's purview are the following:

- Development and implementation of policies for computing services;
- Bureau-wide planning and management related to standards for hardware and software, operating systems policies, licensing agreements registration, directory services integration and domain name services, desktop computers, personal digital assistance units, and wireless technology;
- Bureau-wide management, planning, budgeting, implementation, and operation of telecommunications (voice, video and data); and
- Deployment, operation, and maintenance of an infrastructure that supports improved communication, collaboration, and information sharing across the bureau, focused primarily on bureau-wide management of Lotus Notes.

The ITO office is evolving from the consolidation of a number of work functions and employees geographically dispersed across the multi-disciplines of the USGS. Since the backgrounds of the programs and employees are so diverse and cut across the organization, it is necessary for the ITO to develop a customer focused, common communication strategy both internal and external to the organization.

The ITO recognizes the importance of effective communications in achieving our objectives and increasing understanding and interest in our work. Our strategy is intended to ensure that effective communication methods are in place to clearly and effectively communicate the CTO's message to USGS employees and customers. The USGS is a fast moving, diverse and evolving organization and requires systems to support communications that are quick, simple, reliable and effective. The ITO's office is about change, and communication is a critical link to navigating these changes.

Mandates/External Drivers (DOI Federal Regulations, Etc.): None

Level of Effort Required: Office effort is not required for this project. Offices will benefit from improved communication from the ITO.

Linkages & Dependencies to Other Projects: N/A

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission: Regional GIO staff, USGS System Administrators (SAs), and employees will have an increased awareness of CTO and its activities. Communications will be improved between the CTO and those with whom it has contact. Information on CTO services and events will be easier to find, thus creating an informed staff.

Schedule: The ITO Web page will be drafted in the 2nd quarter of FY04, and the first Information Update will be sent to Regional GIO staff and USGS SAs.

FY 04 Action and Tasks: The resulting strategy from this program will identify processes and procedures for all ITO communication efforts, such as data calls, web presence, routine email updates, bulletin board postings, etc. During FY04, information will be gathered from CTO managers on the process currently used for disseminating information to Information Technology (IT) System Administrators and users, and recommendations will be developed on how to improve this communication process. For example,

5. GIO email distribution lists will be reviewed, renamed using a consistent format, and include local groups that roll up into higher groups.
6. An OIT web page will be created for CTO staff and others
    - To publicize what ITO does and the benefit to the Bureau
    - To promote the use of collaborative available communication tools such as Lotus Sametime and QuickPlace, Team Rooms, etc.
    - To communicate internal office policies on calendar, voicemail, out of office, coverage (flexiplace), purchasing mechanisms and priorities, etc.
    - To share procedures and information on topics such as performance appraisals, rewards, field funding (matrix), Service Level Agreements, Bureau standards and guidelines, i.e. wireless policy
7. The team will identify opportunities to get and give customer feedback.

Project: IT Security Operations Team (ITSOT) - Communications Team

Project Manager: Jeff Brody, Western Region GIO Office

Background: Because of the diversity of organizational issues and technical complexity of systems & networks, a communication system is an important component of the team. Documented guidelines and methods of communication are needed to achieve a consistent and efficient flow of work and information.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

The guidelines identify these levels, the types of communications, and provide a walkthrough of the communication process, highlighting the responsibilities of the ITSOT, key topics of communication, and the appropriate method to interface with other groups.

In addition, the ITSOT Communications team will maintain a website as a central source of information on security techniques, Bureau IT security operations, and the activities of the ITSOT. The Web site also will be a portal to Web-applications developed by the ITSOT.

Level of Effort Required: Policies and guidelines exist and require occasional revision. Website content is dynamic and should be maintained regularly. It is estimated that an ITSOT member should spend 4-6 hours per week maintaining the website. This effort is internal to the ITSOT and should require no effort from the science centers.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: Website development and administration is an ongoing task. Policy and guideline documentation is reviewed and updated on a periodic basis.

FY 04 Action and Tasks: During FY04, the ITSOT Communications team will continue providing guidance, consisting of written policies, standards, technical and procedural controls for communicating with various groups and levels of the organization.

Project: IT Security Operations Team (ITSOT) – Intrusion Detection System Team

Project Manager: Tom Van Dreser, Central Region GIO Office

Background: The goal of the ITSOT intrusion detection system (IDS) team is to detect and respond to suspicious network traffic. To accomplish this goal, Intrusion Detection technology will be deployed throughout the USGS network and configured to detect, correlate, and react to, in near real time, anomalous and suspicious network traffic across the USGS WAN and LANS.

The configuration and administration of Intrusion Detection systems will be centralized under the USGS CTO with guidance and concurrence from the Bureau IT Security Manager. The ITSOT IDS team will manage the IDS in accordance with the DOI Perimeter Security plan. This activity is critical to improving the security posture of the organization.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: This effort is internal to the ITSOT and should require no effort from the science centers. For successful implementation the ISTOT will need assistance from members of the Geonet team to ensure proper placement of the IDS sensors at the WAN gateways. Depending on the proposed location for IDS sensors, additional network hubs might need to be procured.
After initial configuration and deployment of the sensors and console, the level of effort required to maintain the system will low to minimal. However it will be essential that there be staff available to review the logs in near real time and be able to respond to alerts generated by the IDS in a timely manner. The response support may require a substantial level of effort and time when severe incidents are detected.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: The four initial servers have been procured and the operating systems installed. The IDS and database software need to be installed and configured. Final location for the IDS sensors needs to be discussed and coordinated with the GeoNet team. Testing of the IDS sensors and console needs to be completed prior to deployment and the configuration refined afterward deployment. Deployment of the servers will be completed by the end of February 2004.

FY 04 Action and Tasks: During FY04, documentation for standards and procedures for the IDS administration will be developed leveraging the experience gained from operating the Denver Federal Center IDS. After the documentation is drafted, all ITSOT IDS team members will review it, and then it will be shared with the other ITSOT members for review.

Initially three servers will be configured as sensors and an additional server will be configured as the IDS console. The sensors will be deployed near the edges of the USGS Internet perimeter. Later additional IDS will be procured and deployed at points within the USGS WAN.

Project: IT Security Operations Team (ITSOT) - Systems Support Project

Project Manager: Dave Bergstedt, IT Security Operations Team

Background: The Bureau's Information Technology Security Operations Team (ITSOT) is building an IT infrastructure needed to support the duties assigned to the team. This project was created to identify, acquire, and configure computer system platforms, and to build or acquire the necessary tools for these platforms to be used by other ITSOT projects and program tasks.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: On-going system administration resources are critical to sustain the systems and services needed to support the ITSOT operations. A minimum of three qualified full-time system administrators should be allocated to provide adequate support. This effort is internal to the ITSOT and should require no effort from the science centers.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: Currently, deployment and utilization of ITSOT systems is being implemented in a "best effort" mode, until formal commitments are made to ITSOT staffing. The servers are needed immediately, but a lack of resources is slowing the deployment.

FY 04 Action and Tasks: During FY04, eighteen computer servers will continue to be deployed and utilized for various ITSOT operational needs. Specifically, the ITSOT needs servers to manage and monitor USGS firewalls, servers to perform vulnerability assessment scanning, servers to act as intrusion detection sensors and monitors, and servers for web and database applications that collect, store, and serve relevant ITSOT operations data.

Project: Implement Reston IT Call Center

Project Manager: Faye Lee/Kip McCarty/Terry Sutton

Background: A USGS IT Help Desk System will be established as a single point of contact for all IT customer support. The "System" will encompass some hardware and software, but primarily the IT support people across the bureau who will be formally linked together through organizational and matrix relationships to provide consistent help desk and desktop support services. Three "Call Centers" will be established: one in each Region to provide extended time zone coverage. Call Centers will be linked through a call center software suite and will be staffed with a small group of IT generalists for first contact with customers. The Call Centers will have direct links to designated IT support organizations across the bureau and will be primarily responsible for call resolution, call tracking, and customer satisfaction. Eventually all field offices will be expected to use the call centers for IT support.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: "Field" offices within the Powell Building will be expected to use the call center for IT support once it is operational.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: Planning for the Reston Call Center is underway. Initial operation by 2nd- 3rd Quarter FY 04.

FY 04 Action and Tasks: The Reston IT Call Center project is a short-term effort (during FY04) to establish an IT Call Center in Reston to serve as a pilot for the USGS IT Help Desk System. Authority for this project is through Karen Siderelis' 9/24/03 Memorandum, signed by the Director on 10/3/03, subject: "Organizational Strategy for Bureau Information Technology Infrastructure".

Project: Reston Office Automation Technical Support

Project Manager: Faye Lee/Tom Wood

Background: National Center office automation technical support functions and personnel will be consolidated as part of the Help Desk reorganization. The Office Automation Technical Support unit will provide office automation server and desktop support for staff at the National Center and will implement Active Directory in Reston.

Mandates/External Drivers (DOI Federal Regulations, Etc.):

Level of Effort Required: "Field" offices within the Powell Building will be expected to transfer their OA support staff and contractors to the consolidated unit. That process is underway. Once the consolidation is complete, efficiencies will be realized and new value-add resources will be made available to the programs.

Linkages & Dependencies to Other Projects:

Priority: To be determined by CTO and RGIO Staff.

Resources Required (Manpower, Equipment, Software, Etc.):

Estimated Project Cost and Probable Source of Funds:

Benefit to USGS Mission:

Schedule: Planning for the Reston Office Automation Technical Support implementation is underway. Initial operation by 2nd- 3rd Quarter FY04.

FY 04 Action and Tasks: The Reston OA Technical Support Project is a short-term effort (during FY04) to consolidate Reston IT technical support into a single unit, and to implement Active Directory in the Powell Building according to bureau recommendations. Authority for this project is through Karen Siderelis' 9/24/03 Memorandum, signed by the Director on 10/3/03, subject: "Organizational Strategy for Bureau Information Technology Infrastructure".