

**U.S. GEOLOGICAL SURVEY/EROS CENTER
TECHNICAL REQUIREMENTS DOCUMENT
for
TECHNICAL SUPPORT SERVICES CONTRACT SOLICITATION**

TRD NUMBER

0008

PERFORMANCE PERIOD

Contract Base Year: April 1, 2010 thru March 31, 2011

PROJECT NAME

Engineering & Information Technology Support

Introduction:

This document describes the specific TSSC technical work requirements and deliverables in support of certain task areas within the EROS Engineering and IT (E&IT) Support Project. Each of the following sections of this document is intended to be representative of individual Technical Review Documents (TRDs) in their own right. The sections are merged here under a single document only for administrative efficiency. There is no requirement for E&IT project-level support from the TSSC. All support is at the task level and specifically documented for each in the following sections, including reporting requirements. All reports and deliverables should be provided directly to the applicable government task manager and not coordinated with the Project Chief. All documentation should be identified by government task and not by E&IT.

Specific Government Task Support Requirement Areas

The specific government task areas with support requirements include:

- I. Desktop Services Support (DSS)
- II. Network Services Support
- III. Enterprise Architecture, Technology, & Investigations
- IV. IT Security Policy, Coordination & Monitoring
- V. Enterprise IT Services
- VI. USGS ITSOT Support

I. Desktop Services Support (DSS)

A.) Operation, Maintenance, and Development

Scope, Guidelines and Assumptions

DSS:

DSS is an activity that provides true user based desktop services for USGS/EROS. The DSS supports approximately 600 users and 800 PC devices. DSS provides user support as a centralized configuration managed activity. Users are primarily located at the center with a small host of dedicated offsite users both local and national.

Providing a standard and centralized support plan DSS can incorporate general and understandable support practices using established system configurations, Configuration managed PC Images, certified software, and structured access for users on EROS shared drives, folders, and servers. Centralizing creates overall support costs that are maintainable, predictable, and supportable within the established EROS expectation of cost, budget, and support guidelines.

The Center:

EROS as a center maintains a variety of UNIX, Linux, Intel, Windows, and Macintosh computing systems. These systems classified as Project Servers, Dedicated Project & Production Devices, Multi-user, and single user computing systems. This activity only supports the Configuration Managed, Center-wide, Windows & Mac, Non-project specific user based PC architecture.

Who and How DSS is received:

Desktop support as a resource to EROS employees begins with a request for system support from a designated government approving official. Today the following positions have been designated as the centers approving officials for user based, non-project, desktop services, they are as follows; Contracting Officers Onsite Representatives (COR's), USGS EROS Line Supervisors, or the centers Directors Office. Once the system has been installed, this system becomes a congruent device within the larger EROS user based desktop architecture.

Network Backbone Support:

DSS does not manage the network backbone that supports the EROS DSS devices. Network Service initiates at the point of connection or wall plug, from that point forward DSS fully supports the actual desktop, laptop, or tables PC system.

What is included in DSS general PC Support?

Includes, Software Support based on the EROS Standard Configuration Managed Software Image, and Hardware Support (Diagnostic Assistance, and user classified installation of replacement parts as provided by the manufacturers warranty).

What is Included in DSS Specific PC Support:

Includes Configuration and Technical Assistance in the areas of Lotus Mail, MS Office, Internet Explorer, Adobe reader, Security Prevention, Access to the common shared file systems, add-ons to visual displays as well as a second hard drive and memory upgrades compliant to manufacturers warranty provisions.

Most Significant Functional Goal:

Provide all EROS personnel with DSS standardized desktop functionality and support in a centralized service model. Services include installing new Desktop and Laptop systems for DSS customers, repairing PC systems within warranty guidelines, and removing broken or older system from service as they become obsolete or functionally inadequate for the user, project, or program.

PC Systems

The following are critical activities that are users, approving officials, and DSS will be involved with on a daily basis.

1. **Installations of PC Devices with the following activities:**
 - a. User Request Validation
 - b. Approving Officials Validation
 - c. Proposed System Validation
 - d. Continuous Support Validation
 - e. Location Inspection and Validation
 - f. Acceptable Supported Configurations
 - g. Method and Plan of Receiving an Installation
2. **System Maintenance**
 - a. Center Wide Messages, assisting and guiding users.
 - b. Security Updates – Required to maintain a secure environment
 - c. Virus Protections – On the client and server
 - d. Printing Support – Web based locate tool, for windows machines
 - e. Network Support – Compatibility to the network, Network support is not required.
3. **System Repair:**
 - a. Problem Identification – Users contact using email, and telephone request through the DSS Helpdesk
 - b. Remediation – This is provided by the manufacturer for hardware, and DSS for software using the online technicians that are onsite providing remediation at the user’s location.
 - c. Follow-up – This is required to bring all calls to closure. No user request shall be closed until the initial request has been fully completed and the user is satisfied with the final results.
 - d. Closure – One a service is provided DSS shall respond to the user with a statement of the problem, resolution, and outcome including all dates and names.
4. **System Removal**
 - a. **Typical reasons systems will be removed from access.**
 - i. **Employee no longer employed (ENLE) and**

- ii. **System has reached a state of functional or technical obsolescence (OBLs).**
- b. Requesting Pickup – Once the approving official request a system to be removed DSS will provide the Data Cleansing Service and use the approved DSS process to complete the service to include data removal for drives that have bad sectors.
- c. DSS Processing – If a system is removed for ENLE, DSS will cleanse the system using the approved process and evaluate its technical applicability for future Reuse.
 - i. Systems that are considered OBLs will be excessed by the appropriate property official, the system will be removed from the DSS area 300 by an assigned agent of the property official. The official must schedule all pickups with DSS.
 - ii. Systems that are considered Reuse will be categorized by the technical functional usage and housed in the DSS Reuse area until it can be reutilized.
 - 1. These systems will be logged in a database with all identifying information (Past user, Functionality, Configuration, Warranty Data, Date in Reuse, Date out of Reuse. Last know Approving Official.
- d. Data Cleanse – This service assures DSS customers that their privacy and security are assured. All systems that are ENLE, Reuse, or OBLs will be cleansed immediately upon DSS receipt. DSS will provide the agreed process to complete these services. Once complete DSS will notify all OBLs approving officials that the cleansing is complete.
- e. Removal from DSS – All DSS systems that are removed permanently from the Active System Management will be effectively removed from all IP access locations, Active Directory connections, and all users corresponding identification.

Desktop Install Coordination Deliverables

DSS is required to manage all its supported devices for the centers Directors Office. The primary goal of this activity is to provide our users (both government and contractor employees) personal computing systems that are functionally effective for their position requirements, technically appropriate to meet their operational needs at a minimum status (Government Furnished Requirements (GFE)) and that systems are being used to the maximum extent practical while maintaining continuous DSS supportability.

PC Install Coordination is the activity that maintains responsibility for installing and advising on the refresh of government and contractor GFE. The following are critical descriptions and deliverables required to meet this activities needs.

1. Classifications and boundaries:

- User Validation – System and User are established requirements from the appropriate approving official.

- Supported Devices: Workstations (Laptop, Tablet, Desk-side), Windows based Printers, Single and Dual Monitors, and approved internal and external peripherals.
- Supported Configurations: DSS Pre-defined Windows and Macintosh desktop systems, and Printers.
- Methods of Communications: Approved configurations are available online within the DSS dedicated web pages, as well as definitions supported those configurations.
- Hardware Categories: Laptop, Notebook, and Desktop Systems; Printers and Multi-function devices.
- Installation will be provided by EROS through the TSSC contract, cost per unit will be identified.
- New or replaced desktop systems – New Systems will be one of the DSS advertised “Complete” standard configurations.
- The data cleanse process – security defined by the level of system data sensitivity. The appropriate property official must designate the level of the sanitization. System storage device housing non-classified data will be wiped by using the EROS accepted write over methods (6X passes) whereas system storage devices housing personnel data may require degaussing or destruction.
- Data cleansing is extremely important as the public, educational institutions, and non-profit organizations become owners of these USGS systems. It is critical that there is no availability to the prior user’s data, unless prior designation has been appointed by the USGS before the process has initiated.
- Upon Receipt of the system, DSS Technical Staff shall not look or attempt to view data from any other computer system whether it be repaired, replace, cleansed for removal or a know coworker. The data cleanse shall be processed directly upon receipt.

2. Validation of Install Request Data:

The following will be provided to by the approving official DSS to formally initiate the install coordination. The following must be validated:

1. Name and Location of user
2. Type of current functional user and system
3. Date user requires system (2 weeks minimum)
4. Estimation of priority with justification.

3. Required PC Install Coordination Deliverables:

To receive a system installation DSS receives a request from an approving official for a desktop or laptop resource. The following deliverables will be completed by DSS during the request for installation process:

1. Validated Install request from the approving official
2. Completed Requirements analysis that user and DSS mutually agree to.
3. Completed Onsite inspection and modification advisory if required.

4. Unique Customer ID to be used continuously throughout coordination service.
5. Completed Reuse analysis and findings document (New or Reuse) communicated to approving official and user.
6. If New System, completed findings document validating system completeness, burn-in, and user notification that system is here and ready for installation.
7. Once system has been identified for coordination, accepted proposal between DSS and the user committing to a finalized installation plan; to include date, time, place, system configurations being replace and the new system being installed.
8. Complete User Profile identifying all software users will install and all software DSS will install. This should include all the current configurations specification as well as the new configuration.
9. Agreement of closure between DSS and User stating that all deliverable are finalized, and the service has been received in entirety.

4. System Identification - derived from two categories:

1. New, systems delivered direct from the manufacturer - out of the box new (OTBN)
 - a. 5 years of Warranty
 - b. Next Day Onsite
 - c. Telephone and Technical Support
 - d. New or reconditioned parts (as new)
2. Used, system that were transferred form DSS Reuse - reallocation system transfer (RST)
 - a. Usually Supportable by a warranty or extended support plan.
 - b. Usually 1 – 3 years old.
 - c. Provided from a centralized repository
 - d. Usually, no expense to customers or approving officials.

5. Supported System Configurations

To be qualified as a DSS supported system, the configuration must be supportable under the support guidelines of the center as well as DSS. During the Install Coordination Process, DSS will attempt by working with the user and the user's profile to identify the functional requirements of that users needs. Once complete the functional description is mapped to a proposed technical solution. Those final configurations are then matched to the centers catalog of available used systems called Reuse. All systems in Reuse are automatically supported by DSS. However if a system in not available and a new purchase is required the responsible purchasing authority will be required to procure a system that is fully supportable by DSS without additional constraints and support practices/processes. All supported system at a minimum will contain the following:

1. Unless approved the system will be Intel architecture capable of efficiently utilizing a Windows XP operating system.

2. The system will be capable of containing the approved EROS desktop software image.
3. The image will be loaded by using the DSS Ghost server in the same form and function as all other DSS systems are loaded. The contractor will be required to load the appropriate number of system images as to adequately support the DSS installation and rework requirements without undue manual software loading.
4. The system will be maintained within the recommended scope for all I/O interfaces as designated within the DSS Standard Recommended Configurations.
5. The system will be assigned to a dedicated user; the system shall not be installed to directly support any project or production requirements.
6. The system will support users that are security compliant and resident in the USGS Active Directory.
7. DSS Does not support any Non-DSS project systems requiring a general logon or multi-user service account.
8. All supported systems must be USGS Security Compliant and be maintainable through the USGS/EROS Networking infrastructure.
9. Without prior approval DSS will not install any Non-Networked DSS supported systems.

6. DSS Standard Configurations

All DSS standard configurations will be derived from the following potential resources.

1. DSS will create, update, and maintain approximately eight (4 Desktop, 3 Laptop, 1Tablet) recommended standard configurations (DSSSC).
2. Recommendations and changes to the DSSSC will be driven from the current knowledge of our onsite technical staff, using our current Active Management System for purposes of evaluation, and the Install Coordination activity.
3. The DSS requirement specifies that the acceptable level of operations and support shall assure a compliance rating that at least 90% of all DSS supported devices are DSS standard configurations.
4. All DSSSC deviations must be approved by the DSM, DSS, and the Directors Office.
5. Standard Configuration information shall be posted as a user-friendly web page in the DSS Support Website. These pages will maintain to be interactive and optional in the areas of visual display, memory, additional hard drive, add external drive backup, cases, power supplies for mobile units, and docking stations.

7. Non-Standard installations

Configuration Requests that are not derived from the offered DSSSC shall be an independent special request and require approval from DSS (DSM). A follow-on request shall be initiated by the approving official to identify the potential deviated support requirements.

Once approved the TSSC are required to respond to all non-standard actions with an estimated Level of Effort containing time estimates, rates, proposed schedules, skill categories, and a preliminary plan of implementation.

8. DSS Working Guidelines:

- All OTBN installations will be derived from the available standard configuration web pages.
- All OBTN, and RST installations will be completed as agreed to with the requesting and DSS.
- All installations once requested, agreed to, and confirmed will have space allocated for the desktop device and available for receipt of delivery to DSS 300 area within 8 hours of the requestor's confirmation of the delivery.
- All devices that have been processed through a formal coordination will be delivered to DSS area 300, unless agreed and confirm to with the requestor and DSS.
- All new device procurements and delivery arrangements will be the responsibility of the project or ordering official.
- Final installations will not be requested until the user is prepared for and agrees to the proposed DSS delivery arrangements. The user is responsible for establishing a valid installation date with DSS once system availability (Open Box, Inventory, Test Burn 24 hours, and contact purchaser) has been validated and communicated to the user by DSS.
- All Install Coordination Request shall be completed such that an offer of Reuse or New system suggested configuration to the user and approving official within 3 days of initial contact from the approving officials request for a system installation.
- All Reuse systems will be installed NLT five days post acceptance by the user, approving official, and DSS.
- All install requests will be specific to the request and will not initiate follow-on actions like transfers, additional add-ons, or system cleansing.

DSS Resolution and Assistance:

Through the support of on onsite Helpdesk, DSS specific web pages illustrating directions, forms, and configurations together with a qualified technical staff certified in Helpdesk resolution and IT Desktop Knowledge-based software usage is expected to assist with failed systems, software configuration issues, security, access, installations, modifications and online and automated forms support. When a system breaks, DSS will provide a loaner system (LS) from our designated temporary use system pool. These temporary transfers may be in place until the user's system has been repaired or replaced (Not to exceed 60 days). When older systems become ineffective and outdated, DSS will prepare the system for removal of service by performing a data cleansing process and removing IP addressing as well as mail system and USGS directory access.

Tools that are available and supported by DSS include:

1. Helpdesk Common User Actions:
 - a. For users experiencing technical problems with their DSS supported workstations; includes hardware, software, and peripherals,
 - b. To check a status of a repair, replace, or new installation
 - c. To follow-up on user requested action, i.e. security patches
 - d. For users to understand more about a DSS form that they submitted
 - e. To clarify information published by DSS on a EROS web page
 - f.
2. DSS interactive and informational web pages :
 - a. Online forms
 - i. To assist with PC requirements and defining
 - ii. To request the approval and initiation of desktop resources
 - iii. To install DSS supported commercial off the shelf software
 - iv. To request folder permissions
 - v. To request different system access
 - vi. To request a data cleanse or removal
 - vii. To request a vacant system pickup
 - b. DSS Information
3. Center wide Messages

DSS User Actions

1. Desktop Install Coordination

All installations shall be approved, preplanned, and coordinated by DSS using qualified TSSC representation. Installation activities will include a site survey and preliminary planning questionnaire so that installations will be effectively completed at the time of delivery of the desktop system.

The goal of Install Coordination is to eliminate unnecessary redundancy, understand and predict follow-on actions (i.e. network add-on, no room for monitor, no place to image pc, etc), and provide timely effective services without interruption, downtime, missed appointments and aged pc's still in boxes due to unresolved post installation problems.

Installations must be validated with the actual user, and, for DSS, is not considered active until the user is prepared for the installation to be completed.

All contracts like the TSSC will provide the Contracting Representative (COR) with annual desktop requirements. The DSS project does not support GFE requirements analysis within its standard services.

Project requirements analysis and support is available if it relates to a valid DSS support function as a supplemental action. TSSC will direct charge those actions whenever possible while maintaining lead communication and planning actions with the USGS DSS Manager.

2. Desktop and Printer Warranty Support:

- All repair requests will be through the EROS Helpdesk. Unless already documented, hardware analysis will be the first level of resolution. If there is a hardware compatibility issue, functional problem, or failure and the system has a support warranty manufacturer, the warranty process described below is followed.
- If a warranty is in place that provides onsite support, DSS will provide the user with technical assistance to contact the manufacturer. The manufacturer will be responsible to repair the equipment and provide a new system component or a replacement Laptop, Notebook, or Desktop Intel/Macintosh computer.
- User Interface: EROS Desktop Users will contact the helpdesk with hardware issues, problems, or failures. TSSC will contact the Desktop manufacturer as an advocate for the user although not the official manufacturer's onsite representative. TSSC will assist the user to diagnose problems and if it has been established as a hardware issue, TSSC will assist the user or project assignee to request onsite support service with the device warrantor.

3. Classification of Desktops Manufacturer Warranty:

- Full Onsite Support includes three-hour response time and eight hours resolution clock time.
- Calls initiated after 3pm, will be continued the next business day at 8am.
- Days of Coverage is defined as 365 per year, Monday – Friday, 7am – 6pm.
- Replacement Parts: Parts supplied by manufacturer, will be certified as new and not remanufactured and sent by overnight carrier guaranteed 8am delivery.
- Warranty Period: Standard Configurations will cover by five years of coverage.

4. Classification of Printers Manufacturer Warranty:

- Full Onsite Support includes three-hour response time, eight hours resolution clock time. Calls initiated after 3pm, will be continued the next business day at 8am.
- Days of Coverage is defined as 365 per year, Monday – Friday, 7am – 6pm.
- Replacement Parts: Parts supplied by manufacturer will be certified as new and not remanufactured and sent by overnight carrier guaranteed 8am delivery.
- Warranty Period: Standard Configurations will cover by three years of coverage.

5. DSS Support for External Add-ons:

- Secondary support shall transcend to DSS approved peripherals like monitors, docking stations, external media devices, sound, keyboards, and pointing devices.

- When there is a failure or problem that cannot be resolved by available management of the current system, the user or project assignee will be responsible to work with the manufacturer to replace the part or repair the part.
- Based on system complexity and availability, DSS may or may not assist in removal of this part based on definition of this service and how it fits into the functional scope of DSS.
- Dual monitors will receive assistance; however graphical add-ons or non-standard components will require a funded action for the project to be provided this service.

6. Software Support

Software includes the standard configuration managed CM image including office automation, mail systems, security, Internet access, virtual private network (VPN), and mission support systems. Software as defined is listed below.

- If a user has a problem with the software that is part of the standard DSS CM Image, the user can access the Helpdesk by email or telephone to receive support.
- DSS provides configuration support in the areas of installation, patches, and technical conformance.
- DSS will not provide training on applications through the Helpdesk.
- Updates to software will commence once a month on the same day from a general stationary memo that reminds DSS customers of their responsibility to patch from software updates.
- Security related patches will be monitored for compliance. TSSC will compile compliance lists and submit them to the DSS Manager for future actions.

7. Mail Systems:

The USGS EROS Mail system is currently supporting approximately 550 users onsite and approximately 50 concurrent users offsite. Onsite users access the mail system directly from the desktop while offsite users may access the mail system through a virtual private network (VPN), or the online internet version. Typically 5% of all calls relate to a lotus administrator follow-up

- TSSC will support the current USGS EROS Mail System within the hours of the current Helpdesk support hours (7am to 5pm).
- TSSC will provide a consistent level of continuous support throughout the day, week, and month.
- TSSC will respond to users request within 10 minutes by a qualified Lotus support person.
- TSSC will assure that problems are remediated within 1 hour, unless DSM approval has been granted.
- TSSC will provide first call resolution for all base management problems (i.e. password reset, online client termination, archive direction)
- TSSC will provide DSM approved hardware installations (70 – 150 hours annually) for the USGS GIO managed onsite servers.

- TSSC will maintain redundant and/or cyclic center wide messages to DSS user. These messages may request action, confirmation, information, planned outages, and upgrades.
- TSSC will maintain support to maintain the USGS EROS portion of Active Directory to include activities like new user updates, removal of users from system, removal of IP access, etc. Work access includes the connection to the EROS network, an established identity within the Active Directory, and a set of predefined paths to the shared cluster, printers, and the Internet.
- Network Services is an independent activity from Desktop Services and supports our customers through the DSS interface (Helpdesk).

Help Desk Support:

- Problem Resolution includes access to certified ITIL compliant Helpdesk staff. For the remainder of FY09 DSS will implement a single desktop one-click primary access point to the help desk. Secondary contact will be through the telephone, third level will be general email, and fourth will be walk-in. It is required that all customer contacts are generated from our 1st or 2nd point of contact by February 09. Due to unavailable data it is difficult to track and understand general walk-in problems, and forces the TSSC to self generate tickets from our customers.
- DSS goal is that at least 25% of all Helpdesk actions from our customers receive immediate or 1st call resolution from the Helpdesk Technicians and the Knowledge Base Software. Help Desk Support services support all DSS customers and assist in the primary and secondary support areas of DSS installation, repair, system failures, shared access, printer connections, CM software issues, Lotus mail systems, and offsite support. DSS requires an LOE for major call categories included those handled within the initial call.

Secondary – Security Access & ID:

Security Access & ID includes establishing and monitoring access into file systems, folders, drives, and software applications like Lotus and Active directory. This also includes establishing and resetting of passwords, and using VPN for offsite and not here systems, including access profiles and system registration.

Active System Management:

Asset Management and Reporting is included for all DSS customers. This services provides a concurrent status of all users in DSS, including complete configurations, critical dates like install and warranty, type of system, level of support and method of acquisition (accounting and project). These data points are referenced to the DSS support registration that tracks all current users within the support environment. Although DSS does not include the actual acquisition there are some resources that can assist a user in the purchase of their next system.

Standard Configurations:

Through our configuration team we will publish a variety of system configurations to meet users' needs like desktops for administrative professionals, power GIS, and engineering users, mobile light for users with Laptop requirements less than four pounds, and a standard laptop to used for occasional travel.

Our desktop support, based on the ability to configure systems from the standard configuration page, is estimated to be approximately 220 systems per year. Non-standard configuration may impact the number of standard configurations without increasing the support cost. The DSS requires that configuration assistance can be provided for 100 systems per year without an increase to the cost allocation tax base.

Requirements Profile:

Total FYxx Estimates	
Number of Systems	1153
Number of Charged systems	786
Number of integrated systems	45
Number of non-supported systems	319

<u>Systems</u>		<u>People</u>	
Desktop	410	Onsite	460
Laptop	300	Offsite	135
Support	97	Outside Contracts	53
IT infrastructure	56	Other (Education)	15
Macintosh	30		
Storage	190	Organizations:	
Training	40	USGS	103
Loaner PC	20	USGS Intern	20
Outdated Parts	40	Other Gov IT	76
		Non IT Contracts	27
	1153	IT Contract	340
		Scientific	43
Age and Warranty			
Systems		On Warranty	820
Less than 1 year old	186	Off Warranty	333
1 to 2 years old	183		
2 – 3 years old	408	Projected New System Installs	610
3 – 5 years old	331	Out of the Box	220
Beyond 5 years old	45	New to You (Transfer)	250
Total Systems	1153	Rework System	140

Qualifications for Full Support:

- GFE in support of an active EROS project
- EROS as a primary location of user or project
- Installed (Configured & Integrated) by Desktop Services
- Supported by Desktop Services

- Network Connection to USGS EROS network
- Lotus mail client and server access required
- Online or Phone access to Help Desk
- Utilizes Patch Management
- On the USGS EROS Network
- Access to Shared Drives J: and K:

Specific Areas of Work and Deliverables

Desktop Direct

- **Installations** (For Volume See above)
 - Request will not be initiated until the system delivery arrives in the Warehouse.
 - Request for all installations (New, and New2you) will be through the EROS Web interface by using the desktop Hot Button or Web install form.
 - Request to install will be initiated by the user or the assigned POC.
 - Request will be initiated once warehouse has confirmed a complete system delivery.
 - Installations will be confirmed within 1 business day with a tentative install date.
 - Once warehouse schedules delivery installation coordination will be finalized
 - Installations will be completed within 15 business days of confirmed delivery.
 - Approximately 6 installations per week will be completed.
 - Installations will be priced per unit, based on an end-to-end cycle

- **Repairs or Reworks** – Estimated 300 – 600 annually
 - All repairs will be initiated as a follow-on action from an active Help Desk request for service.
 - All minor repairs will be completed within 3 business days.
 - All major repairs will be completed within 1 week.
 - All system failures that have been determined final will be provided with a short-term system from the system pool facility.
 - Project will have access to this system NTE 60 calendar days until the replacement system has been procured, received, installed and operational.
 - All new replacements from failures will be first replaced with available systems within the Directors office, prior to purchasing a new replacement system.
 - If the system is under warranty and the user is still functional, DSS will initiate the service call and arrange for the technician to complete the service call.
 - If the system is under warranty and the user is no longer functional, DSS will initiate a request to install a RST system.

- The temporary system will be installed within 4 hours, and must not exceed 30 continuous days of service.
 - Once completed DSS will pick-up the system, finalize reintegration of the repaired system. The Loan2you system will be returned to our facility for the next user.
 - If the system is no longer under warranty and is no longer functional, DSS will provide a short-term system from the Loan2you facility NTE 60 days.
 - It is advised that if your system is older than 5 years and in need of repairs exceeding \$300.00 that a short term Loan2you system will be provided and a new system procured by the project to replace the older failing system.
- **Data Cleansing and System Removal Preparation** – Estimate 550 units annually
 - Once it has been determined that the system has become obsolete and incapable of meeting the user or the project requirements the user will contact the property management staff to complete the excess property requirements (Form 9064).
 - Once the project has completed the property management requirements, the user or POC will create a request to prepare the system for excess.
 - The request will be completed by the user or POC, using the online system or the Desktop Hot Button.
 - The request will be acknowledged within 1 business day with a proposed schedule for the excess preparation.
 - The system will be picked up and processed according to applicable security standards set forth by this document (Security Manual, Chapter 12, storage and magnetic media cleansing).
 - Once processing is complete DSS will attach the Certification of Cleansing to the prepared system, and notify the user or POC that the cleansing is complete and submit the request to transfer the system to the property management staff.
 - Once finalized DSS will close the request with a confirmation of completion to the user or POC.
- **Reuse Management – 150 systems annually**

The Directors Office requires DSS to manage the system reutilization process.

Once a system becomes vacant without a direct user the system will become part of the Reuse availability. This activity manages, tracks, and logs all systems coming and going out of the Reuse inventory. This will be integrated within the Install Coordination process.
- **Desktop Ops daily**
 - Support CM EROS Image Standard Configuration.
 - Investigate monthly changes.

- Adapt user requirements from IT comfit group.
 - Publish to Web, updates and changes.
 - Meet with group, present changes.
 - CM Standard Software Install.
 - CM Standard Network and Shared Access.
 - Security.
 - Monitoring, monthly average 500-user base.
 - Upgrade and repair, patch cycle for all Cots and OS.
 - Assist other agencies, Interface with BWTST.
 - Meetings preparations, establish access points and Desktop comfit 20 meetings per year and 300 – 550 personnel.
 - Reporting, to Desktop Services Manager Monthly.
 - Meeting Interface (number of meeting appointments).
 - IT Desktop Configuration Group 12 annually.
 - IT Desktop Services Panel, 20 annually.
 - IT Desktop interface to Security, 12 annually.
- Web Support
 - Update and maintain approximately 15 pages on IT Desktop Support Site.
 - Desktop User Initiated Action Forms.
 - Update and maintain BPA standard configurations.
 - Information Pages.
- Remove and disable approximately 10 pages currently on IT Desktop Support Site
 - Property Input Forms on Desktop Support Site.
 - Project Direct Install, rework, and repair forms.
 - Project Server Configurations, not supported in Desktop Services.
 - Outdated Procurement Documentation.
 - Remove and disable all printer related request forms.
 - Security Port Scanning
- Security Port Scanning of DSS Devices
 - Utilize EROS Enterprise Server to perform tri-monthly vulnerability scans.
 - On a monthly cycle, perform the IT specified port scans on one third of the DSS system.
 - Compile a report of all DSS vulnerabilities and forward to the DSM within 2 business days of processing.
 - Report as follows
 - Date of last Scan and new scan, and Type of Scan
 - Vulnerability Assessment
 - System IP and System Name
 - System User, and approving official
 - Level of Vulnerability - Moderate, Medium, or Critical
 - Description of Vulnerability
 - Suggested Remediation of Vulnerability

Help Desk Support

- Incident Tracking
- System Requests
 - Estimated actions.
 - Telephone Contacts – 150 weekly, 8000 annually.
 - Web Support – 50 – 80 weekly, 3000 annually.
 - Walk in Support – 10 – 20 weekly, 800 – 1000 annually.
 - USGS actions – 2000 – 3000 annually.
 - (Security, Property, Active Directory, Lotus mail).
 - User Initiated.
 - New Installations – 500 annually.
 - Repairs – 2600 – 5000.
 - General Questions – 3500.
 - Technical Clarifications – 3500.
 - Patching and Access – 2500.
 - System actions, problems, and processes are managed with the Heat integrated Helpdesk applications.
- Service Hours
 - DSS Standard service desk hours are Monday through Friday, 7 a.m. – 5 p.m.
- Customer requests
 - Customer questions, request and/or problems are assigned a unique call tag.
 - All requests are tracked from initiation to completion or resolution.
- Concurrent tracking
 - All incidents will be tracked centrally so that DDD will be capable of implement actions from the point of discovery, analysis, and resolution to eliminate redundancy, or duplication or common problems in the EROS computing environment.
- Work Assignments
 - All work assigned from or through the Helpdesk or Web support will be tasked and tracked within the Heat Application so historical or performance metrics data will be available in reports, review, or notes.
- Ticket Escalation
 - Ticket escalation shall be documented as a policy and will be based on the importance or significance of the system degradation.
 - Element to consider will be the level of degradation, size of group affected, the application, the failed or effected service, and the hardware involved in the issue.
- Ticket Point of Contact
 - The TPOC will be the person or team responsible for managing tickets in a particular service group, the user originating the work request, and the Helpdesk Technician that managed the request.
- Continuous User Communication
 - Customer status by use of the Hot Button, Web Support, or the Telephone shall be available to see tickets and request 24x7X365.

- Status of Help Desk Calls
 - Help Desk statistic summary page.
 - Help Desk escalation policy.
 - Help Desk guidelines and expectation for PC installations.
- Create and maintain desktop Hot Button to access Desktop Helpdesk
 - Located on Desktop.
 - Activates online screen for helpdesk support.
 - Automates new call tag.
 - Provides user with estimated response time.

Facilities Managed Conference Room IT Support

Provide Conference Room Support to Eros Projects and Users.

EROS as a Center has approximately a dozen dedicated conference rooms that will require support. Each of the rooms has a minimal desktop support device, an active network connection, intermittent visitor's network access, and a mounted projector. These facilities are managed by the Centers Facilities Management. Contact to provide support is through this organization.

Typically in an annual cycle there are 40 events that may require support, 20 of the event require minimal support, 7 -9 require medium support, and the remainder require comprehensive support.

1. Minimal = Single IT User, projector Usage, shared access using the available pc system, no storage scanning

2. Medium = Multiple IT Users, Projector Usage, Shared access using the available pc system, 4 – 8 additional user based systems accessing the local visitors network, some storage scanning.

3. Comprehensive = Mixed users typically 15 – 30, variety of access (Secured and Unsecured), system require scanning and updates, and hard drives require virus scans.

Process:

1. DSS is contacted by Facilities
2. DSS contacts conference sponsor
3. Requirements analysis is completed from sponsor meeting
4. Estimate provided to DSM within 2 business days of sponsor/DSS meeting
5. DSM finalizes support agreement
- 6 TSSC provides support.

Performance:

1. TSSC will contact conference sponsor within 1 business day.
2. TSSC will meet with conference sponsor within 2 business days of initial request.
3. Once conference has been approved by DSM, TSSC performs as designated in the support proposal.
4. TSSC will provide a proposal that is clear and concise.
5. TSSC will provide a description of like deliverables aligned to expected cost and schedule.
6. TSSC, whenever possible will use established unit pricing to streamline

- and simplify the language, structure, and estimate of the support proposal.
7. TSSC will not allow changes without consent and approval of the DSM.
 8. TSSC will provide only the agreed services, without deviation or change.

Follow-up

1. TSSC will provide the report depicted the actual verses estimated planned expenses
2. The final report will be provided to the DSM within 7 calendar days.

Reporting:

- All reports if containing data will be provided in both PDF and Excel format.
- Desktop Request Status Report: Data will be primarily in excel and depict the weekly in and out flow of user request for services. This report will be specific to forms activity and our response. As a starting point DSS requires that we track number of all installs, transfers, data cleanse, terminations (need to redefine), and reworks (Reasons why) requests, completions, and current status.
- Storage Report: Once a month what is in current storage and progress of project to complete projected usage of systems. Please adjust current reports slightly only to add scheduled departures of current storage systems and those storage systems that are resident for production or DSS usage.
- Customer Service Be-Weekly Report: This report will be focused on customer performance reporting, including service areas, processing time, received customer evaluations, customer comments, customer name, and service received.
- Desktop Weekly Summary Report: This should be standard bullets that depict what TSSC has accomplished through the past week and current work in progress. This report will contain contractor labor costs by major activity category (customer service, Helpdesk, system installs, service requests, user incidents, and other). The report detail will address general summarization of the user form activity, security, virus activity, patch management status, special actions and non-standard requests. Help desk activity summaries need to add major and minor reason codes to create a more detailed depiction of helpdesk and Heat activity.
- Monthly Detail Heat Report: This report depicts an overall center-wide perspective of DSS work that has been performed. A basic need is establishing reason codes for the various activities. The report should categorize work and service areas within reason code, each depicting work being performed, contractor labor costs and applicable performance data.
- EROS Center Messaging:
 - TSSC will maintain stationary for all standard cyclic center-wide messages.
 - Center-wide stationary will be reviewed quarterly.

B. New Developments and Investigations

Beyond the day to day operational and performance expectations of Desktop Services there remains a necessary technical requirement to look down the road and plan for future developments. These developments include but are not limited to new hardware platforms and architectures, upcoming software implementations, streamlined operational advancements, and efficiencies to Desktop Services internal processes and customer interfaces. It remains a necessary component to Desktop Services to fully develop actions before implementation to a center wide change. These activities apply to USGS EROS center as described in the Desktop Introduction and element (A) Desktop Operations and Maintenance. These activities may be driven from internal directions within EROS as well external organizations through mandatory agency and department wide technology plans.

A. Software

1. Lotus Conversion to R8 continued
 - a. Proceeding with R8, user assistance -
2. MS Office 2007 (Migration) Summary, the USGS will be implementing Office 2007 over the next six months, the following steps are required to create this implementation. Assumption, for scope please refer to (A).
 - a. Planning
 - b. Migration
 - c. Follow-on
3. Windows 2007 (Investigation) The USGS will be implementing Office 2007 over the next 12 – 18 months; the following steps are required to create this implementation. Assumption, for scope please refer to (A).
 - a. Research
 - b. Investigation
 - c. Published Findings
4. Windows Apps (Investigation)
 - a. General Study,
 - i. Ghost, the CM Image
 - ii. Additional COTS
 - iii. Long term Planning

B. Hardware (To be defined further at a later date)

1. Alternative Platform
2. Configuration Management (Definition, Requirements Establishment)

C. Procedures

1. Installing and Maintaining Desktop Computers, Lifecycle Management (Investigation)

D. Management and Accountability (Over the last 12 months there was a definition, and a table to initiate an asset management database, at the time all of the IT investments were to be included in that system. The redefinition only

includes the management of DSS direct and customers' assets including desktops, laptops, attached peripherals like storage and monitors as well as medium to large volume printers. Secondly, network services maintains equipment, this would also be included.

The direction over the next year will be focused on user interface, data integrity, and establishing standard processing for data input, updates, and reporting. We are currently investigating new methods for gathering data. The following are considerations for the next follow-on phase of Asset Management.

1. Asset Management
 1. Definition (Recast)
 2. Proposal
 3. Implementation

II. Network Services Support

Scope

The Network Services Task is a component of the Engineering & Information Technology Project (E&IT). The TSSC supports both Center Infrastructure tasks as well as Project-specific tasks. This document describes the scope for Center Infrastructure tasks. Scope applies to office automation connectivity as well as common network interconnections utilized by projects to receive and deliver data to and from users and cooperators. The LP DAAC, Landsat, and LDCM projects have project-specific sub-networks with separate network switches and firewalls that are not part of this TRD.

The Network Services Task supports both the Local Area Network (LAN) as well as connections to multiple wide-area networks (WANs). There are four WAN networks currently: 1) the original USGS network (GeoNet3) providing connectivity to all USGS field offices, regional offices, and Headquarters; 2) the Department of the Interior's Enterprise Services Network (ESN), which provides connectivity to the Internet and to all DOI bureaus and offices; 3) the Starlight NISN/Internet2 connection to NASA via the NASA Integrated Services Network (NISN) that supports large volumes of Land Processes Distributed Active Archive Center (LP DAAC) data ingest and distribution and provides connectivity to Internet2, National Lambda Rail, DREN, and other high-speed private networks; and, 4) the South Dakota Research, Education, and Economic Development (REED) optical network that provides very high-speed (10 Gigabit/second) connectivity to the South Dakota universities.

The existence of the Starlight and REED networks complicates the WAN relationship with DOI's ESN. The emergence of the Office of Management and Budget's (OMB) Trusted Internet Connection (TIC) initiative in FY09 will initially complicate but eventually simplify the Center's unique contribution to DOI's ESN. The emergence of the 10-Gigabit optical REED network in late FY08 is a tremendous opportunity for future high-speed connectivity, but a number of issues must be addressed before the future potential can be tapped.

In the following sections the work required to support the Network Services Task is allocated between Planning and Development and Operations and Maintenance. The O&M work is further subdivided into tasks focused on the LAN or the WAN.

An assumption has been made in the scope of the deliverables described below in terms of functions provided by the Help Desk. For this TRD, the Help Desk functions used to facilitate network problem resolution or change request will be obtained through the Desktop Support Services (DSS) task. No additional effort should be allocated to the Network Services task for providing Help Desk support.

Only Center-wide infrastructure requirements are defined. Project-specific service requests would be defined by the projects and communicated via their TRDs. It's presumed that the TSSC resources supporting infrastructure tasks also would support

project-specific tasks. An example of project-specific support is the maintenance of firewall rules in a project-owned firewall, or maintenance of operating-system upgrades in project-owned switches.

When the final scope of Network Services technical requirements is negotiated, the TSSC will be asked to assist in breaking the work into relatively small work elements with an LOE not exceeding \$30,000 per element. In option years this ceiling may be increased.

In addition, the TSSC will be requested to define specific work scope, approximate schedule, and best-estimate of cost for each element. The final document shall also define skill-level criteria and estimated cost range for each skill level. It further shall identify the percentage of time each resource is estimated to apply to each work element. The result will be a classic project management scope/schedule/cost triangle.

Additionally, the TSSC will be requested to capture costs at the work-element level, through an easy-to-use infrastructure tool such as the existing HEAT call-management tool. The goal will be to capture work-element costs on a weekly basis, to support work-breakdown and performance-assessment objectives.

A. Planning and Development Task

1) DOI/ESN and USGS Collaboration

- a) Support architecture definition and local implementation considerations in migrating to Trusted Internet Connection (TIC) Access Point configuration
 - i) Support DOI/ESN and USGS/Geonet discussions regarding EROS network capacity planning and TIC architecture / requirements
 - ii) Document DOI/USGS/EROS agreed-to architecture and internal / external network user impacts
 - iii) Document local developmental and long-term operational costs as a consequence of the new network architecture
 - iv) Support the NSM in preparation of briefing documents regarding TIC alternatives and impacts
- b) Support documentation required by USGS GIO to satisfy Certification and Accreditation of IT computing resources at EROS

2) Security

- a) Complete the configuration and project-by-project roll-out of the Barracuda NetContinuum security appliance. The NetContinuum is a required security-enhancing appliance that acts as a reverse-proxy server to provide a layer of intrusion protection for all public-facing web servers (part of EROS' Public Access subnet). Work with Central Region GIO to coordinate proxy addresses and overall appliance management (configuration solely managed by Central Region GIO).
 - i) Ensure testing of configuration, stability, and performance for each project connected to through the NetContinuum. Coordinate and install the appliance in line with the identified public-facing servers. Work with the Regional SPOC to configure the appliance for EROS' environment & Level3 load-leveling proxy service
 - ii) Conduct thorough testing with the identified suite of project servers. Evaluate and document adverse or unanticipated results, such as constrained throughput. Test Level3 server IP failover by manually triggering a non-conformal event
 - iii) Document and resolve, if required, any non-conformances or throughput restrictions
 - iv) Transition to a fully operational status and support discussions with Regional SPOC
- b) Enhance LAN Intrusion Detection/Protection capability (ISG-2000)
 - i) Prepare an implementation plan, including schedule, configuration, risk management approach, communication plan, and test plan
 - ii) Initially, install components in spare firewall on test network. Configure (or download) intrusion pattern detection algorithms. Test intrusion detection performance, and document anomalous results
 - iii) Test intrusion protection performance impact on LAN throughput

- iv) When conformal, install, configure, and test as part of the operational network. Correct any failure conditions and retest
- v) Document final architecture. Document benefits that accrue from identification and blocking of malware, SQL injection, or other network-penetration exploits

3) Modernization

- a) Assess existing wireless internal and visitor connectivity
 - i) Document and present limitations/drawbacks of current internal (trusted) and visitor wireless access, security, and management capabilities. Document maintainability and performance issues
 - ii) Propose improved approach to mitigate existing constraints/inefficiencies
 - iii) Evaluate and propose at least two alternate solutions for wireless Access Points
 - iv) Install, test, and characterize all aspects of the candidate APs. Recommend optimal solution, document advantages, and provide final proposed architecture of new AP web for both internal and visitor networks
 - v) Support any user connectivity configuration changes required by new APs

- b) Implement if required any augmentations or enhancements to the new Remote Access Control Virtual Private Network (VPN) Juniper SA4500 appliance
 - i) Identify shortcoming(s), propose remediation, estimate cost and schedule consequence of proposed augmentation
 - ii) Implement, test, and report on approved change(s)
 - iii) Prepare additional training materials required and support roll-out of the VPN capability

- c) Replace current network-management applications server (pending availability of funds for hardware procurement)
 - i) Receive, install, configure, and verify functionality and performance of hardware
 - ii) Install, configure, and test migrated application software
 - iii) Demonstrate reliable functioning of all migrated software applications and release to operations

- d) Upgrade Visitor Network Firewall (Gateway) (Juniper SSG-20)
 - i) Document an implementation plan, device management plan, and schedule
 - ii) Receive and install the Gateway; configure and test performance
 - iii) Document test results and upon approval release to operations

- e) Replace Server-Management Network Firewall (Juniper SSG-20)
 - i) Document an implementation plan, device management plan, and schedule
 - ii) Receive and install the Gateway; configure and test performance

- iii) Document test results and upon approval release to operations
- f) Replace Extreme Alpine Office Automation Network switch with Extreme Black Diamond
 - i) Prepare implementation plan, test plan, and schedule
 - ii) Receive, install, and test Black Diamond switch on test network. Document satisfactory operation and performance, or issues as encountered
 - iii) Upon approval, install, configure, and test switch in the operational network
 - iv) Report implementation status
- g) Update the three-year plan in the fourth fiscal quarter, prior to the start of the next FY.
 - i) Ensure that all device interfaces and configurations have been properly updated from the prior quarter's Change Management and Configuration Management activities. Summarize where appropriate major architectural or configuration changes in LAN, WAN, Security, or Remote Access for input to the Task manager
 - ii) Summarize traffic volumes by project and WAN component for the prior four quarters. Identify potential bottlenecks or network performance constraints which may emerge in the subsequent FY
 - iii) Identify LAN components recommended as candidates for modernization, enhancement, or upgrade in the subsequent FY. Identify ROM costs for modernized/ enhanced/ or upgraded equipment, maintenance, and labor
 - iv) Recommend increases or decreases in maintenance support levels or coverage for LAN devices
 - v) Recommend reductions or deletions of communications services based on usage levels or technology obsolescence
 - vi) Recommend (and justify) augmentation or enhancement of the network architecture, based on traffic volumes across the subnetworks or other factors. Identify ROM costs for reconfiguration and/or enhancement, and estimate savings if any from the reconfiguration or augmentation. Identify increased network traffic volume headroom resulting from the reconfiguration or augmentation
 - vii) Recommend changes to the security hardware, monitoring software, or operational mitigation processes to improve and harden the Center's security profile.
 - viii) Document successful intrusions or service attacks on the Center's network through malware or coordinated external threats. Document lessons learned and revised operational procedures implemented to block or thwart future intrusions
 - ix) Include in the Plan update, as appropriate, diagrams, graphs, and charts to visually augment the statistical data and descriptions

4) Enhancement

- a) Propose benefits/drawbacks, operational procedures, and estimated initial and operational costs to expand the current Network Management network to control all switches, routers, firewalls, intrusion protection devices, and other configurable appliances outside the operational LAN (i.e., via an out-of-band management network)
 - i) Document configuration, management approach, implementation schedule and cost, operational concept, security plan, and long-term operational cost for a multi-year implementation
 - ii) Upon request, submit an implementation plan and schedule for each logical phase of the network implementation
 - iii) Upon approval, configure and connect the controlled network devices via the out-of-band management network. Document functional capabilities
 - iv) Document annual (or more frequent) management audit procedures to ensure operational security and adherence to management standard procedures
 - v) Revise architectural drawings per standard CM practices

- b) Assess and document benefits/drawbacks of an Infrastructure-based network-device-configuration event-logging capability (e.g., a LogLogic-type appliance) that would monitor configuration changes to switches, firewalls, routers, and similar devices
 - i) Define the scope, schedule, and cost of the proposed beneficial change-logging functionality and the corresponding management practices proposed. Identify both initial installation as well as extended operational costs
 - ii) Iteratively, refine the scope of the change-monitoring function to an economical and managerial beneficial level
 - iii) Develop and document an operations concept for management of the logging function. Define security procedures and anomaly alarm pathways
 - iv) Prepare and submit an Implementation Plan including procurement plan and implementation plan, defining schedule, configuration, risk management approach, communication plan, and test plan
 - v) Upon approval of the implementation plan, install, connect, configure, and test the logging appliance with associated network devices. Demonstrate anomaly detection of the logging appliance.
 - vi) Upon approval, deliver to operations

- c) Migrate current spreadsheet-based IP assignment information and procedures to a database solution
 - i) Evaluate competitive commercial solutions and recommend best-practice IP tracking software
 - ii) Upon delivery, receive, install, and configure the database
 - iii) Migrate the existing IP information to the database
 - iv) Document standard IP-management procedures required for the new capability

- v) Upon approval, transition to operations
- d) Enhance current network volume and user-project traffic monitoring and statistics collection
 - i) Implement the Traffic Sentinel monitoring and diagnostic toolset on a high-performance Linux server (traffic-characterization server) (as available)
 - ii) Identify and document operational modes, anomaly detection capabilities, enhanced traffic monitoring functionality
 - iii) Document standard operational configurations, standard reports, typical monitoring applications
 - iv) Determine anomaly detection procedures that can be applied operationally and document
 - v) Transition the tool to operations
- e) Improve wireless monitoring and optimization (i.e., apply Fluke wireless toolset)
 - i) Assess need for Fluke wireless software suite given the plan to upgrade AP architecture and management
 - ii) If approved, prepare implementation plan for installation, configuration, and application of software suite to assess wireless AP connectivity, range, reliability, interference, and other operational parameters
 - iii) Assess operational parameters of newly installed APs
 - iv) Use results of assessment to adjust configuration and location of AP modules to optimize internal and visitor connectivity and reliability via wireless
 - v) Document use of the wireless assessment suite in an operational environment
- f) DHCP Server software replacement
 - i) Document requirement (if any) to adopt new security procedures as part of hacker-hardened Domain Name Service software (DNSSEC initiative)
 - ii) Identify approved DHCP software. Upon delivery, install DNSSEC server software on a test server.
 - iii) Document an implementation plan, identifying approach, schedule, and cost
 - iv) Upon software delivery, install and configure test DNS server in test network
 - v) Conduct DNSSEC test procedures to demonstrate performance compliant to specifications
 - vi) When approved, integrate DNSSEC software on existing DNS servers and transition to operations. Monitor results
 - vii) Document compliant DNSSEC performance, mitigate issues where possible, and report issues

- g) Complete link aggregation of the Juniper ISG-2000 backbone firewalls with the backbone switch 'BB2'. Measure backbone data transfer rates to validate performance increase to approximately 1.7 Mbps.
 - i) If not completed, update network architecture diagrams, identifying switches and networks that were link-aggregated (or trunked)
 - ii) Document perceived benefits of link aggregation. Operationally monitor the backbone throughput headroom and notify Network Task manager when headroom routinely diminishes to less than 25% of demonstrated throughput (or data rates increase to 1,275 megabits per second sustained)
 - iii) Document mitigation actions to be employed operationally if a problem arises on the link-aggregated backbone

5) Collaboration

- a) Contribute to and support planning to better utilize the Research, Education, and Economic Development (REED) Network, which has the potential to provide I2 and NLR connectivity via an alternate path to the StarLight circuit to Chicago for connection to NISM and I2/NLR
 - i) Participate in technical exchange telecons among USD, SDSU, DSU, BIT, and BOR
 - ii) Document potential cost and service benefits of expanding existing WAN circuits to I2 via REED, in a 2-5 year timeframe
 - iii) Include REED documentation as part of the Network Three-Year Plan

6) Technology Investigation

- a) Investigate and document alternatives to existing 622-Mbps StarLight circuit to Chicago, which may no longer be primarily NASA-funded post-FY11.
 - i) Characterize traffic volumes on all WAN segments and LAN trunks and project the growth for two years. Document available headroom or throughput constraints for projects using the WAN segments
 - ii) Document history, current status, two-year projected headroom/constraint, and provide recommended approach or solution for impacted projects, in particular the LP DAAC.
- b) Update the results and conclusions of the technology investigation conducted in FY09 regarding the benefits and costs of installation and operation of an intrusion detection & protection device such as the Fore Scout CounterACT Edge.

7) Technical Support

- a) Provide technical support in selected external meetings and/or selected conferences
 - i) Annually attend two technical interchange meetings (DOI/USGS or equivalent) and two network consortium conferences during the FY.
 - ii) Support agenda preparation and general meeting planning as applicable
 - iii) Support documentation of meeting summaries, actions, and technical recommendations which may have resulted from the meetings or conferences

- b) Provide technical support for local meetings
 - i) Support discussions of technical approach, architecture, equipment, cooperative agreements, political considerations, and other topics which may be needed to aid decision-making by the Task manager. Assume two such meetings per month
 - ii) Support briefings to Branch/Division/Center management or USGS/DOI as required. Assume four such briefings per year
 - iii) Support Regional, HQ USGS or DOI visitor agenda preparation, technical meeting support, and results documentation. Assume two such meetings per year

- c) Provide technical support for *ad hoc* activities identified during the course of the contract year
 - i) Activities may involve WAN or LAN, planning or development, and may include discussions and meetings with Bureau, Department, and/or external cooperators
 - ii) Scope of the activities will be identified at the time of request Support Regional, HQ USGS or DOI visitor agenda preparation, technical meeting support, and results documentation. Assume two such meetings per year
 - iii) Support requests shall be assessed by TSSC management for priority relative to on-going scheduled activities, and with this knowledge the request shall be accommodated as directed by the Task manager. This effort is estimated to not exceed 120 hrs during the contract year, and no more than 20 hours will be requested in any one month

8) Management

- a) Document task accomplishments and status of issues, investigations, reports, action items, telecons, and other contacts
 - i) Maintain a (shared) activity list and schedule with stoplight status by identified tasks. Identify causes for activities lagging plan (schedule). Update status weekly
 - ii) Document accomplishments and status weekly, as of the close of Wednesday
 - iii) Document monthly the month's accomplishments and status, plus a rolling three-month overview of future plans. Identify concerns, risks, and mitigation of identified risks. Identify recurring problem areas and mitigation/action plan. Provide a formal remediation plan for any major activity behind schedule by more than two weeks.
 - iv) Support one weekly management planning meeting and one technical status meeting with the Network Task Lead (100 total). Provide account financial report monthly, NLT the 15th of the month. The financial data shall include plan by month, actual by completed month, estimate to complete to FY, and estimate at complete of FY. Provide the same data for the contract year. Identify variance for month, YTD, and EAC. Provide an explanation for and mitigation for any variance exceeding 3%

for the month. Provide an action plan for any variance exceeding 5% of EAC.

- b) Track actual labor hours expended weekly by work-breakdown element
 - i) Provide weekly summaries monthly for all active (uncompleted) elements
 - ii) Use a government-provided database tool (notionally the same tool as used to enter and track Help Desk support calls) to capture hours by skill category using dropdown selection boxes for activities arranged in a hierarchical tree.
 - iii) Review the labor summaries monthly with the Task manager and provide explanations for high or low levels of effort relative to the scheduled hours.

B. LAN Operations and Maintenance (O&M) Task

1) Infrastructure LAN Operations and Maintenance

- a) Manage and maintain network infrastructure components, including backbone switches, firewalls, VPN concentrators, wireless access points, and traffic monitoring software
 - i) Accept assigned Network Services calls from Help Desk personnel and resolve questions or issues associated with wired or wireless local-area network or Virtual Private Network connectivity or data transfer. Conduct fault identification and repair.
 - ii) Manage and maintain internal web-based network statistical & graphical monitoring and display pages. Maintain a web-based real-time display of data volume at key points on the LAN, as well as an aggregation of this data into historical graphs depicting one-day, one-week, one-month, and one-year timeframes. Key points should include the public-access sub-net, office automation sub-net, R&D sub-net; and the three project sub-nets. Maintain traffic data statistics for a period of 3 years.
 - iii) Provide to the Network Task manager monthly statistics of data volume on the four WANs, categorized by the project originating or receiving the data.
 - iv) Maintain sufficient field-replaceable spare parts to replace all single-point-of-failure components and interface boards, as identified in a key-components list prepared and maintained by TSSC staff
 - v) Administer Firewall rules as required for approved user requests for access to infrastructure (non-project) components. Document actions on change requests. Maintain a current record of Firewall rules as well as a change record extending to the beginning of the prior fiscal year
 - vi) Investigate, document, and support firewall Incident Responses, where an attempt to breach an infrastructure firewall succeeded or failed
 - vii) Maintain a capability to automatically and continuously monitor key LAN components, using commercial applications to poll key network components periodically to detect non-responsive components and to auto-generate personnel alerts
 - viii) Maintain knowledge requisite to utilize the USGS Level3-contract load-balancing proxy server for appropriate infrastructure EROS servers. Directly charge to applicable projects all support services provided on a per-project basis
 - ix) Manage Linux and Windows servers that host key monitoring and security software. These servers may include applications such as Network Chemistry, EpiCenter, WhatsUp, NetFlow, SFlow, Traffic Sentinel, DNS, DHCP, and IP assignment management. Ensure relevant data is backed up on-site weekly
 - x) Ensure staff remains trained, competent, and cross-trained to configure, diagnose, and repair LAN network faults as well as infrastructure

hardware or software, such as switches, firewalls, IDP components and appliances, etc.

- xi) Maintain LAN backbone components (switches, firewalls, intrusion detection appliances, DNS servers, etc.) plus spares such that LAN availability (connectivity) is 99.85%, which allows an average of 1 hr of unscheduled backbone downtime per month. Maintain downstream devices (closet switches, etc) to achieve 99.7% per month, or 2 hrs unscheduled sub-network (PA, OA, Dev/Prod) downtime per month

- b) Document the network configuration, including identification of all components and interconnecting cables to at least the following levels of detail:
 - i) Maintain Visio circuit diagrams of the LAN architecture at a minimum of three levels of detail, from a high-level overview down to individual network components and servers interfacing to multiple similar distribution components. Begin one level below the ESN architecture level
 - ii) In cooperation with the Facilities contractor (currently DCT), maintain a spreadsheet or other document correlating cable interconnects with specific ports of hardware components and punch-down jack. Label endpoints of interconnecting cables

- c) Maintain a Network Management network as a separate but integral component of the LAN
 - i) Maintain user names and passwords or encryption key techniques to ensure management-network access only by authorized users. Employ strict security processes to control, monitor, and log individual activities to accomplish device configuration/control
 - ii) Update network architecture and wiring diagrams as additions or changes are made to the Network Management network devices, as part of normal CM practices

2) WAN Operations and Maintenance

- a) Manage and maintain network infrastructure components, including routers, monitoring devices, security devices, and as required circuits associated with networks provided by Enterprise Services Network (ESN), USGS (GeoNet3) (StarLight Optical Network), and the South Dakota University System Research, Education, and Economic Development Network (REED)
 - i) Support with Network Task manager approval action requests from DOI ESN, Verizon Business Network Operations & Security Center (NOSC), HQ GIO, Regional GIO, NASA Integrated Services Network (NISN), or NASA Goddard Space Flight Center EOS Core System (ECS) network engineering or security POCs involved in investigating or resolving router operability or network connectivity failure or issues; security equipment or incidents; loss of DNS functionality; or, circuit degradation or less associated with the physical wide-area networks. Support is expected to

- consist of approximately 12 requests occurring during the year with an average staff allocation of 3 hrs per request
- ii) Resolve reported connectivity or security issues associated with POC requests noted in paragraph a) i) above, or escalate unresolved issues to the respective impacted vendor/cooperator higher-level support group. Document action/date/resolution, and convey updates involving problem resolution to the Network Task manager as available
 - iii) Participate in REED engineering coordination telecons. Allocate approximately 1 hr per month for telecon participation
 - iv) Participate in DOI ESN weekly network status telecons currently occurring at 9:00 a.m. every Thursday. Convey news or actions from the telecon to the Network Task manager. Allocate 1 hr per week for telecon participation
 - v) Maintain architectural drawings and other documents as modifications are made to WAN architecture or devices. Document network devices, configuration, and connectivity of all monitoring and intrusion protection appliances connected to the EROS network edge that are operated and maintained by other entities, such as ESN or GeoNet3. Include this documentation as a component of the overall LAN configuration and connectivity documentation package
 - vi) As a one-time activity for FY10 only, document the responsibilities, skill categories, levels of effort, and non-prime hours required to support WAN component failure debug and repair, component reconfiguration, POC communications, network vendor communications, and other efforts required to support uninterrupted WAN connectivity. Document these items based on recollection of FY09 activities

3) Operational Security

- a) Provide operational security monitoring of LAN traffic, through adherence to industry best-practices in regards to firewall rules, DHCP spoofing, IP address and network-topology protection, and other defensive procedures
 - i) Remediate identified vulnerabilities arising from monthly ITSOT security scans
 - ii) Provide coordination and liaison for security issues associated with DOI and USGS special security devices, such as the Einstein Box, NetContinuum, Ninja2000, etc.
 - iii) Maintain network security devices in coordination with and support of ESN or USGS security or network personnel. Devices may include firewalls, proxy or reverse-proxy servers, IP logging servers, and intrusion-detection/protection appliances. Supported personnel may include the ITSOT, Regional SPOCs, DOI ESN operations manager, Bureau GeoNet3 manager, and the Verizon GNOSC, as approved by the Network Task Lead
 - iv) Provide operational technical support to external network security personnel on an approved ad hoc basis. Support is expected to consist

of 12 requests spread evenly over the year, with each request requiring approximately 2 hours to close.

- v) Detect nefarious attempts to penetrate the firewalls; add offending IP addresses to a database of annoyances for temporary or permanent blocking. For estimating purposes, assume 12 additions per year to the annoyances database.
 - vi) Develop and maintain a tabulation of DOI, USGS, and EROS operational network security events/intrusions/attacks. For estimating purposes, assume a total of 100 various “events” per year.
 - vii) Coordinate with the Enterprise Security Task to ensure that the appropriate network- connection approval documentation (e.g., MOUs, MOAs, and ISAs) is in place prior to connecting any external system or component to the Enterprise network by projects supporting external cooperators or customers.
 - viii) Provide coordination and technical support to network task lead for *ad hoc* security-related events, external inquiries, or network appliance issues (maximum 2 hrs/month)
- b) Manage firewall rules periodically through an approved configured process
- i) Update firewall rules by implementing new rules, as requested by users and projects through the Help Desk
 - ii) Maintain a database of firewall rules by device, together with a change log as part of standard CM processes
 - iii) Update firewall rules as required to maintain LAN and WAN security, according to USGS Perimeter Security Standard, USGS Security Handbook (PHB), or applicable DOI/USGS directive
 - iv) Monitor source and destination IP addresses for all network traffic. Maintain a log of all IP traffic for a period of one year
 - v) If requested by the Network Task manager, retrieve and provide IP logs for selected time periods. Plan to fulfill two IP log requests during the FY
 - vi) Provide support for IP-related questions or issues for infrastructure components as requested through the Help Desk.

4) DNS/DHCP/IP Management

- a) Manage Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) servers (or appliances) and naming functions for all Center devices requiring Internet Protocol (IP) services.
 - i) Administer and maintain a database of IP address assignments by computer or network device as additions, changes, and replacements occur
 - ii) Periodically (as required) provide the Help Desk with blocks of IP addresses as new servers, desktops, or laptops are added to the local network. Assume quarterly delivery of blocks of available IP addresses
 - iii) Provide support for DHCP, DNS, and IP-related questions or issues for infrastructure components as requested through the Help Desk

5) Network Access

- a) Provide Virtual Private Network (VPN) connectivity and security group management.
 - i) Administer specific VPN groups by project or user group to enhance network security, for both the current VPN Concentrator and future VPN implementation if applicable
 - ii) Support investigation and resolution of user Help requests

- b) Manage and maintain a trusted wireless network connected to the LAN, with access points in an approved configuration. Manage and maintain a wireless visitor's network isolated from the trusted internal network and connected to a separate 15-Mbps Internet connection.
 - i) Resolve Network Service Calls from EROS/Department/Bureau users and non-affiliated users experiencing configuration or connectivity problems perceived to be associated with the wireless network
 - ii) Document procedures and manage operational security for the wireless networks. Measure and document trusted and visitor AP reception circles annually for each AP

6) Management

- a) Support Configuration and Change Management (CM) process
 - i) Review Configuration Change Requests (CCRs) for need, feasibility, urgency, compatibility, risk, and scope under an Engineering Configuration Control Board (ECCB). Propose disposition of major requests to a Task Configuration Control Board (TCCB). Dispose minor and routine CCRs directly in ECCB.
 - ii) Support review and disposition of CCRs considered by the TCCB with staff having appropriate technical expertise
 - iii) Support maintenance of a CM database with results of ECCB and TCCB

- b) Support review and improvement of various existing user forms related to network access.
 - i) Forms will include at least the following: VPN access; system access (firewall rule) change; wireless trusted access; and wireless visitor access
 - ii) New forms will be web-based or PDF user-fillable forms, designed to be signed and archived electronically and without scanning
 - iii) Forms approach will be coordinated with the Desktop Services Task

- c) Support a process to annually inventory and to excess obsolete equipment
 - i) Leverage Desktop excess procedures to document steps to promptly transfer obsolete equipment to the appropriate depot. Plan to excess approximately two hardware device per month spread over a year [24]
 - ii) Scan Excess Property lists from civil government installations to determine if suitable non-end-of-life equipment can be obtained by transfer rather than procurement. Department of Energy centers and

laboratories may be sources of powerful but locally insufficient switches, firewalls, etc.

- d) Document accomplishments and status of issues, investigations, reports, action items, telecons, other contacts for the current year
 - i) Document maintenance activity schedule and status weekly by identified tasks. Document completion LOE against estimated LOE where such metrics apply
 - ii) If it is determined that the Desktop Services Manager is not able to provide usage statistics via Help Desk activity logs, separately provide a summary of category, task, and frequency of the network support tasks for the month. The list should include user-support requests, configuration change requests, and infrastructure maintenance – schedule and unscheduled. Other categories may be appropriate, TBR during iteration of the Work Commitment
 - iii) Support, TBD, 1-hr monthly meetings with project representatives to vet support, security, procedure, data volume, or other relevant topics that require user input to resolve
 - iv) Document and interactively review task accomplishments, task status, unresolved issues, monthly and YTD budget, and other pertinent information
 - v) Ensure standard procedure documents have been written for appropriate processes and are available for operations staff reference and review

III. Enterprise Architecture, Technology, & Investigations

Scope

This task supports the Center's efforts to define and implement a formal, Center-level configuration management process and to initiate the process of formalizing architecture principles and guidelines for future systems. The technology investigation portion of the task provides analysis and recommendations for common technologies within the EROS enterprise systems architecture.

Specific Areas of Work and Deliverables

- Overall CM and EA task coordination assistance
 - Once weekly (one hour) CM EA planning sessions with Task Manager
 - Documentation of discussions and maintenance of an action list for the Task Manager
 - Help draft task plans and estimate schedules and level of effort for various tasks
 - Facilitate communication with TSSC engineers
- Enterprise CM Process Execution and Enhancement
 - Review and comment from a TSSC project engineering perspective
 - Two drafts of an EROS CM Implementation Plan identifying steps and schedule for the rollout review and implementation
 - Two drafts of an EROS CM Policy Document documenting the roles and responsibilities and processes of CM at EROS including levels of change needing review and approval
 - Assistance with the gathering of information to draft, finalize and then maintain a list of "systems" at EROS to be formally configured
 - Assistance with drafting requirements for, gathering and maintaining configured system baseline artifacts, e.g.,
 - Architecture/design diagram(s) of current system
 - Lists of hardware and software components employed
 - Operations Concept documentation
 - Interfaces (e.g. ICDs, SLAs, critical dependencies)
 - Operate a CM Repository and plan for future enhancement
 - To maintain baseline configuration artifacts
 - To track changes and review/approval artifacts
 - To maintain architectural and technical guidelines
 - Keep it simple for initial implementation (using available tools and minimal processes)
 - Gather lessons learned, generate requirements for, and investigate COTS tools that are good candidates for enhanced automation of repository
- Enterprise Architecture Guidelines and Strategies Support
 - Facilitate two ½ day workshops to develop draft guidelines for two sub-architecture areas such as:
 - SOA Implementation
 - Information Access and Web Services

- Storage (near line and online)
 - In preparation for each workshop:
 - Gather inputs from FY08 and FY09 architecture sharing sessions among projects
 - Draft common threads of vision and guidelines
 - Review with Task Manager
 - Update Draft for review with Projects
 - Conduct workshops with Projects to review, enhance and finalize guidelines
 - Document final guidelines for formal review and approval and store in CM Repository
- Technology Investigations
 - Lead and conduct two technology investigations. Examples are:
 - Blade servers
 - Cloud computing
 - The primary purpose of each investigation is to explore the maturity of the technology and its feasibility for use, and rough estimate of cost involved, for one or more Projects at EROS to employ the technology
 - At a minimum, the investigations should answer the following questions
 - What kinds of applications does the technology seem most suited to?
 - If not yet mature enough for operations, what weaknesses does it have and what would seem to need to be overcome to make it mature enough for routine operations?
 - What are the lifecycle costs associated with development and initial installation and a nominal period of operations and maintenance?
 - Document findings, submit for review and comment by Task Manager and Projects, update as appropriate, and finalize and place in CM Repository.

IV. IT Security Policy, Coordination & Monitoring

Scope

The IT Security Management task objective is to provide technical expertise to the EROS IT Security Officer in day-to-day activities involving all aspects of EROS IT Security Management and Communications.

Specific Areas of Work and Deliverables

- Provide project management, technical expertise, planning, monitoring, technology support, and vulnerability assessment to maintain and enhance confidentiality, integrity and availability of EROS computing and data resources within the EROS IT Security Framework.
- Test and implement AppDetective data base vulnerability assessment tool. Assess and report infrastructure vulnerabilities for the E&IT Enterprise IT and IT Security data bases. Assimilate and report results of all data base vulnerability scans at EROS to the IT Security Officer. The IT Security Officer or a designee will forward the report to the HQ IT Security Office.
- Coordinate USGS EROS Plans of Actions and Milestones remediation management with Project Chiefs, Work Managers and IT Security Technical Points of Contact (STPOCs).
- Coordinate monthly vulnerability scan remediation with Project STPOCs.
- Test and implement port vulnerability scanning capabilities for IP addresses inside the EROS Firewall. Perform vulnerability scanning and problem mitigation for IP addresses for Enterprise IT and IT Security servers on a monthly basis. It is assumed DSS will provide vulnerability scanning and mitigation for desktop IP addresses. Assimilate results of all project IP address scanning activities on a monthly basis. Review consecutive scan results to determine if vulnerability mitigations are being performed. Deliver a report of those vulnerabilities appearing for the same IP address for two consecutive months to the IT Security Officer. The IT Security Officer or a designee will forward the results of each monthly compiled scan to the HQ IT Security Office.
- Promote EROS IT Security Awareness.
 - Communicate to raise the awareness of EROS staff on IT Security topics relevant to EROS computing environment, resources, and data archive.
 - Communicate IT Security technology advancements and IT Security risks occurring on the Internet.
 - Communicate long-term EROS IT Security strategies.
- Periodically review Firewall Review Board requests for access and openings for conformance to USGS Perimeter Security Standard and Policy.
- Assist and support EROS staff and EROS projects with individual IT Security responsibilities and IT Security best practices in a responsive and timely manner.
- Lead EROS IT Security Working Group and inform EROS IT Security Manager of major plans and issues in regards to overall EROS IT Security.
- Lead EROS IT Security incident response and investigation, in-depth analysis as necessary of logs for routers, firewalls, intrusion detection, tripwire, and system.

- Participate as a technical expert in IT Security related audits or visits that occur at EROS.
- Actively monitor all components of EROS IT Security and investigate abnormalities.
- Review and assess the firewall, operating systems, applications, database and physical IT Security using vulnerability assessment and intrusion detection tools and techniques.
- Participate in USGS Bureau IT Security Manager (BITSM) activities:
 - EROS Security Point of Contact and IT Security focal point.
 - Adherence to USGS IT Security reporting requirements.
 - DOI and USGS IT Security Policy and Standards expertise.
 - USGS EROS Plans of Actions and Milestones reporting.
 - USGS EROS coordination and reporting for OIG, DOI, and USGS vulnerability assessment scanning and penetration testing.
 - USGS C&A Automation and Streamlining Team participation.
- Gather information the IT Security Officer in response to USGS IT Security related data calls from HQ or CR Geospatial Information Office (GIO).
- Participate on IT Security Steering Committee (ITSSC) Security Working Group (SWG) which oversees IT security policy formulation throughout the USGS. Specific activities will include but are not limited to:
 - Assure representation of EROS on the ITSSC SWG with guidance as directed by the EROS IT Security Officer vetting IT Security policies, guidelines, and directives.
 - Review and provide feedback on numerous DOI draft policies in multiple versions as directed/approved by the EROS IT Security Officer.
- Coordinate migration of the EROS IT Security Tracking Tool from SQL to a modern database architecture.
- Assess and propose hardware efficiencies regarding IT Security servers and associated hardware.

V. Enterprise IT Services

Scope

Enterprise IT Services involve those activities that provide broad, general tools and services to the Projects and staff of the Center that are not easily or readily distributable directly to Projects but are of common need. Examples of these kinds of services include enterprise server and database maintenance, offsite tape storage support, assistance with the maintenance of enterprise COTS licenses, and computer room coordination and monitoring.

Specific Work Areas and Deliverables

Database Updates and Maintenance

- Provide database updates and maintenance support including maintaining and monitoring logs, responding to security vulnerabilities resulting from internal and external scans, and monitoring and applying database system patches. All tasks are done with approval of the work sponsor before applying. This support is specifically required for the following databases:

‘igskmncngs118’

‘util’

‘utild’

‘igskmncngs079’

Offsite tape storage

- Provide technical support for the maintenance of an offsite tape storage facility. Since labor for generating, transporting, and retrieving offsite tapes are to be charged directly to EROS Projects as part of their backup or offsite archive storage support, this support activity is primarily limited to the support and maintenance of the tape storage inventory system.

IT-related Web Forms

- Support for the maintenance of EROS IT-related web forms on the internal web pages that are not specifically related to Desktop Services, Network Services, or IT Security. This includes the following forms:
 - COTS Software Request
 - EROS Anonymous FTP Access Request
 - System Access Request

CR1-CR2-CR3 Coordination and Room Maintenance

- This activity involves support for conducting regular computer room coordination meetings. This also involves monitoring physical temperature and humidity levels and reporting issues and the monitoring of needed room supplies such as generic media labels and entrance floor mats. Also included is coordination of planning activities to assist with facilities power and heating/cooling issues in the computer rooms.

Server Assessment, Maintenance, and Backup

- Provide systems administration, hardware maintenance, and system backup support for the following enterprise servers:
 - IGSKMNCNDC501 Virtual - Domain Controller DMZ (Virtual Server)

- IGSKMNCNDC500 Domain Controller DMZ
 - IGSKMNCNFS101 File storage for Acronis Images/Backups
 - IGSKMNCNGS010 Windows ArcServe Backup Software
 - IGSKMNCNGS132 Virtual Machine Host (vm009, 10, 20, 59, 100, GS107)
 - IGSKMNCNGS072 Host to Acronis File storage, administration server.
 - IGSKMNCNGS079 Windows Log Server
 - IGSKMNCNGS118 Sharepoint Server - Documentation storage for all E&IT
 - IGSKMNCNGS120 Terminal Server
 - IGSKMNCNGS516 DMZ DC01 Virtuals
 - IGSKMNCNVM000 Virtual - Reserved for Master OS Install
 - IGSKMNCNVM020 Virtual - GS Domain - WSUS Server patching
 - IGSKMNCNVM500 Virtual - EROS Domain - Remote login for password changes/administration
 - IGSKMNCNVM501 Virtual - EROS Domain - Symantec/Group Policy/Administration
 - IGSKMNCNVM502 Virtual - EROS Domain - WSUS Server patching
 - edclxs50 Test system for operating systems
 - edclxs69 Test system for data base administration
 - edclxs71 Linux - EROS Anonymous FTP - EDCFTP
 - edcsgeng Unix SG Engineer System (viable until SGS20 is gone)
 - edcsgs20 Unix Shared Server (planning for removal)
 - nces001 Unix Log Management
 - edclks1 Linux image server, Unix printing
 - edcsns1 Unix Shared Server, primary DNS
 - edcsns2 Unix - Backup DNS, label printing services
 - edcsns6 Unix COTS License server, Legato Networker
 - IGSKMNCNGS123 WebInspect Server
 - IGSKMNCNGS165 Host server for Foundstone and Teneble
 - IGSKMNCNVM046 Virtual server for Foundstone software
 - IGSKMKNCNVM047 Virtual server for Teneble software
- Assess and propose hardware efficiencies regarding Enterprise IT servers and associated hardware.
 - Assess and propose efficiencies/upgrades in the Windows Server Backup process.

Enterprise COTS package support

- Provide assistance and support with the maintenance of enterprise COTS packages in the following areas:
 - Assist the government sponsor with the annual renewal scheduling, procurement package preparation, and update tracking of COTS software and various minor supplies renewals and purchases.

- Provide COTS software administration, patch update and maintenance support, user notification, usage tracking, and vendor troubleshooting interface support for SPLUS, EXCEED, GO-GLOBAL, ENVI/IDL, ERDAS IMAGINE, and ESRI ARCGIS

Bureau Technical Support Team Participation

- Support EROS participation in both the USGS Bureau Windows Technical Support Team (BWTST) and the Bureau UNIX Technical Support Team (BUTST) meetings by sitting in via telecom and once a year in person on the respective regular meetings of the BWTST and the BUTST. Within three working days following each meeting, provide a written meeting summary including technical observations and recommendations regarding the discussions to the government work sponsor. Forward copies of all emails received from TST members or leaders to the government work sponsor and seek guidance from the government work sponsor before replying to any requests for information or commitment of action.

VI. USGS ITSOT Support

Scope

The ITSOT support subtask provides the local operational support for the USGS ITSO activities carried out by EROS staff. The EROS IT Security Officer approves all tasking and reporting.

Specific Areas of Work and Deliverables

- USGS Computer Security Incident Response Team (CSIRT).
 - Acts as the EROS point-of-contact to the USGS CSIRT incident manager in the classification, correction and reporting of security incidents.
 - Reports IT security events and incidents to the USGS CSIRT or the Department of Interior Computer Security Incident Response Center (DOICIRC).
 - Facilitates incident response and investigation, in-depth analysis as necessary of logs for routers, firewalls, intrusion detection, tripwire, and system logging.
- ITSOT Security Point of Contact.
 - Acts as the ITSOT EROS Point of Contact, and routinely distributes incident and security issues to IT security, desktop services and network services managers. Within three days provide a report of any observations or technical evaluations of significant issues.
 - Participate in the EROS common controls for the C&A process.
 - Participate in setting up EROS Patch Control System as needed reporting to the HQ Enterprise Patch Control System.