



USAID-Funded Economic Governance II Project

Phase II SSN Application Rollout Plan V 1.8

DATE: JANUARY 26, 2009



Revision History

Version	Revision Date	Summary of Changes	Modified by
1.9	Feb. 11, 2009	<ul style="list-style-type: none"> • Addition of revision history • Changes to target deployment completion from Feb. 2009 to Mar. 2009. Changes made throughout the document. • Target logical environment diagram was changed to reflect changes to the MoLSA – Baghdad Pilot Internet connection. Baghdad Pilot no longer will have its own dedicated Internet connection. Instead it will share MoLSA HQ’s connection via a wireless connection. • Removed - “The current Phase I data has to be migrated between the two versions. This will require database scripts to be written and tested. It has been estimated that the development and testing of the scripts could take up to 2 months to complete. This timeline did not fit with the committed system deployment for having 2 support sites completed by the end of the year. It was therefore decided that the deployment would proceed and the Phase I to Phase II data migration would occur as a separate deployment.” Phase I to phase II data migration is no longer required. Data will be imported from Access instead. 	Mark Hoy

Phase II SSN Application Rollout Plan

TABLE OF CONTENTS

IMPLEMENTATION ROLLOUT PLAN OBJECTIVE	4
DEPLOYMENT REQUIREMENTS	4
ASSUMPTIONS, DEPENDENCIES, AND ADDITIONAL CONSTRAINTS	5
CURRENT PRODUCTION ENVIRONMENT.....	6
TARGET ENVIRONMENT.....	7
DEPLOYMENT STRATEGY	10
PHASING	10
INFRASTRUCTURE.....	10
ROLES AND RESPONSIBILITIES	11
DETAILED PLAN	11
PHASE 1	11
Scope	11
Prerequisites for the start of Phase 1	12
Phase 1 Timeline.....	12
PHASE 2 AND 3.....	20
Scope	20
Prerequisites for the start of Phase 2 and 3	21
Phase 2 and 3 Timeline.....	21
BACK OUT PLAN	34
PHASE 1	34
Strategy	34
Prerequisites for Back Out	34
Phase 1 Back Out Timeline.....	35

Implementation Rollout Plan Objective

The objective of this deployment is to implement the SSN Phase II Application across five support offices in partnership with MoLSA staff and Primus. There is a Pilot system that is running at the MoLSA Central and Baghdad Pilot site; this system is to be replaced by the new application leveraging a mix of new and existing equipment. The rollout includes the following locations:

- Molsa Central – Central SSN Application
- Baghdad Pilot – Support Site
- Kharkh – Support Site
- Rusafa – Support Site
- Basra – Support Site
- Najaf – Support Site

The target for completing the rollout is prior to the end of March 2009.

Deployment Requirements

Req #	Requirement Description
DEP-1.0	The following sites are to have the Phase II SSN Application installed: <ul style="list-style-type: none"> • MoLSA Central • Baghdad Pilot • Kharkh • Rusafa • Basra • Najaf
DEP-2.0	The SSN Application Phase II role out needs to occur in the following order: <ol style="list-style-type: none"> 1. MoLSA Central – SSN Central System 2. Baghdad Pilot – Support Site <p>These sites can occur in any order but must be performed after the MoLSA Central SSN system has been deployed.</p> <ul style="list-style-type: none"> • Kharkh • Rusafa • Basra • Najaf
DEP-3.0	The target for completing the rollout is prior to the end of March 2009.
DEP-4.0	The server equipment currently used for the SSN pilot system will be reused for the Phase II application at MoLSA Central and Baghdad Pilot. The following systems will be reformatted and reinstalled from scratch: <ul style="list-style-type: none"> • MoLSA HQ – Application Server (for use at MoLSA Central) • MoLSA HQ – Database Server (for use at MoLSA Central) • MoLSA HQ – Domain Controller (for use at MoLSA Central) • Baghdad Pilot – Database Server (for use at Baghdad Pilot) • Baghdad Pilot – Application Server (for use at Baghdad Pilot) • Baghdad Pilot – Domain Controller (for use at Baghdad Pilot)
DEP-5.0	Data entry into the Phase I SSN Application Pilot system is an on-going effort. There is no short term business impact to taking the current Pilot

Req #	Requirement Description
	system off-line. However, data entry needs to continue using the Test Pilot system, with a minimum of disruption to this exercise.
DEP-6.0	Prior to the current SSN Pilot Application servers being reformatted, all databases must be backed up using MS SQL 2005 backup functions. These backups will be used for data migration between SSN Pilot and SSN Phase II. Full Phase I SSN Application configuration must also be written prior to the systems being re-purposed.
DEP-7.0	Primus (the SSN software vendor) will require remote access to all the SSN servers at all sites. This DOES NOT include access to the domain controllers or firewalls.
DEP-8.0	<p>Prior beginning the deployment an installation package is to be created that includes:</p> <ul style="list-style-type: none"> • This Rollout Plan • System Test Cases and scripts • SSN Deployment guides • Completed Site Survey • Primus Deployment Files
DEP-9.0	System Acceptance Testing must be completed by MoLSA before the deployment at each site is considered complete. The system test scripts developed by BearingPoint will be used for this testing.

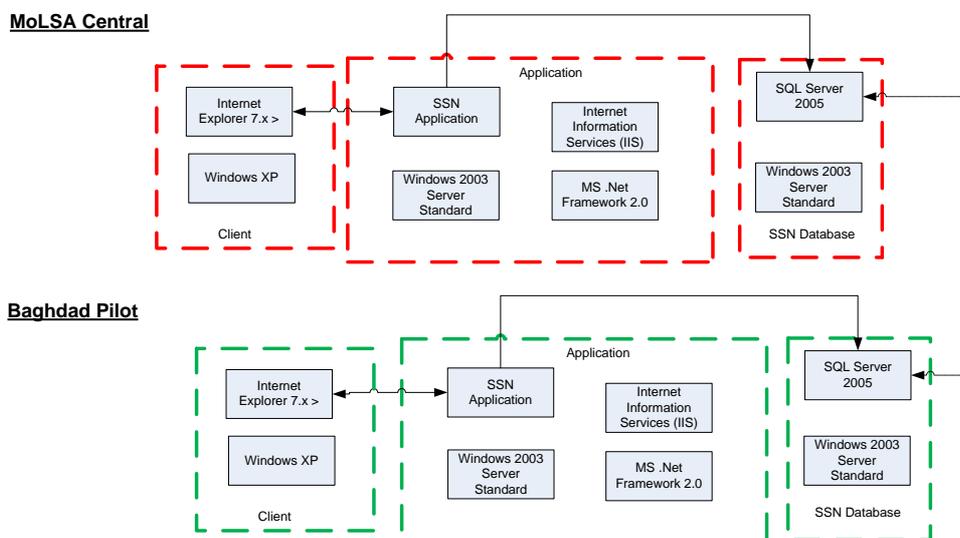
Assumptions, Dependencies, and Additional Constraints

- It is assumed that there is no impact to MoLSA if the Phase I SSN Pilot Application is taken off-line permanently.
- It is assumed that there is no impact to MoLSA if there is no SSN Application available for up to 2 - 3 days while the Phase II SSN Application is being deployed to MoLSA Central and Baghdad Pilot sites.
- It is assumed that there is no impact to MoLSA if data that was previously available in the Phase I SSN Pilot Application is not available until the data migration has been completed. The data migration will occur sometime (possibly months) after the Phase II deployment.
- Phase I to Phase II data migration is out of scope for this deployment
- MS Access Application to Phase II SSN Application is out of scope for this deployment
- The current infrastructure deployed at MoLSA is not being used for any functions other than to use the SSN Application, specifically Active Directory. Any effects of changes made to the infrastructure to support the SSN application will not be taken into consideration. Additionally, it is assumed that any changes to infrastructure required as a result of the deployment is out of scope and will NOT be performed by Bearingpoint.
- Current network configuration and architecture at MoLSA Central and Baghdad Pilot will not be changed with the exception of additional VPN's to remote sites. New sites being deployed will include the deployment of network devices sufficient for client workstations communicate with the Phase II SSN Application and for the Support Sites to communicate with the Phase II SSN Application at MoLSA central.

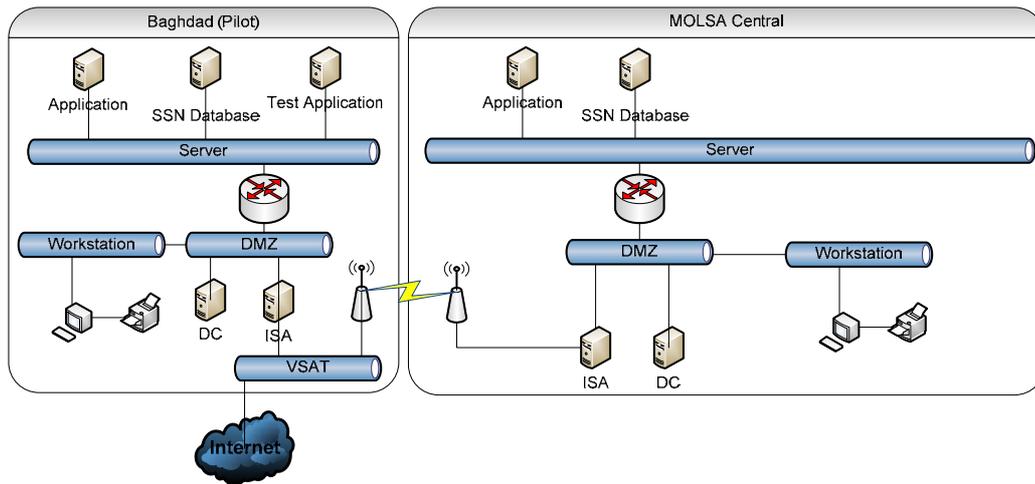
- The scope of this roll out includes only deploying the Phase II SSN Application and the minimum required to use the application. This excludes anti-virus, backup, monitoring, file/print services, workstation installation, security hardening, cabling and power.
- This deployment is dependent on free access to the sites and unhindered access to equipment and software.
- Equipment has been received for all the sites.
- Business processes to support the use of the application is out of scope for this deployment.
- Specific deployment dates are estimates only because of the environment. Resource availability, current operating environment, counterpart availability, political will all influence deployment schedules.

Current Production Environment

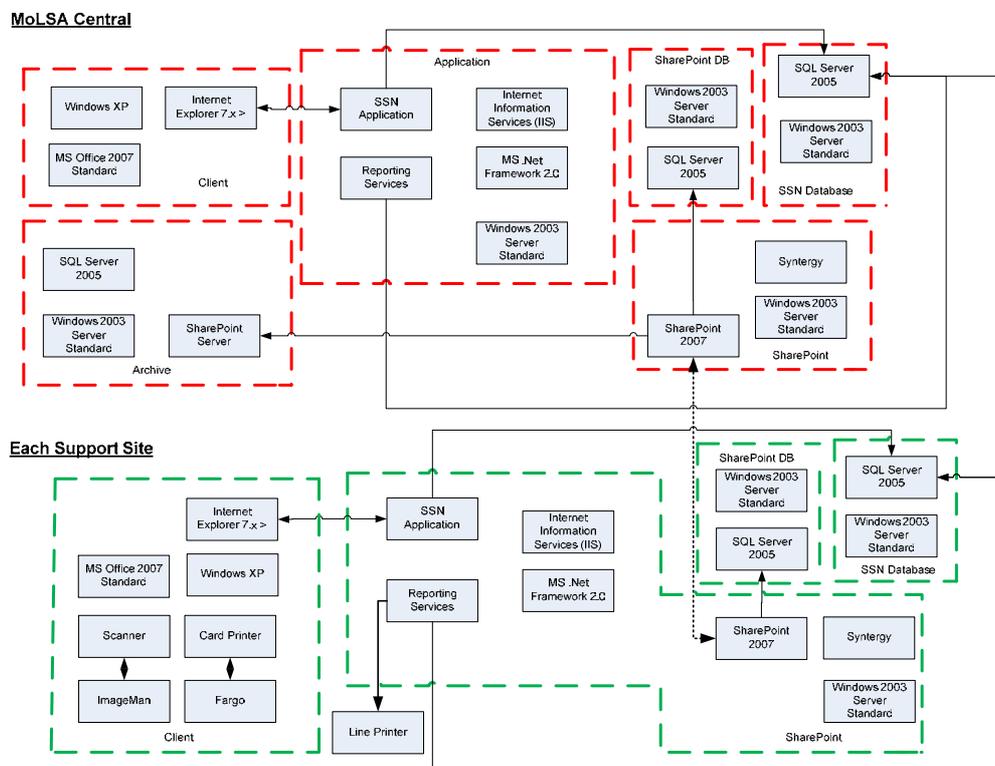
There is no production environment per say, the network and systems currently in place are supporting a pilot application deployed in 2007. The Phase I SSN Pilot Application is deployed at two locations, MoLSA Central and Baghdad Pilot. The pilot system is currently being used to capture data, completed paper forms are manually entered into a test system. Once the data has been entered it is audited by BearingPoint staff and once the data has been confirmed as been entered correctly, the database is backed up and restored to the Baghdad Pilot system. Data is replicated by physically moving the data between MoLSA HQ and Baghdad Pilot via USB drives.



There is some infrastructure in place today. The MoLSA Central and Baghdad Pilot locations have networks and Internet connectivity to support the Phase I SSN Pilot Application. These two locations do not have connectivity between them, but do share an Internet connection via a wireless connection. Each site has a domain controller with unrelated domains.



Target Environment



MoLSA Central Application – The application server runs the SSN application and reporting services. The application is based on Microsoft Visual Studio 2005, IIS and MS .Net Framework 2.0. Clients access the SSN Application via IIS and a web browser.

MoLSA Central SharePoint – The SharePoint server is used to upload and retrieve image files. An application called Synergy is also installed and used to replicate data between the support sites and MoLSA.

MoLSA Central SharePoint DB – This database is used in conjunction with the SharePoint and contains the SharePoint application database. The RDBMS is MS SQL Server 2005.

MoLSA Central SSN Database – This database server is used to house the MIS and SSN Application databases. These databases are replicated daily between MoLSA Central and the Support Sites. The RDBMS is MS SQL Server 2005.

MoLSA Central Archive – This system is used for archiving data that has been inactive for 12 months. It runs SharePoint server and SQL Server, data from SSN Application is converted into XML and moved to the Archive server with all the supported documents contained on the MoLSA Central SharePoint Server.

MoLSA Central Client – Since clients access the SSN Application via a web browser there are no components installed on the client.

Support Site SharePoint – The SharePoint server is used to upload and retrieve image files. An application call Synergy is also installed and used to replicate data between the support sites and MoLSA. The SSN application and reporting services are also installed. The application is based on Microsoft Visual Studio 2005, IIS and MS .Net Framework 2.0. Clients access the SSN Application via IIS and a web browser.

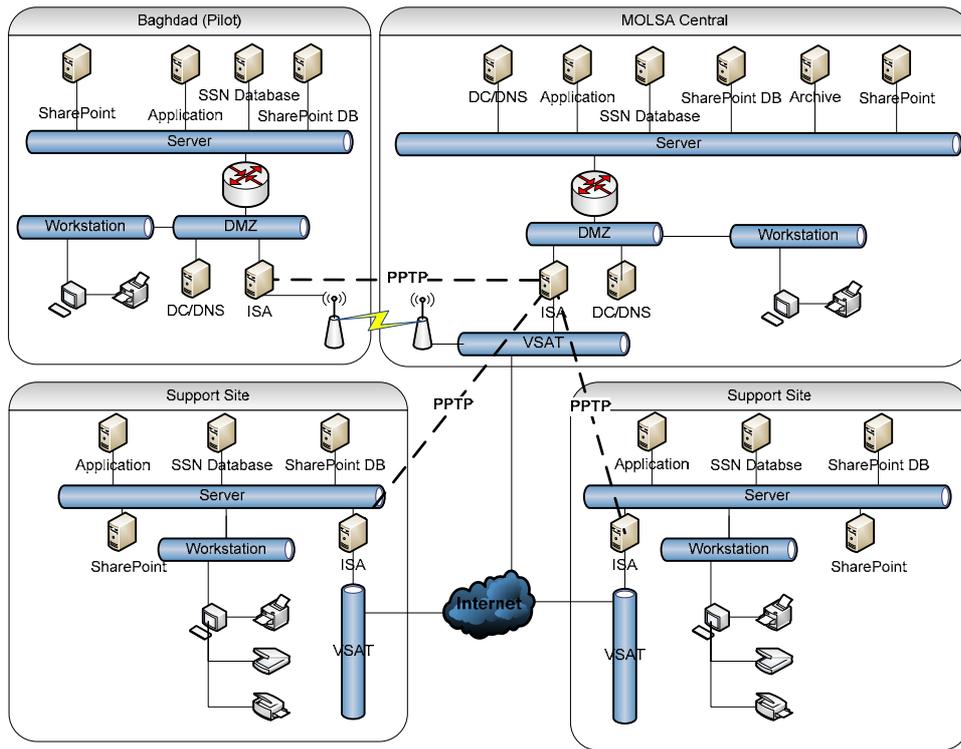
Support Site SharePoint DB – This database is used in conjunction with the SharePoint and contains the SharePoint application database. The RDMS is MS SQL Server 2005.

Support Site SSN Database – This database server is used to house the SSN Application databases. These databases are replicated daily between MoLSA Central and the Support Sites. The RDMS is MS SQL Server 2005.

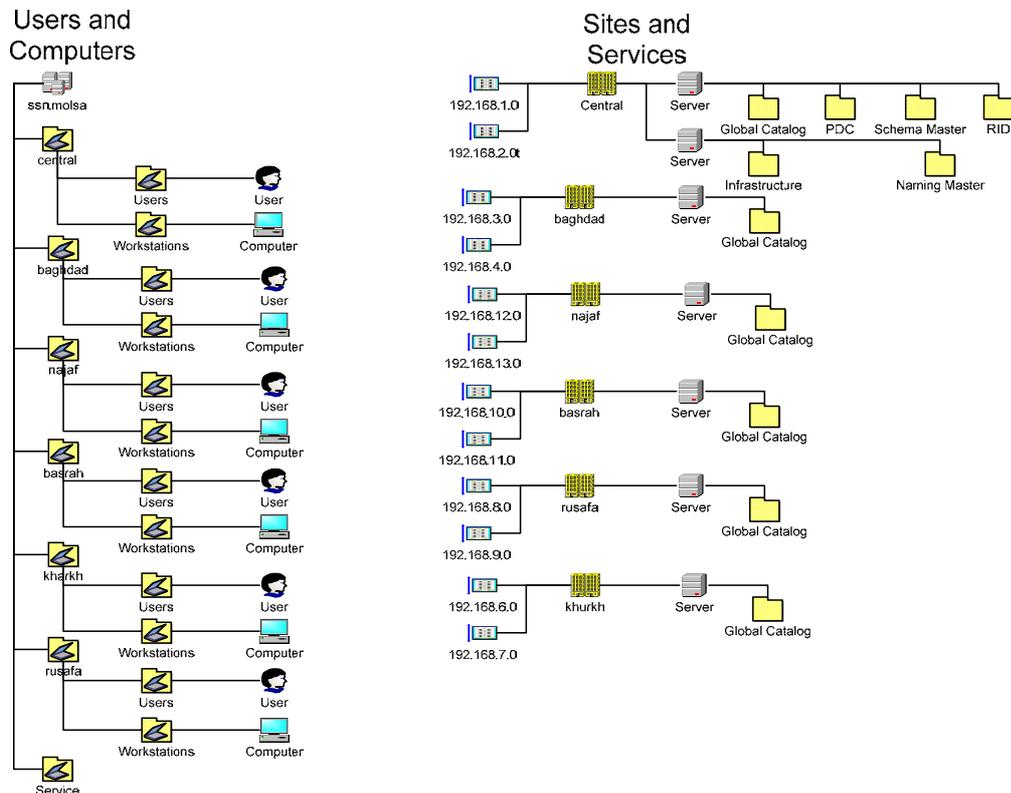
Support Site Client – Clients access the SSN Application via a web browser, MS Office 2007 is required to run on each workstation and there are specific configuration settings that are required. If the client will be performing scanning then there are some configuration and software requirements. In each office a workstation will be setup to print cards which has configuration and software requirements. A networked line printer will also be installed at each office; this is used for printing reports.

The target infrastructure environment consists of a central SSN system located at MoLSA Central and support sites that connect back to it. Each office will connect back to the central location via a VPN connection over a VSat connection to the Internet. Baghdad Pilot and MoLSA HQ will share a single Internet connection located at MoLSA HQ. This is to take advantage of the close proximity of the two buildings. These two sites are connected via a wireless access points and share the same Vsat subnet.

Each Support Site is connected back to MoLSA Central via an PPTP VPN tunnel. The firewalls used are MS ISA 2004 servers that are configured as standalone systems. The ISA servers are configured using default settings with some expectations to allow the SSN Application replication to work correctly. These settings are detailed in the Implementation procedures later in the document.



A single AD domain will be used, with two domain controllers located at MoLSA Central and one at each support site. Each domain controller will run DNS services and be configured as Active Directory Integrated. Servers and workstation IP configuration will be configured to point to their local Domain Controller as the primary DNS server. As a backup, the secondary DNS server will be a MOLSA Central Domain Controller.



Deployment Strategy

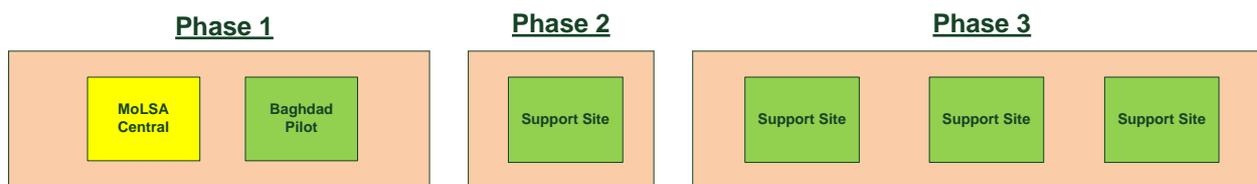
The general strategy used for the deployment of the Phase II SSN Application will be net new system installations performed one site at a time. There are however several considerations that complicate this strategy. The first is that a pilot system is currently being used at MoLSA Central and Baghdad Pilot sites. The hardware used at these sites is required for deploying Phase II. Existing infrastructure also needs to be modified to correctly support Phase II, this includes modifications to Active Directory and firewall settings.

There is also specific order in which some of the sites must be deployed. MoLSA Central must be deployed first because it is the central system where approvals and archiving are performed. For a deployment to be tested and determined successful each support site must be able to connect to and perform replication tasks with the central system. Lastly, equipment required to build the infrastructure is being ordered on a site by site basis. Deployment of each support site is dependent on the equipment having been received.

The Phase I SSN Pilot Application contains data. Initially it was thought that Phase I would have to be upgraded to Phase II. This would require that upgrade scripts and procedures would have to be tested prior to deployment. After speaking with the vendor – Primus, it was discovered that there is no upgrade path from Phase I to Phase II. Phase II will have to be deployed as a net new system using the existing Phase I hardware.

Phasing

There are three phases to this deployment.



Phase 1 – Initial System Deployment

This phase involves configuring the infrastructure to support the Phase II SSN Application and deploying it at the existing Phase I locations. During this phase we will also be validating our deployment guides and strategies to ensure subsequent phases can be deployed without error.

Phase 2 – First New Support Site Deployment

This phase involves deploying a net new Support Site. MoLSA staff will shadow BearingPoint staff on the Phase II SSN Application deployment.

Phase 3 – Subsequent Support Site Deployments

This phase includes deploying the remaining three Support Sites. During this phase MoLSA will deploy the sites with on-site support of BearingPoint staff. This will prepare the MoLSA staff to deploy subsequent sites with on their own.

Infrastructure

The existing infrastructure at the MoLSA Central and Baghdad Pilot site will be largely unchanged with the exception of the a VPN and Active Directory. The servers used for the Phase I SSN application will be reused for the Phase II application. These changes will be completed prior to implementing the new application.

The new Support Sites will have completely new infrastructure deployed, it is assumed that all cabling, physical space, HVAC, power and workstation deployment will be completed by MoLSA staff prior to the Phase II SSN Application rollout.

Roles and Responsibilities

Group	Role
BearingPoint	<p>BearingPoint group is responsible for:</p> <ul style="list-style-type: none"> • Deployment planning • Determining site readiness • Infrastructure deployment <ul style="list-style-type: none"> ○ SSN Application ○ Server ○ Active Directory ○ VPN – Firewall ○ Networking ○ SSN Client setup incl. scanners and printers and adding them to the domain. • Deploying the SSN Application to MoLSA and the first two sites • Providing on-site support the remaining three support sites • Performing Phase I data migration for the MoLSA and Baghdad 1 sites • Performing the MS Access Application data migration
Primus	<p>Primus is responsible for:</p> <ul style="list-style-type: none"> • Providing remote support during the deployments
MoLSA	<p>MoLSA is responsible for:</p> <ul style="list-style-type: none"> • Preparing the sites for deployment • Shadowing BearingPoint on the MoLSA and Baghdad Pilot site deployment • Deploying the final three support sites • Performing system acceptance testing for all five support sites and MoLSA Central • Infrastructure deployment <ul style="list-style-type: none"> ○ Cabling ○ Workstation installation ○ VSat • Will provide necessary information to configure the application: <ul style="list-style-type: none"> ○ Governorate names in Arabic, English and Kurdish ○ Governorate ID's ○ A list of users who will be using the application and there access privileges

Detailed Plan

Phase 1

Scope

The scope of this phase includes:

- MoLSA Central and Baghdad Pilot sites
- VPN connections between MoLSA Central and Baghdad Pilot
- Active Directory rebuild
- Installation of Domain Controllers
- DNS implementation

- Deployment of Phase II SSN Application at both MoLSA Central and Baghdad Pilot
- Line printer, scanner and card printer setup
- Client configuration as it relates to the Phase II SSN Application deployment.

Prerequisites for the start of Phase 1

- Completed site survey
- Completed Phase I system document for rollback
- Backup of all Phase I application and system databases
- The following is determined
 - Active Directory username used for deploying the application with
 - SQL server/Database User who will be used by the SSN Application and services that access data on the SQL Server. (this includes a password)
- The following information is received from MoLSA:
 - Application name (URL that will be used to access the application)
 - A list of Governorate ID's
 - A list of users and access privileges for Domain and Application access
- Workstations have been physically installed and have network connectivity
- Installation CD's for:
 - Windows 2003 Server and latest service packs
 - MS ISA 2004 Server and latest service packs
 - Internet Explorer 7
 - MS SharePoint 2007 and latest service pack
 - SQL Server 2005 and latest service pack
 - .Net 2.0
 - SSN Deployment CD

Phase 1 Timeline

ID	Task Name	Duration	Pred.	Resource
1	Infrastructure			
2	Network			
3	Create Site to Site VPN	3 hrs.		Inf-1
4	Create User Accounts	1 day	24	Inf-1,Dev-1
5	MoLSA Central			
6	Build/Rebuild Servers	8 hrs.	15,16	Inf-1
7	Create New Active Directory Domain	1 hrs.	6	Inf-1
8	Add Workstation to the New Domain	4 hrs.	7	Inf-1
9	Baghdad Pilot			
10	Build/Rebuild Servers	8 hrs.	19,20,3	Inf-1
11	Add Workstations to the New Domain	4 hrs.	9,7	Inf-1
12				
13	Application			
14	MoLSA Central			
15	Configuration Document of Phase I Systems	3 days		Dev-1, Inf-1
16	Backup of Phase I Data	4 hrs.		Dev-1, Inf-1
17	Install SSN Application	3 days	6,7	Dev-1
18	Baghdad Pilot			
19	Configuration Document of Phase I Systems	3 days		Dev-2,Inf-2
20	Backup of Phase I Data	4 hrs.		Dev-2,Inf-2
21	Install SSN Application	3 days	17,10	Dev-1
22	Client Setup	2 days		Dev-1
23	Testing			

ID	Task Name	Duration	Pred.	Resource
24	System Testing	2 days	17,21,22,3	MoLSA

Phase 1 Implementation Procedure

The steps in this implementation procedure are ordered in the way they should be executed. Some of these steps however have overlapping start times and finish times. Each step will indicate this. These procedures do not include step by step instructions, it includes high level activities and critical information required to successfully deploy the Phase II SSN Application.

Infrastructure - Network

“Infrastructure – MoLSA Central” steps can be performed concurrently with this step.

1. Create a VPN Tunnel Between MoLSA Central and Baghdad Pilot Sites – VPN configuration is listed below.

MoLSA Central MS ISA 2004

Local Login: Username: bagpntp
Password: *****

Site Name: bagpntp

Address Range: 192.168.4.0 – 192.168.4.255
192.168.3.0 – 192.168.3.255
w.x.y.z (External IP of the local server)

Remote Gateway Login: Username: bagpntp
Domain: <blank>
Password: *****
Confirm Password: *****

Terminate Inactive Connection: Never

Protocol: PPTP

Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2)

Firewall Rule: Name: Site to Site
Action: Allow
From: bagpntp, External
To: Internal, Local Host
Condition: All Users

Network Rule: Name: bagpntp
Relation: Route
Source Network: bagpntp
Destination Network: Internal

Baghdad Pilot MS ISA 2004

Local Login: Username: bagpntp
Password: *****

Site Name: bagpntp

Address Range: 192.168.1.0 – 192.168.1.255
192.168.2.0 – 192.168.2.255
w.x.y.z (External IP of the local server)

Remote Gateway Login: Username: bagpntp
Domain: <blank>
Password: *****
Confirm Password: *****

Terminate Inactive Connection: Never

Protocol: PPTP

Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2)

Firewall Rule: Name: Site to Site
Action: Allow

From: bagpntp, External
To: Internal, Local Host
Condition: All Users
Network Rule: Name: bagpntp
Relation: Route
Source Network: bagpntp
Destination Network: Internal

Infrastructure - MoLSA Central

All the following steps can be performed concurrently with the configuration of the VPN tunnels.

1. Build New Domain Controllers – Configuration information located below.

Server Name	Configuration
HQDC01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.1.17 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.1.1 • DNS Servers – 192.168.1.17, 192.168.2.17 <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • DNS • DHCP
HQDC02	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.2.17 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.2.1 • DNS Servers – 192.168.2.17, 192.168.1.17 <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • DNS • DHCP

2. Create a new Active Directory domain – See the Active Directory Target state for details on the configuration. Domain Name: ssn.molsa
3. DNS Configuration – Verify that the zone ssn.molsa is configured as Active Directory Integrated. Add following list of records below.

Name	Record Type	IP Address/Alias
------	-------------	------------------

HQ	CNAME	HQAPP01.ssn.molsa
HQAPP01	Alias	192.168.2.18
HQSPDB01	Alias	192.168.2.19
HQARC01	Alias	192.168.2.20
HQAPPDB01	Alias	192.168.2.21
HQSP01	Alias	192.168.2.22

4. Configure DHCP Scope on HQDC01– DHCP Scope configuration is list below.

Scope Name: 192.168.1.x

Start IP: 192.168.1.1

End IP: 192.168.1.254

Excluded IP Addresses: 192.168.1.203 – 192.168.1.254

Lease Duration: 3 day(s) 0 hours 0 minutes

DNS Configuration:

Dynamically update DNS A and PTR records only if requested by the DHCP Client.

Discard A and PTR records when lease is deleted.

Scope Options:

003 Routers 192.168.1.1

006 DNS Servers 192.168.1.17, 192.168.2.17

015 DNS Domain Name “ssn.molsa.”

5. Configure DHCP Scope on HQDC02 – DHCP Scope configuration is list Below:

Scope Name: 192.168.1.x

Start IP: 192.168.1.1

End IP: 192.168.1.254

Excluded IP Addresses: 192.168.1.1 – 192.168.1.202

Lease Duration: 3 day(s) 0 hours 0 minutes

DNS Configuration:

Dynamically update DNS A and PTR records only if requested by the DHCP Client.

Discard A and PTR records when lease is deleted.

Scope Options:

003 Routers

006 DNS Servers 192.168.1.17, 192.168.2.17

015 DNS Domain Name “ssn.molsa.”

6. Configure Cisco Router as DHCP Relay – Agent to allow broadcast DHCP Discover and DHCP request messages to cross form network 192.168.1.x/24 to network 192.168.2.x/24

7. Build Application Servers – Configuration information located below.

Server Name	Configuration
HQAPP01	Operating System <ul style="list-style-type: none"> Windows Server 2003 Standard SP2 Drives Partitioning <ul style="list-style-type: none"> disk 0 RAID 0+1 Network <ul style="list-style-type: none"> IP Address – 192.168.2.18 Subnet Mask – 255.255.255.0

Server Name	Configuration
	<ul style="list-style-type: none"> • Default Gateway – 192.168.2.1 • DNS Servers – 192.168.2.17, 192.168.1.17 • Domain – ssn.molsa System <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled Services <ul style="list-style-type: none"> • IIS
HQSPDB01	Operating System <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 Drives Partitioning <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 Network <ul style="list-style-type: none"> • IP Address – 192.168.2.19 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.2.1 • DNS Servers – 192.168.2.17, 192.168.1.17 • Domain – ssn.molsa System <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled Services <ul style="list-style-type: none"> • IIS
HQARC01	Operating System <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 Drives Partitioning <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 Network <ul style="list-style-type: none"> • IP Address – 192.168.2.20 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.2.1 • DNS Servers – 192.168.2.17, 192.168.1.17 • Domain – ssn.molsa System <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled Services <ul style="list-style-type: none"> • IIS
HQAPPDB01	Operating System <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 Drives Partitioning <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 Network

Server Name	Configuration
	<ul style="list-style-type: none"> • IP Address – 192.168.2.21 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.2.1 • DNS Servers – 192.168.2.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
HQSP01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.2.22 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.2.1 • DNS Servers – 192.168.2.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS

8. Create Printer Queues – This includes both laser and line printers
9. Add Workstations to the New Domain –
 - a. Add all workstations to the Domain ssn.molsa.
 - b. Modify the date/time format to MM/dd/yy and set the Time Zone to Baghdad.
 - c. Install MS IE 7.x.
 - d. MS Office 2003 Standard
 - e. Scanners and printers should be setup on the workstations as required.

Application – MoLSA Central

The Phase II SSN Application installation must occur after the all the steps under the section “Infrastructure – MoLSA Central” has been completed. Deployment code can be found on the deployment CD.

1. Install the Phase II SSN Application – Reference the document “SSN Pilot Project – Installation Guide MOLSA” for deployment instructions. This document can be found on the deployment CD.
2. Configure database backups to occur on a regular basis. Transaction Log backup 3 times a day and a full database backup daily.

Infrastructure – Baghdad Pilot

All the following steps can be performed must be performed after the steps in the sections “Infrastructure - Network” and “Infrastructure – MoLSA Central” have been completed.

1. Build New Domain Controller – Configuration information located below.

Server Name	Configuration
BAGDC01	Operating System <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 Drives Partitioning <ul style="list-style-type: none"> • disk 0 RAID 0+1 Network <ul style="list-style-type: none"> • IP Address – 192.168.4.17 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.4.1 • DNS Servers – 192.168.4.17, 192.168.1.17 System <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled Services <ul style="list-style-type: none"> • DNS • DHCP

2. Promote BAGDC01 to a Domain Controller – See the Active Directory Target state for details on the configuration. Domain Name: ssn.molsa
3. DNS Configuration – Verify that the zone ssn.molsa is configured as Active Directory Integrated. Add following list of records in table B.

Name	Record Type	IP Address/Alias
BAGHDAD	CNAME	BAGAPP01.ssn.molsa
BAGAPP01	Alias	192.168.3.17
BAGSPDB01	Alias	192.168.3.18
BAGAPPDB01	Alias	192.168.3.19
BAGSP01	Alias	192.168.3.20

10. Configure DHCP Scope on BAGDC01– DHCP Scope configuration is list below.

Scope Name: 192.168.4.x

Start IP: 192.168.4.1

End IP: 192.168.1.254

Excluded IP Addresses: 192.168.4.1 – 192.168.4.31

Lease Duration: 3 day(s) 0 hours 0 minutes

DNS Configuration:

Dynamically update DNS A and PTR records only if requested by the DHCP Client.

Discard A and PTR records when lease is deleted.

Scope Options:

003 Routers 192.168.4.1

006 DNS Servers 192.168.4.17, 192.168.1.17

015 DNS Domain Name ssn.molsa

4. Build Application Servers – Configuration information located in table D.

Server Name	Configuration
BAGAPP01	Operating System <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 Drives Partitioning

Server Name	Configuration
	<ul style="list-style-type: none"> • disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.3.17 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.3.1 • DNS Servers – 192.168.4.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
BAGSPDB01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.3.18 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.3.1 • DNS Servers – 192.168.4.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
BAGAPPDB01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.3.19 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.3.1 • DNS Servers – 192.168.4.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
BAGSP01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2

Server Name	Configuration
	<p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.3.20 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.3.1 • DNS Servers – 192.168.4.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS

5. Printer Setup – This includes both laser and line printers.
6. Add Workstations to the New Domain –
 - a. Add all workstations to the Domain ssn.molsa.
 - b. Modify the date/time format to MM/dd/yy and set the Time Zone to Baghdad.
 - c. Install MS IE 7.x.
 - d. MS Office 2007 Standard
 - e. Scanners and printers should be setup on the workstations as required.

Application – Baghdad Pilot

The Phase II SSN Application installation must occur after the all the steps under the section “Infrastructure – Baghdad Pilot” and “Application – MoLSA Central” has been completed. Deployment code can be found on the deployment CD.

1. Install the Phase II SSN Application – Reference the document “SSN Pilot Project – Installation Guide MOLSA” for deployment instructions. This document can be found on the deployment CD.
2. Configure database backups to occur on a regular basis. Transaction Log backup 3 times a day and a full database backup daily.

Testing

All deployment steps at both sites need to be completed prior to starting the test.

1. System Testing – the final step is to have MoLSA validate the deployment. Reference “Phase II SSN Application Test Cases” and “Phase II SSN Application Test Scripts”. These files can be found on the deployment CD.
2. Create Domain and Application Accounts

Phase 2 and 3

Scope

The scope of this phase includes:

- Deployment to the remaining Support Sites
- Network Configuration – including switches, routers and firewalls
- VPN connections between MoLSA Central and Support Site
- Installation of Domain Controller
- Setup of DHCP services
- Deployment of Phase II SSN Application

- Line printer, scanner and card printer setup
- Client configuration as it relates to the Phase II SSN Application deployment.

Prerequisites for the start of Phase 2 and 3

- Completed site survey
- The Phase II SSN Application has been deployed in MoLSA Central
- The following information from MoLSA:
 - A list of Governorate ID's
 - A list of SSN ID ranges for each Governorate
 - A list of users and access privileges for Domain and Application access
- Workstations have been physically installed and have network connectivity
- Installation CD's for:
 - Windows 2003 Server and latest service packs
 - MS ISA 2004 Server and latest service packs
 - Internet Explorer 7
 - MS SharePoint 2007 and latest service pack
 - SQL Server 2005 and latest service pack
 - .Net 2.0
 - SSN Deployment CD

Phase 2 and 3 Timeline

ID	Task Name	Duration	Pred.	Resource Names
1	Infrastructure			
2	Network			
3	Configure Network	2 days		
4	Install MS ISA Server 2004	3 hrs.	3	
5	Create Site to Site VPN	3 hrs.	4	Inf-1
6	Create User Accounts	1 day	16	Inf-1, Dev-1
7	Support Site			
8	Build/Rebuild Servers	8 hrs.	5	Inf-1
9	Add Workstations to the New Domain	4 hrs.	8	Inf-1
10				
11	Application			
12	Support Site			
13	Install SSN Application	3 days	8	Dev-1
14	Client Setup	2 days	13	Dev-1
15	Testing			
16	System Testing	2 days	14,13,9,5	MoLSA

Phase 2 and 3 Implementation Procedure

The steps in this implementation procedure are ordered in the way they should be executed. Some of these steps however has overlapping start times and finish times. Each step will indicate this. These procedures do not include step by step instructions, it includes high level activities and critical information required to successfully deploy the Phase II SSN Application.

Infrastructure - Network

1. Configure Network – The specific configuration requirements of the network will depend on the physical layout of the Support Site. The network configuration described below needs to implement.

Location	Server Subnet	Workstation Subnet
----------	---------------	--------------------

Rusafa	192.168.8.0/24	192.168.9.0/24
Kharkh	192.168.6.0/24	192.168.7.0/24
Najaf	192.168.12.0/24	192.168.13.0/24
Basrah	192.168.10.0/24	192.168.11.0/24

2. Configure InterVLAN Routing with L3 Cisco Switch model 3560.

Location	Configuration						
Rusafa	<p>L3 Switch Configuration</p> <ol style="list-style-type: none"> Add VLANs 8, 9 to the Switch VLAN database <ul style="list-style-type: none"> VLAN 8 Name: VLAN Server Net VLAN 9 Name: VLAN Workstation Net VLAN interfaces with IP address <ul style="list-style-type: none"> VLAN 8 # 192.168.8.1 255.255.255.0 VLAN 9 # 192.168.9.1 255.255.255.0 Assign the following ports to the specific VLAN. <table border="1" style="margin-left: 20px;"> <tr> <td>VLAN 8</td> <td>GE 0/1 – GE 0/16</td> </tr> <tr> <td>VLAN 9</td> <td>GE 0/17 – GE 0/32</td> </tr> <tr> <td>Default VLAN</td> <td>Remaining Ports in Switch</td> </tr> </table> Enabling routing on the Switch. Make the interface GE 0/48 Layer 3 capable. Configure the default route for the switch. Configure end devices to use catalyst 3560 VLAN interface as their default gateway. 	VLAN 8	GE 0/1 – GE 0/16	VLAN 9	GE 0/17 – GE 0/32	Default VLAN	Remaining Ports in Switch
VLAN 8	GE 0/1 – GE 0/16						
VLAN 9	GE 0/17 – GE 0/32						
Default VLAN	Remaining Ports in Switch						
Kharkh	<p>L3 Switch Configuration</p> <ol style="list-style-type: none"> Add VLANs 6, 7 to the Switch VLAN database <ul style="list-style-type: none"> VLAN 6 Name: VLAN Server Net VLAN 7 Name: VLAN Workstation Net VLAN interfaces with IP address <ul style="list-style-type: none"> VLAN 6 # 192.168.6.1 255.255.255.0 VLAN 7 # 192.168.7.1 255.255.255.0 Assign the following ports to the specific VLAN. <table border="1" style="margin-left: 20px;"> <tr> <td>VLAN 6</td> <td>GE 0/1 – GE 0/16</td> </tr> <tr> <td>VLAN 7</td> <td>GE 0/17 – GE 0/32</td> </tr> <tr> <td>Default VLAN</td> <td>Remaining Ports in Switch</td> </tr> </table> Enabling routing on the Switch. Make the interface GE 0/48 Layer 3 capable. Configure the default route for the switch. Configure end devices to use catalyst 3560 VLAN interface as their default gateway. 	VLAN 6	GE 0/1 – GE 0/16	VLAN 7	GE 0/17 – GE 0/32	Default VLAN	Remaining Ports in Switch
VLAN 6	GE 0/1 – GE 0/16						
VLAN 7	GE 0/17 – GE 0/32						
Default VLAN	Remaining Ports in Switch						
Najaf	<p>L3 Switch Configuration</p> <ol style="list-style-type: none"> Add VLANs 12, 13 to the Switch VLAN database <ul style="list-style-type: none"> VLAN 12 Name: VLAN Server Net VLAN 13 Name: VLAN Workstation Net VLAN interfaces with IP address 						

Location	Configuration						
	<ul style="list-style-type: none"> • VLAN 12 # 192.168.12.1 255.255.255.0 • VLAN 13 # 192.168.13.1 255.255.255.0 <p>3) Assign the following ports to the specific VLAN.</p> <table border="1" data-bbox="588 338 1265 445"> <tr> <td>VLAN 12</td> <td>GE 0/1 – GE 0/16</td> </tr> <tr> <td>VLAN 13</td> <td>GE 0/17 – GE 0/32</td> </tr> <tr> <td>Default VLAN</td> <td>Remaining Ports in Switch</td> </tr> </table> <ul style="list-style-type: none"> 4) Enabling routing on the Switch. 5) Make the interface GE 0/48 Layer 3 capable. 6) Configure the default route for the switch. 7) Configure end devices to use catalyst 3560 VLAN interface as their default gateway. 	VLAN 12	GE 0/1 – GE 0/16	VLAN 13	GE 0/17 – GE 0/32	Default VLAN	Remaining Ports in Switch
VLAN 12	GE 0/1 – GE 0/16						
VLAN 13	GE 0/17 – GE 0/32						
Default VLAN	Remaining Ports in Switch						
Basarh	<p>L3 Switch Configuration</p> <ol style="list-style-type: none"> 1) Add VLANs 10, 11 to the Switch VLAN database <ul style="list-style-type: none"> • VLAN 10 Name: VLAN Server Net • VLAN 11 Name: VLAN Workstation Net 2) VLAN interfaces with IP address <ul style="list-style-type: none"> • VLAN 10 # 192.168.10.1 255.255.255.0 • VLAN 11 # 192.168.11.1 255.255.255.0 <p>3) Assign the following ports to the specific VLAN.</p> <table border="1" data-bbox="588 1025 1265 1133"> <tr> <td>VLAN 10</td> <td>GE 0/1 – GE 0/16</td> </tr> <tr> <td>VLAN 11</td> <td>GE 0/17 – GE 0/32</td> </tr> <tr> <td>Default VLAN</td> <td>Remaining Ports in Switch</td> </tr> </table> <ol style="list-style-type: none"> 4) Enabling routing on the Switch. 5) Make the interface GE 0/48 Layer 3 capable. 6) Configure the default route for the switch. 7) Configure end devices to use catalyst 3560 VLAN interface as their default gateway. 	VLAN 10	GE 0/1 – GE 0/16	VLAN 11	GE 0/17 – GE 0/32	Default VLAN	Remaining Ports in Switch
VLAN 10	GE 0/1 – GE 0/16						
VLAN 11	GE 0/17 – GE 0/32						
Default VLAN	Remaining Ports in Switch						

3. Install MS ISA 2004 Server – Table B outlines the configuration for each Support Site.

Location	Configuration
Rusafa	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> • Name: RAISA01 • NIC #1 - Internal <ul style="list-style-type: none"> ○ IP Address – 192.168.8.18 ○ Subnet Mask – 255.255.255.0 ○ Default Gateway – None ○ DNS Servers – 192.168.8.17, 192.168.1.17 • NIC #2 - External <ul style="list-style-type: none"> ○ IP Address – w.x.y.z

Location	Configuration
	<ul style="list-style-type: none"> ○ Subnet Mask – x.x.x.x ○ Default Gateway – w.x.y.z ○ DNS Servers – w.x.y.z, w.x.yz <p>System</p> <ul style="list-style-type: none"> ● Time Zone – Baghdad <p>Software</p> <ul style="list-style-type: none"> ● MS ISA 2004 Server
Kharkh	<p>Operating System</p> <ul style="list-style-type: none"> ● Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> ● disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> ● Name: NFISA01 ● NIC #1 - Internal <ul style="list-style-type: none"> ○ IP Address – 192.168.6.18 ○ Subnet Mask – 255.255.255.0 ○ Default Gateway – None ○ DNS Servers – 192.168.6.17, 192.168.1.17 ● NIC #2 - External <ul style="list-style-type: none"> ○ IP Address – w.x.y.z ○ Subnet Mask – x.x.x.x ○ Default Gateway – w.x.y.z ○ DNS Servers – w.x.y.z, w.x.yz <p>System</p> <ul style="list-style-type: none"> ● Time Zone – Baghdad <p>Software</p> <ul style="list-style-type: none"> ● MS ISA 2004 Server
Najaf	<p>Operating System</p> <ul style="list-style-type: none"> ● Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> ● disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> ● Name: NFISA01 ● NIC #1 - Internal <ul style="list-style-type: none"> ○ IP Address – 192.168.12.18 ○ Subnet Mask – 255.255.255.0 ○ Default Gateway – None ○ DNS Servers – 192.168.12.17, 192.168.1.17 ● NIC #2 - External <ul style="list-style-type: none"> ○ IP Address – w.x.y.z ○ Subnet Mask – x.x.x.x ○ Default Gateway – w.x.y.z ○ DNS Servers – w.x.y.z, w.x.yz <p>System</p> <ul style="list-style-type: none"> ● Time Zone – Baghdad <p>Software</p> <ul style="list-style-type: none"> ● MS ISA 2004 Server
Basarh	<p>Operating System</p> <ul style="list-style-type: none"> ● Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> ● disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> ● Name: BHISA01

Location	Configuration
	<ul style="list-style-type: none"> • NIC #1 - Internal <ul style="list-style-type: none"> ○ IP Address – 192.168.10.18 ○ Subnet Mask – 255.255.255.0 ○ Default Gateway – None ○ DNS Servers – 192.168.10.17, 192.168.1.17 • NIC #2 - External <ul style="list-style-type: none"> ○ IP Address – w.x.y.z ○ Subnet Mask – x.x.x.x ○ Default Gateway – w.x.y.z ○ DNS Servers – w.x.y.z, w.x.yz <p>System</p> <ul style="list-style-type: none"> • Time Zone – Baghdad <p>Software</p> <ul style="list-style-type: none"> • MS ISA 2004 Server

1. Create a VPN Tunnel Between MoLSA Central and Support Site – VPN configuration for each site is listed below.

Location	MoLSA Central	Support Sites
Rusafa	Local Login: Username: rapptp Password: ***** Site Name: rapptp Address Range: 192.168.8.0 – 192.168.8.255 192.168.9.0 – 192.168.9.255 w.x.y.z (External IP of the local server) Remote Gateway Login: Username: rapptp Domain: <blank> Password: ***** Confirm Password: ***** Terminate Inactive Connection: Never Protocol: PPTP Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2) Firewall Rule: Name: Site to Site Action: Allow From: rapptp, External To: Internal, Local Host Condition: All Users Network Rule: Name: rapptp Relation: Route Source Network: rapptp Destination Network: Internal	Local Login: Username: rapptp Password: ***** Site Name: rapptp Address Range: 192.168.1.0 – 192.168.1.255 192.168.2.0 – 192.168.2.255 w.x.y.z (External IP of the local server) Remote Gateway Login: Username: rapptp Domain: <blank> Password: ***** Confirm Password: ***** Terminate Inactive Connection: Never Protocol: PPTP Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2) Firewall Rule: Name: Site to Site Action: Allow From: rapptp, External To: Internal, Local Host Condition: All Users Network Rule: Name: rapptp Relation: Route Source Network: rapptp Destination Network: Internal
Kharkh	Local Login: Username: khpptp Password: ***** Site Name: khpptp Address Range: 192.168.6.0 – 192.168.6.255 192.168.7.0 – 192.168.7.255 w.x.y.z (External IP of the local server) Remote Gateway Login: Username: khpptp Domain: <blank> Password: ***** Confirm Password: ***** Terminate Inactive Connection: Never Protocol: PPTP Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2) Firewall Rule: Name: Site to Site Action: Allow	Local Login: Username: khpptp Password: ***** Site Name: khpptp Address Range: 192.168.1.0 – 192.168.1.255 192.168.2.0 – 192.168.2.255 w.x.y.z (External IP of the local server) Remote Gateway Login: Username: khpptp Domain: <blank> Password: ***** Confirm Password: ***** Terminate Inactive Connection: Never Protocol: PPTP Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2) Firewall Rule: Name: Site to Site Action: Allow

Location	MoLSA Central	Support Sites
	<p>From: khpptp, External To: Internal, Local Host Condition: All Users</p> <p>Network Rule: Name: khpptp Relation: Route Source Network: khpptp Destination Network: Internal</p>	<p>From: khpptp, External To: Internal, Local Host Condition: All Users</p> <p>Network Rule: Name: khpptp Relation: Route Source Network: khpptp Destination Network: Internal</p>
Najaf	<p>Local Login: Username: nfpptp Password: *****</p> <p>Site Name: nfpptp Address Range: 192.168.12.0 – 192.168.12.255 192.168.13.0 – 192.168.13.255 w.x.y.z (External IP of the local server)</p> <p>Remote Gateway Login: Username: nfpptp Domain: <blank> Password: ***** Confirm Password: *****</p> <p>Terminate Inactive Connection: Never Protocol: PPTP Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2) Firewall Rule: Name: Site to Site Action: Allow From: nfpptp, External To: Internal, Local Host Condition: All Users</p> <p>Network Rule: Name: nfpptp Relation: Route Source Network: nfpptp Destination Network: Internal</p>	<p>Local Login: Username: nfpptp Password: *****</p> <p>Site Name: bagpptp Address Range: 192.168.1.0 – 192.168.1.255 192.168.2.0 – 192.168.2.255 w.x.y.z (External IP of the local server)</p> <p>Remote Gateway Login: Username: nfpptp Domain: <blank> Password: ***** Confirm Password: *****</p> <p>Terminate Inactive Connection: Never Protocol: PPTP Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2) Firewall Rule: Name: Site to Site Action: Allow From: nfpptp, External To: Internal, Local Host Condition: All Users</p> <p>Network Rule: Name: nfpptp Relation: Route Source Network: nfpptp Destination Network: Internal</p>
Basrah	<p>Local Login: Username: bhpptp Password: *****</p> <p>Site Name: bhpptp Address Range: 192.168.10.0 – 192.168.10.255 192.168.11.0 – 192.168.11.255 w.x.y.z (External IP of the local server)</p> <p>Remote Gateway Login: Username: bhpptp Domain: <blank> Password: ***** Confirm Password: *****</p> <p>Terminate Inactive Connection: Never Protocol: PPTP Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2) Firewall Rule: Name: Site to Site Action: Allow From: bhpptp, External To: Internal, Local Host Condition: All Users</p> <p>Network Rule: Name: bhpptp Relation: Route Source Network: bhpptp Destination Network: Internal</p>	<p>Local Login: Username: bhpptp Password: *****</p> <p>Site Name: bhpptp Address Range: 192.168.1.0 – 192.168.1.255 192.168.2.0 – 192.168.2.255 w.x.y.z (External IP of the local server)</p> <p>Remote Gateway Login: Username: bhpptp Domain: <blank> Password: ***** Confirm Password: *****</p> <p>Terminate Inactive Connection: Never Protocol: PPTP Authentication: Allow Microsoft CHAP Version 2 (MS-CHAP v2) Firewall Rule: Name: Site to Site Action: Allow From: bhpptp, External To: Internal, Local Host Condition: All Users</p> <p>Network Rule: Name: bhpptp Relation: Route Source Network: bhpptp Destination Network: Internal</p>

Infrastructure – Support Sites

11. Build New Domain Controller – Configuration information for each is located below.

Location	Configuration
----------	---------------

Location	Configuration
Rusafa	<p>Operating System</p> <ul style="list-style-type: none"> Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> Name – RADC01 IP Address – 192.168.8.17 Subnet Mask – 255.255.255.0 Default Gateway – 192.168.8.1 DNS Servers – 192.168.8.17, 192.168.1.17 <p>System</p> <ul style="list-style-type: none"> Date/Time Format – MM/dd/yy Time Zone – Baghdad Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> DNS DHCP
Kharkh	<p>Operating System</p> <ul style="list-style-type: none"> Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> Name – KHDC01 IP Address – 192.168.6.17 Subnet Mask – 255.255.255.0 Default Gateway – 192.168.6.1 DNS Servers – 192.168.6.17, 192.168.1.17 <p>System</p> <ul style="list-style-type: none"> Date/Time Format – MM/dd/yy Time Zone – Baghdad Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> DNS DHCP
Najaf	<p>Operating System</p> <ul style="list-style-type: none"> Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> Name – NFDC01 IP Address – 192.168.12.17 Subnet Mask – 255.255.255.0 Default Gateway – 192.168.12.1 DNS Servers – 192.168.12.17, 192.168.1.17 <p>System</p> <ul style="list-style-type: none"> Date/Time Format – MM/dd/yy Time Zone – Baghdad Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> DNS

Location	Configuration
	<ul style="list-style-type: none"> DHCP
Basrah	<p>Operating System</p> <ul style="list-style-type: none"> Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> Name – BHDC01 IP Address – 192.168.10.17 Subnet Mask – 255.255.255.0 Default Gateway – 192.168.10.1 DNS Servers – 192.168.10.17, 192.168.1.17 <p>System</p> <ul style="list-style-type: none"> Date/Time Format – MM/dd/yy Time Zone – Baghdad Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> DNS DHCP

12. Update Active Directory with New Site Information – See the Active Directory Target state for details on the configuration. Domain Name: ssn.molsa.

13. DNS Configuration – Verify that the zone ssn.molsa is configured as Active Directory Integrated. Add following list of records below.

Location	Name	Record Type	IP Address/Alias
Rusafa	RA	CNAME	RAAPP01.ssn.molsa
	RASPDB01	Alias	192.168.8.19
	RAAPPDB01	Alias	192.168.8.21
	RASP01	Alias	192.168.8.22
Kharkh	KH	CNAME	KHAPP01.ssn.molsa
	KHSPDB01	Alias	192.168.6.19
	KHAPPDB01	Alias	192.168.6.21
	KHSP01	Alias	192.168.6.22
Najaf	NF	CNAME	NFAPP01.ssn.molsa
	NFSPDB01	Alias	192.168.12.19
	NFAPPDB01	Alias	192.168.12.21
	NFSP01	Alias	192.168.12.22
Basrah	BH	CNAME	BHAPP01.ssn.molsa
	BHSPDB01	Alias	192.168.10.19
	BHAPPDB01	Alias	192.168.10.21
	BHSP01	Alias	192.168.10.22

14. Configure DHCP Scope - DHCP Scope configuration for each Support Site is listed below.

Location	Scope Definition
Rusafa	<p>Scope Name: 192.168.8.x Start IP: 192.168.8.32 End IP: 192.168.8.254</p>

Location	Scope Definition
	Lease Duration: 3 day(s) 0 hours 0 minutes DNS Configuration: Dynamically update DNS A and PTR records only if requested by the DHCP Client. Discard A and PTR records when lease is deleted. Scope Options: 006 DNS Servers 192.168.8.17, 192.168.1.17 015 DNS Domain Name ssn.molsa 003 Router 192.168.8.1
Kharkh	Scope Name: 192.168.6.x Start IP: 192.168.6.32 End IP: 192.168.6.255 Lease Duration: 3 day(s) 0 hours 0 minutes DNS Configuration: Dynamically update DNS A and PTR records only if requested by the DHCP Client. Discard A and PTR records when lease is deleted. Scope Options: 006 DNS Servers 192.168.6.17, 192.168.1.17 015 DNS Domain Name ssn.molsa 003 Router 192.168.6.1
Najaf	Scope Name: 192.168.12.x Start IP: 192.168.12.32 End IP: 192.168.12.254 Lease Duration: 3 day(s) 0 hours 0 minutes DNS Configuration: Dynamically update DNS A and PTR records only if requested by the DHCP Client. Discard A and PTR records when lease is deleted. Scope Options: 006 DNS Servers 192.168.12.17, 192.168.1.17 015 DNS Domain Name ssn.molsa 003 Router 192.168.12.1
Basrah	Scope Name: 192.168.10.x Start IP: 192.168.10.32 End IP: 192.168.10.254 Lease Duration: 3 day(s) 0 hours 0 minutes DNS Configuration: Dynamically update DNS A and PTR records only if requested by the DHCP Client. Discard A and PTR records when lease is deleted. Scope Options: 006 DNS Servers 192.168.10.17, 192.168.1.17 015 DNS Domain Name ssn.molsa 003 Router 192.168.10.1

15. Build Application Servers

Server Name	Configuration
Rusafa	
RASPDB01	Operating System <ul style="list-style-type: none"> Windows Server 2003 Standard SP2 Drives Partitioning <ul style="list-style-type: none"> disk 0 RAID 0+1 disk 1 RAID 5 Network <ul style="list-style-type: none"> IP Address – 192.168.9.19 Subnet Mask – 255.255.255.0

Server Name	Configuration
	<ul style="list-style-type: none"> • Default Gateway – 192.168.9.1 • DNS Servers – 192.168.8.17, 192.168.1.17 • Domain – ssn.molsa System <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled Services <ul style="list-style-type: none"> • IIS
RAAPPDB01	Operating System <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 Drives Partitioning <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 Network <ul style="list-style-type: none"> • IP Address – 192.168.9.21 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.9.1 • DNS Servers – 192.168.8.17, 192.168.1.17 • Domain – ssn.molsa System <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled Services <ul style="list-style-type: none"> • IIS
RASP01	Operating System <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 Drives Partitioning <ul style="list-style-type: none"> • disk 0 RAID 0+1 Network <ul style="list-style-type: none"> • IP Address – 192.168.9.22 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.9.1 • DNS Servers – 192.168.8.17, 192.168.1.17 • Domain – ssn.molsa System <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled Services <ul style="list-style-type: none"> • IIS
Kharkh	
KHSPDB01	Operating System <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 Drives Partitioning <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 Network

Server Name	Configuration
	<ul style="list-style-type: none"> • IP Address – 192.168.7.19 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.7.1 • DNS Servers – 192.168.6.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
KHAPPDB01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.7.21 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.7.1 • DNS Servers – 192.168.6.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
KHSP01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.7.22 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.7.1 • DNS Servers – 192.168.6.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
Najaf	
NFSPDB01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1

Server Name	Configuration
	<ul style="list-style-type: none"> • disk 1 RAID 5 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.13.19 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.13.1 • DNS Servers – 192.168.12.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
NFAPPDB01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.13.21 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.13.1 • DNS Servers – 192.168.12.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
NFSP01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.13.22 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.13.1 • DNS Servers – 192.168.12.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
Basrah	
BHSPDB01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2

Server Name	Configuration
	<p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.11.19 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.11.1 • DNS Servers – 192.168.10.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
BHAPPDB01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 • disk 1 RAID 5 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.11.21 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.11.1 • DNS Servers – 192.168.10.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS
BHSP01	<p>Operating System</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard SP2 <p>Drives Partitioning</p> <ul style="list-style-type: none"> • disk 0 RAID 0+1 <p>Network</p> <ul style="list-style-type: none"> • IP Address – 192.168.11.22 • Subnet Mask – 255.255.255.0 • Default Gateway – 192.168.11.1 • DNS Servers – 192.168.10.17, 192.168.1.17 • Domain – ssn.molsa <p>System</p> <ul style="list-style-type: none"> • Date/Time Format – MM/dd/yy • Time Zone – Baghdad • Remote Desktop Enabled <p>Services</p> <ul style="list-style-type: none"> • IIS

16. Add Workstations to the New Domain –
 - a. Add all workstations to the Domain ssn.molsa.
 - b. Modify the date/time format to MM/dd/yy and set the Time Zone to Baghdad.
 - c. Install MS IE 7.x.
 - d. MS Office 2007 Standard
17. Printer Setup – This includes laser and line printers

Application – Support Site

The Phase II SSN Application installation must occur after the all the steps under the section “Infrastructure – Network” and “Infrastructure – Support Site” has been completed. Deployment code can be found on the deployment CD.

1. Install the Phase II SSN Application – Reference the document “SSN Pilot Project – Installation Guide Governorate” for deployment instructions. This document can be found on the deployment CD.
2. Configure database backups to occur on a regular basis. Transaction Log backup 3 times a day and a full database backup daily.

Testing

All deployment steps at both sites need to be completed prior to starting the test.

1. System Testing –the final step is to have MoLSA validate the deployment. Reference “Phase II SSN Application Test Cases” and “Phase II SSN Application Test Scripts”. These files can be found on the deployment CD.
2. Create Domain and Application Accounts

Back Out Plan

A back out plan is only required for Phase I. This is because the Phase I SSN Pilot Application will be replaced with the Phase II SSN Application in the MoLSA Central and Baghdad Pilot locations. There will be no changes to existing production systems with the deployment of additional sites.

Phase 1

Strategy

The back out strategy to restore the Phase I SSN Application is to redeploy the application from scratch. This will require detailed system configuration information, Phase I SSN Application deployment guides and database backups. Once the servers have been rebuilt then all system and application databases are restored. Phase I will run within the newly deployed Active Directory, so only application servers will be impacted by the back out procedure.

Prerequisites for Back Out

This is the list of prerequisites to execute the back out procedure successfully.

- Backup of all Phase I SSN Pilot Application system and application databases.
- The Phase I SSN Pilot Application configuration guide.
- Phase I SSN Pilot Application deployment guide.
- Installation CD for:
 - SharePoint 2004
 - Windows 2003 Server SP2
 - MS SQL Server 2005 and latest service pack

Phase 1 Back Out Timeline

ID	Task Name	Duration	Pred.	Resource Names
1	Infrastructure			
2	MoLSA Central			
3	Build/Rebuild Servers	8 hrs.		Inf-1
4	Baghdad Pilot			
5	Build/Rebuild Servers	8 hrs.		Inf-2
6				
7	Application			
8	MoLSA Central			
9	Install SSN Application	3 days	3	Dev-1
10	Restore system and application databases	1 day	9	Dev-1
11	Baghdad Pilot			
12	Install SSN Application	3 days	5	Dev-2
13	Restore system and application databases	1 day	12	Dev-2
14	Testing			
15	System Testing	2 days	10,13	MoLSA