



**IRAQ FINANCIAL MANAGEMENT INFORMATION
SYSTEM
PRODUCTION ENVIRONMENT PLAN**

Powered by ProvenCourseSM

Iraq Economic Governance II



USAID
FROM THE AMERICAN PEOPLE

Saturday, April 9, 2005

Disposition {Final}



Authors

| | | |
|--|---|---|
| Nate Nash, Senior Consultant BearingPoint, Inc. 1676 International Drive McLean, VA 22102 T: 703-747-4330 nate.nash@bearingpoint.com | Robert Caffery, Senior Consultant BearingPoint, Inc. 1676 International Drive McLean, VA 22102 T: 703-747-3000 robert.caffery@bearingpoint.com | Zaid Al-Ogaily, IT Specialist BearingPoint, Inc. 1676 International Drive McLean, VA 22102 T: 703-994-4675 ce-zaid.al-ogaily@bearingpoint.com |
| Jay Hariani, Senior IT Advisor Manchester Trade Subcontractor BearingPoint, Inc. 1676 International Drive McLean, VA 22102 T: 703-747-4330 jhariani@gmail.com | Lynda Roades, Senior Consultant BearingPoint, Inc. 1676 International Drive McLean, VA 22102 T: 703-747-4822 lynda.roades@bearingpoint.com | |

| Date | Document Version | Document Revision Description | Document Author |
|---------------|------------------|--|-----------------|
| 2/22/2005 | 0.1 | Initial Draft | Jay Hariani |
| 2/24/2005 | 0.2 | Added network procedure, pre-production check list, fire protection, UPS/Gen/electrical | Jay Hariani |
| 2/28/2005 | 0.3 | Added patch management, backup and restore, and anti-virus operations sections | Robert Caffery |
| 2/28/2005 | 0.4 | Added embedded server build sheet template (embedded file), updated inline sample in document. Updated rack diagram. Updated pre-deployment checklist, IP address and password tables. Added remote sites list, new servers (DC 1 & 2) | Zaid Al-Ogaily |
| 03/3/2004 | 0.5 | Updated server and added desktop image build sheets | Jay Hariani |
| 03/3/2005 | 0.6 | Formatted and updated all sections | Nate Nash |
| 03/12/2005 | 1.0 | Final | Lynda Roades |
| 03/21/2005 | 1.1 | Updated MOFDC rack diagram and updated IP address table to include FB servers, failover FirePass | Jay Hariani |
| Approval Date | Approved Version | Approver Role | Approver |
| | 1.0 | Internal Approval | Terence Murdoch |
| | | MoF Approval | Najwa Fathalla |

This document is protected under the copyright laws of the United States and/or other countries as an unpublished work. This document contains information that is proprietary and confidential to BearingPoint, Inc. and/or affiliates or its technical alliance partners, which shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate BearingPoint, Inc. and/or its affiliate(s). Any use or disclosure in whole or in part of this information without the express written permission of BearingPoint, Inc. and/or its affiliate(s) is prohibited.

© 2005 BearingPoint, Inc. and/or its affiliate(s) (Unpublished). All rights reserved.

The ProvenCourse methodology is a component of BearingPoint's ProvenCourse delivery framework and contains process, templates and techniques used to deliver BearingPoint services.

ProvenCourseSM, BearingPointTM, and Business and Systems Aligned. Business EmpoweredTM are trademarks or service marks of BearingPoint, Inc. and/or its affiliates.



TABLE OF CONTENTS

| | |
|--|----------|
| 1. INTRODUCTION..... | 1 |
| 1.1. SCOPE | 1 |
| 2. PRODUCTION ENVIRONMENT..... | 1 |
| 2.1. FACILITIES..... | 1 |
| 2.2. SOFTWARE AND HARDWARE | 2 |
| 2.3. OPERATIONS..... | 5 |
| 3. DEFINITIONS, ACRONYMS, AND ABBREVIATIONS..... | 7 |
| 4. OPEN ISSUES AND FUTURE CONSIDERATIONS..... | 8 |
| 4.1. COMPLETE PHYSICAL BUILD-OUT OF THE MOF DATA CENTER SERVER ROOM..... | 8 |
| 4.2. KNOWLEDGE TRANSFER TO MOF IT STAFF..... | 8 |
| 4.3. SECURE THE MOF DATA CENTER SERVER ROOM..... | 8 |
| 5. REFERENCES..... | 8 |
| APPENDICES..... | 9 |
| APPENDIX A – PRE-PRODUCTION / START-UP CHECKLIST – INITIAL AND DATE..... | 10 |
| APPENDIX B – NAMING CONVENTIONS, IP ADDRESSES, AND PASSWORDS..... | 11 |
| APPENDIX C – BUILD SHEETS..... | 13 |

1. INTRODUCTION

To assist the Iraqi government meet generally accepted standards in budget execution, the United States Agency for International Development (USAID) teamed with BearingPoint to implement a financial management information system, which is composed of FreeBalance eFinancials software, supporting hardware infrastructure, and the Ministry of Finance (MoF) local area network (LAN). This system provides the Iraqi government the basic tools for federal financial management, combined with the flexibility to adjust to a fluid political environment during this period of reconstruction. The Iraqi Financial Management Information System (IFMIS) will provide automated budget execution capabilities to all 62 Iraqi Federal spending units, and will be accessed on a regular basis by MoF staff and officials in Baghdad and remote sites.

This Production Environment Plan (Plan) provides the technical design specifications for IFMIS at the MoF Data Center. The MoF Data Center, located in Baghdad, is a critical facility designed and constructed to house computing resources related to both the operations of the MoF and IFMIS, the Iraqi Federal Government budget execution system. These resources include computer servers, network switching equipment, satellite communication systems, monitoring devices, and supporting hardware and software. This Plan targets the establishment of the infrastructure and production environment for the IFMIS, and will be updated periodically to reflect maturing business processes and other system changes.

1.1. Scope

The scope of this document covers the production environment (i.e. facilities, software and hardware, operations) of the MoF Data Center.

2. PRODUCTION ENVIRONMENT

2.1. Facilities

The following section describes the non-computing facilities and equipment for the MoF Data Center.

2.1.1. Equipment Space and Office Space

The MoF Data Center is one room on the first floor of the MoF Computer Center. The room is approximately 400 square feet and has room for three to four racks, two desks, and supporting equipment. There is a pre-existing raised floor and there are designs for additional climate control functionality and fire cessation capabilities.

The MoF Information Technology (IT) staff is housed in an adjacent room (200 square feet) with approximately six desks, computers, and one printer. This room will also function as the War Room and Operations Room to support the implementation of IFMIS.

2.1.2. Security and Access

The MoF Data Center server Room is a physically controlled, secured environment with climate control, and dedicated electrical and fire safety equipment. It has no windows, and access is restricted to the following individuals:

- BearingPoint Local IT Staff.
- BearingPoint IT Advisors.
- MoF IT Staff.

The MoF Data Center server room is secured with electronic access doors and only the above-authorized personnel have cards for entry. Unauthorized personnel are not allowed into the Data Center unless escorted by the MoF IT Manager or the BearingPoint Technical Lead. The racks within the Data Center are closed and locked 24-hours a day. The MoF IT Manager and the BearingPoint Technical Lead hold the only two keys.

The business continuity generator and fuel tanks are within a steel cage, which remains locked at all times.

Business hours for the building are Sunday through Thursday, 0830-1430. The MoF Computer Center is secured by armed guards 24-hours a day. It is surrounded by 8-foot blast walls and entry through the two gates is limited to staff of the MOF, staff of the Board of Supreme Audit, and approved foreign contractors.

2.1.3. Fire Protection

The MoF Data Center facility will be equipped with dry-chemical type fire extinguishers. The facility will have four fire extinguishers within the Data Center itself and additional units spread throughout the building.

2.1.4. Uninterruptible Power Supplies (UPS) and Generators

All servers, networking equipment and communication systems in the MoF Data Center will be connected to the main power source via UPS. These UPS will have sufficient capacity to function for up to ten minutes prior to failure. The UPS units utilized in the MoF Data Center will also support line conditioning features, allowing them to moderate the current supplied to the equipment, and prevent under-volt/over-volt conditions from causing damage or instability.

The UPS units will have their batteries checked and verified on a regular basis to verify they are still capable of supporting the equipments' load. In addition to the UPS units, the MoF Data Center is equipped with generators to provide backup power. These generators have the capability of cutting over from the municipal power grid in less than the ten-minute UPS power window provided. These generators will have regular maintenance performed on them. The MoF IT Staff support staff will contract with a local fuel vendor to deliver fuel to the location's storage tanks on a regular basis.

2.2. Software and Hardware

The following section describes the critical applications and supporting infrastructure hardware that are used at the MoF Data Center.

2.2.1. Free Balance: FBPROD, FBDEV, FBTEST, FBTRAIN

The core line-of-business application located at the Data Center is FreeBalance eFinancials version 4.6.2. Free Balance is a client-server based Microsoft Windows application, with a Microsoft SQL Server 2000 database backend. The four separate instances (FBPROD, FBDEV, FBTEST, and FBTRAIN) of Free Balance, as implemented in the MoF Data Center, run on three production servers. Each instance will run on its own physical server except for FBDEV and FBTEST, which will run on one physical server. These three servers will access individual SQL Server 2000 databases, and provide development and training environments respectively.

2.2.2. Microsoft SQL Server 2000: FBPROD, FBDEV, FBTEST, FBTRAIN

Microsoft SQL Server 2000 is currently running on FBPROD, FBDEV, FBTEST, and FBTRAIN patched to SP3a. These database servers host the Free Balance data store and configuration information. The database instance name is FBSQLPROD.

2.2.3. Microsoft Windows 2003 / Domain Controller: MOFDC-DC-01

Microsoft Windows Server 2003 provides Active Directory (AD) domain and authentication services, DNS, DHCP, and WINS to the MoF Data Center network.

2.2.4. Microsoft Windows 2003 / Domain Controller: MOFDC-DC-02

Microsoft Windows Server 2003 provides AD domain and authentication services to the MoF Data Center network.

2.2.5. Microsoft Windows 2003 Server: MOFDC-APPS-01

This server provides basic application serving functionality, print serving, anti-virus updates, and file storage.

2.2.6. Microsoft ISA Server: MOFDC-ISA-01

This server, running Windows Server 2003 Standard Edition and Microsoft ISA Server 2004, routes the MoF Data Center's wide area network (WAN) connection to the Internet via RRAS, and serves as a firewall. Currently, this server is homed to the LunaSat VSAT Internet WAN.

2.2.7. Microsoft ISA Server: MOFDC-ISA-02

This server is running Windows Server 2003 Standard Edition and Microsoft ISA Server 2004. It is configured identically to MOFDC-ISA-01, but is homed to the Plenexis VSAT Private WAN.

2.2.8. Microsoft Terminal Server: MOFDC-TERM-01

This server runs Windows Server 2000 and Microsoft Terminal Services. Its purpose is to distribute access to the FMIS application via the Fire Pass SSL VPN. When any client attempts to access the FMIS via their web browser, Fire Pass automatically launches a terminal session to present the application to the user.

2.2.9. Fire Pass

Fire Pass is a stand alone SSL VPN. It is the only access method for the MoF Data Center's network from remote locations. Fire Pass presents a web interface into any server or desktop client on in the MoF Data Center and MoF LAN.

2.2.10. Rack Diagram

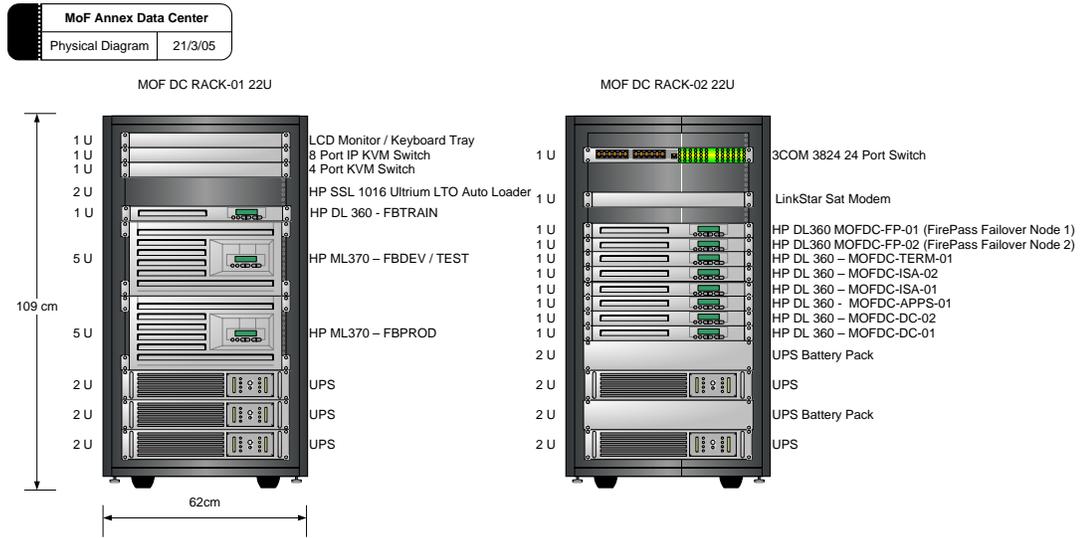


Figure 1: MoF Data Center Rack Diagram

2.2.11. Logical Architecture

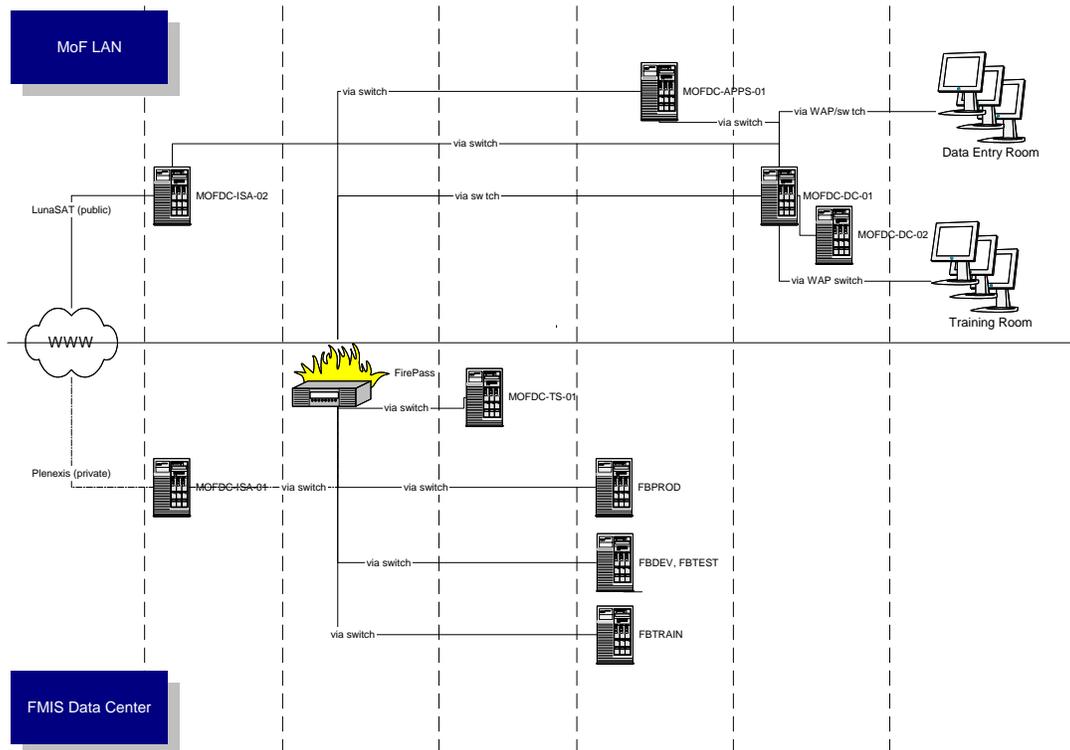


Figure 1: Logical Architecture

2.2.12. Communications Infrastructure

A LunaSat VSAT Internet WLAN, and a Plenexis VSAT Private WLAN are currently used for connectivity out of the MoF Data Center site.

2.3. Operations

2.3.1. Anti-Virus Software and Update Mechanism

The MoF Data Center will provide anti-virus protection via Symantec AntiVirus server and client. Both of these components are rolled out from the Symantec System Center console. When installing from the Symantec System Center console, FMIS uses Elevated Privileges rather than granting administrative privileges. The Symantec AntiVirus server program is installed on a single non-production Windows 2003 server, which becomes its primary server. Symantec AntiVirus client protects all other Windows-based network servers.

A central LiveUpdate server is placed in the environment from which all clients and servers retrieve virus definitions updates. The updates are randomly scheduled to reduce network bandwidth. The LiveUpdate server automatically retrieves virus definitions directly from Symantec. The server is set to automatically check Symantec site for updates once a day, preferably early morning.

2.3.2. Backup and Restore Strategy

Veritas NetBackup Data Center Media Server will provide backup infrastructure for the Data Center. Veritas NetBackup will be installed on all servers requiring backup, with the primary server designated the 'master server', and each subsequent server designated as the 'media server.' VERITAS NetBackup software accommodates multiple servers working together under the administrative control of one of the servers. The master server can also function as a media server.

All NetBackup administrative functions are performed centrally from the master server, and the master server controls all backup scheduling for each media server. Each of the media servers performs the actual backup operations under direction from the master, and backup data stays local to the media servers and their respective storage devices. A master server and its associated media servers are referred to collectively as a NetBackup storage domain, and large networks may have more than one domain. Client systems backup data to NetBackup servers.

2.3.2.1. Backup Job Types / Scheduling:

The Master Server and all Media Servers should have a full backup done on Friday each week, with incremental backups each day thereafter.

2.3.2.2. Rotation of Tapes:

Tapes are labeled for each day of the week (i.e. Monday through Thursday). Note: If weekend backups are needed, add appropriate tapes labeled for Saturday or Sunday. Additionally, another four tapes are labeled Fri1, Fri2, Fri3, and Fri4.

All servers get a full backup on Friday, after which the tape is to be removed off-site. On each subsequent Friday, the next 'FriX' tape is used for the full backup. On the last Friday of the month, the tape labeled Fri4 should be held out of rotation and stored off-site, and a new Fri4 tape labeled for use next month. Using this rotation, data can be recovered as far back as needed.

2.3.3. Patch Management

All servers updates (security updates and patches only) are to be performed via Windows Update, which is set to automatically check for critical updates on Microsoft website, and automatically download the update to each server. The administrator will install updates manually at an appropriate

time when the server may be rebooted. Once the first server has successfully rebooted, all subsequent installs should follow soon after.

Service pack updates should only be done after administrators agree on need for the update, and only after at least one week has passed since the release of the service pack. This allows enough time for any major problems to surface in the server community at large, which could indicate whether the particular service pack is stable. This protocol regarding security updates and patches should be followed: updating and rebooting one server successfully before applying updates/service packs to remaining servers.

2.3.3.1. HFNETCHK

This utility used to check the security patch level of various Windows operating systems, (e.g., Windows 2003 Server, Windows XP, Windows 2000). HFNETCHK is invoked using the Microsoft Baseline Security Analyzer (MBSA) as follows:

From command line of the appropriate computer, type: `mbsacli.exe /hf -v -z -s 1`

The results returned by this command indicate the patch-level of the computer, including references to Microsoft knowledge-base articles associated with these patches. Using this information, an administrator is able to determine if additional patches need to be applied. MBSA can also be run on remote computers (requiring Server service and Remote Registry service running on remote machines).

Note: The latest version of MBSA is Version 2.1, and can be downloaded from Microsoft download site at: <http://www.microsoft.com/downloads/search.aspx?displaylang=en>

2.3.4. Testing

Before the MoF Data Center is put into production, a series of tests will be performed on the network, servers, and communications equipment. These tests will verify that the system can be sustained once in production with the required levels of availability.

Other tests will verify that the system can accept remote administration requests, that there is sufficient bandwidth to support the level of IFMIS application users both internally and externally, and that the physical infrastructure supplies constant power and climate control.

The below list comprise a series of basic tests that must be completed before the system can be put into production:

- UPS Runtime: Verify that the UPS units provide sufficient power to keep servers and communications equipment functional until on-site power generation is able to switch over.
- Generator Switch-Over: Verify that the generators switch over from the municipal power grid automatically, and in a time period less than the UPS runtime window.
- FreeBalance eFinancials Application Test: Verify the function of the application.

2.3.5. Network Restart Procedure

In the event of power loss to the MoF Data Center, the network should be recovered in a specific manner. Servers and network devices contain certain dependencies for one another's availability. These dependencies need to be met in order to restart the network "gracefully," and in a way that will restore original, full functionality. In the event of a power loss situation, follow this procedure.

- Verify municipal or generator power is functioning: If under generator power, be sure to determine that sufficient fuel remains to retain power to the network.



Iraq Economic Governance II

- Start communications equipment: This includes switches, VSATs, and routers. Follow the individual procedures located for starting the individual pieces of equipment. These can be found in the equipment’s user manual.
- Verify internal and inbound connectivity: To check for internal connectivity, login to one of the client PCs, and attempt to ping a server on the network, or vice versa. If internal connectivity is unavailable, troubleshoot and resolve this issue before continuing.
- Start Domain Controller: This server is essential to network logon and authentication, and must be active before other serves on the network can be brought on line. If the domain controller is not responding to ping requests or is unable to be accessed via Terminal Services/Remote Desktop, troubleshoot this issue before continuing.
- Start ISA Servers: Activate the ISA servers on the network, and wait for them to come on line. This may take several minutes. ISA Servers provide routing and firewall services, and are essential to the operation of both the client personal computers (PC) and MoF Data Center servers. If the ISA Servers are not responding to ping requests or are unable to be accessed via Terminal Services/Remote Desktop, troubleshoot this issue before continuing.
- Verify outbound connectivity: Check for access to the WAN, or Internet. To do this, login to a client PC or server, and attempt to ping a host on the Internet. This could be any common site. If ping packets are not returned, troubleshoot and resolve this issue before continuing.
- Start Domain Controller: This server is essential to network logon and authentication, and must be active before other serves on the network can be brought on line. If the domain controller are not responding to ping requests or are unable to be accessed via Terminal Services/Remote Desktop, troubleshoot this issue before continuing.
- Start Production Servers: Start Free Balance, SQL Database Servers, and any other production servers. Verify functioning of Free Balance application, and verify database start up has been successful.
- Start Fire Pass: Start Fire Pass and verify it is accessible internally and externally.
- Start Client PCs: Start client PCs, and verify that they can access applications, other internal resources and the Internet.

3. DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

| | |
|-------|--|
| AD | Active Directory |
| IFMIS | Iraqi Financial Management Information System |
| IT | Information Technology |
| LAN | Local Area Network |
| MBSA | Microsoft Baseline Security Analyzer |
| MoF | Ministry of Finance |
| MS | Microsoft |
| PC | Personal Computer |
| UPS | Uninterrupted Power Supply |
| USAID | United States Agency for International Development |
| WAN | Wide Area Network |

4. OPEN ISSUES AND FUTURE CONSIDERATIONS

4.1. Complete Physical Build-Out of the MoF Data Center Server Room

In order for the technical environment to function as designed to support the Government of Iraq's Federal budget execution, the MoF IT must complete the following tasks:

- Complete installation of electrical wiring
- Install air conditioning units
- Tint or shade the windows
- Install a secure door
- Place four dry-chemical type fire extinguishers in the server room
- Contract for fuel services for the dedicated generator

4.2. Knowledge Transfer to MoF IT Staff

As BearingPoint is provisioning the IT hardware environment at the MoF Data Center, this offers the MoF IT staff an opportunity to gain practical experience in working with the technology. We recommend that the MoF IT Director General:

- Identify staff members who will be responsible for day-to-day operations so they can “shadow” their BearingPoint counterparts and become familiar with the equipment, procedures, and technology prior to Go-Live
- Start and stop the servers at the beginning (0830 hours, local time) and end (1400 hours, local time) to establish business practices prior to full implementation

4.3. Secure the MoF Data Center Server Room

At present, the MoF Data Center server room does not meet international practices for security. BearingPoint recommends that the MoF IT Director General establish security policies and procedures, and enforce those as much as is practicable (e.g., keeping the door to the server room closed).

5. REFERENCES

Go-Live Support Plan, March 11, 2005, BearingPoint, Inc.

APPENDICES

Appendix A – Pre-Production / Start-Up Checklist – Initial and Date

1. _____ - UPS Runtime test complete.
2. _____ - Generator switch-over test complete
3. _____ - Fuel delivery contract established.
4. _____ - FMIS Application tests complete.
5. _____ - Remote access to system verified.
6. _____ - Check client connectivity from training and data entry rooms.
7. _____ - Check client access to wireless access points (WAPs).
8. _____ - Check client access to printers.
9. _____ - Access list to server room complete, and access limited.
10. _____ - Fire extinguishers placed in Server Room
11. _____ - AC/climate control deemed sufficient
12. _____ - Server Room windows bricked.
13. _____ - Backup and Recovery Plan established
14. _____ - “Start State” gold backup performed and kept at BE Camp.
15. _____ - Offsite backup location established.
16. _____ - Test restore performed.
17. _____ - Racks locked, keys given to local point of contact.
18. _____ - Copies of finalized IDS delivered to local points of contact.

Appendix B – Naming Conventions, IP Addresses, and Passwords

Naming Conventions

The MoF Data Center will use standard naming conventions for all servers, printers, routers, switches and users. The naming conventions are as follows:

Servers: MOFDC-ROLENAME-NUMBER, for example: MOFDC-ISA-01

Printers: MOFDC-PRINTERNAME-LOCATION, for example: MOFDC-HP-TRAINING

Switches: MOFDC-SW-Number, for example: MOFDC-SW-01

Routers: MOFDC-RT-Number, for example: MOFDC-RT-01

IP Addressing

IP Ranges:

| | |
|-----------------------------------|-------------------------|
| Subnet mask | 255.255.0.0 |
| IP Range – Servers | 10.1.3.1 – 10.1.3.254 |
| IP Range - Routers | 10.1.1.1 – 10.1.1.254 |
| IP Range - Switches | 10.1.2.1 – 10.1.2.128 |
| IP Range - Wireless Access Points | 10.1.2.129 – 10.1.2.254 |
| IP Range – Printers | 10.1.4.1 – 10.1.4.254 |
| IP Range – Work Stations | 10.1.74.1 – 10.1.74.254 |

Server IP Addresses:

| | |
|---------------|-----------|
| MOFDC-DC-01 | 10.1.3.2 |
| MOFDC-DC-02 | 10.1.3.5 |
| FBPROD | 10.1.3.16 |
| FBTRAIN | 10.1.3.17 |
| FBDEV | 10.1.3.15 |
| MOFDC-ISA-01 | 10.1.3.1 |
| MOFDC-ISA-02 | 10.1.3.3 |
| MOFDC-TERM-01 | 10.1.3.6 |
| MOFDC-APPS-01 | 10.1.3.4 |
| Firepass - 1 | 10.1.3.10 |
| Firepass - 2 | 10.1.3.11 |

Iraq Economic Governance II

Passwords

| Supplicant | Password |
|---|-----------|
| Local Admin Password – Client PCs | Sun\$et! |
| Local Admin Password – Servers (mofadmin) | 498xmtY#X |
| Domain Admin Password (mofadmin) | !t1zaj89x |
| Switch Password | |
| Router Passwords | |
| Printer Passwords | |
| Other Passwords | |
| DC Restore Passwords | trz61x3! |
| Local Admin Password (During Setup) | 498xmtY |
| FirePass Admin (fpadmin) | dead2you! |

Appendix C – Build Sheets

Client Workstation Image Build Check List

HP DX6100

Version: FMIS-HP-DX6100 Ver:1.0

Date: 7 / March / 2005

| Item | Version | |
|--|-----------------|---|
| Operating System: | | |
| Windows XP Pro (Corporate Edition) | | √ |
| Set Local Admin Password to | Sun\$et! | √ |
| Windows XP Service Pack 2 (SP2) | | √ |
| Windows Critical Updates | latest (7/3/05) | √ |
| Copy the Installation files into the folder C:\I386\ and change the registry installation path | | √ |
| Device Driver: | | |
| Chipset Driver | | √ |
| Network LOM Card Driver | | √ |
| Wireless LAN Driver (If exist) | | |
| Video Card Driver | | √ |
| Sound Card Driver | | √ |
| USB 2.0 Driver | | √ |
| Other Peripherals Driver | | |
| BIOS Update | | √ |
| Programs: | | |
| Microsoft Office 2003 (Corporate Edition) Complete Installation | | √ |
| MS Office 2003 Service Pack 1 (SP1) | | √ |
| MS Office 2003 Critical Updates | latest (7/3/05) | √ |
| MS Visio Viewer | | √ |
| Windows Media Player 10 | | √ |
| Adobe Acrobat Reader | 7.0 | √ |
| Macromedia Flash 7 | | √ |
| Real Player light | | √ |
| SpyWare Programs: | | |
| MS AntiSpyware | Beta | √ |
| Ad Aware | SE 1.05 | √ |
| Anti Virus Program: Only one | | |
| AVG 7.0 (Free Edition) | | √ |

CD-Key: J7MJP-RMMYM-4FC4H-J8R6K-C42DM

Check: www.windowsupdate.com

Change the Registry
 HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Setup\Source path into C:\

Check: support.HP.com

Note: Install all the drivers in one folder called **Drivers** in the C Drive

CD-Key: QVY8V-V2QPQ-MCQ43-VHWQX-X9G7M

Check : www.officeupdate.com

Check : www.microsoft.com

Check: www.adobe.com

Check: www.adobe.com

Check: www.grisoft.com



Iraq Economic Governance II

| | | |
|---|--|---|
| Other Settings: | | |
| Install the Arabic Support & Keyboard | | √ |
| Set the non-Unicode for Arabic (Saudia Arabia) | | √ |
| Set the Arabic As Default Language | | √ |
| Enable Remote Access | | √ |
| Enable Remote Desktop | | √ |
| Enable Auto Update | | √ |
| Enable Firewall on the NIC card | | √ |
| Pre-Image Settings: | | |
| Delete the prefetch files | | √ |
| Delete the Temp Files | | √ |
| Delete the temp internet files, cookies & the History | | √ |
| Run SysPrep with the Reseal option | | √ |
| Image Phase: | | |
| Imaging using the Image for DOS | | √ |
| Burn the Image on CDs & DVDs | | √ |

Client Workstation
Image Build Check List

Version:

Date: / / 2005

| Item | Version | |
|--|----------------|---|
| Operating System: | | |
| Windows XP Pro (Corporate Edition) | | √ |
| Set Local Admin Password to | | |
| Windows XP Service Pack 2 (SP2) | | |
| Windows Critical Updates | | |
| Copy the Installation files into the folder C:\I386\ and change the registry installation path | | |
| Create a Local user Account | | |
| Device Driver: | | |
| Chipset Driver | | |
| Network LOM Card Driver | | |
| Wireless LAN Driver (If exist) | | |
| Video Card Driver | | |
| Sound Card Driver | | |
| USB 2.0 Driver | | |
| CD Burner Driver (if exist) | | |

CD-Key: J7MJP-RMMYM-4FC4H-J8R6K-C42DM

Check: www.windowsupdate.com

Change the Registry
 HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Setup
 ource path into C:\

Note: Install all the drivers in one folder called **Drivers** in the C: Drive



Iraq Economic Governance II

| | | |
|---|----------|--|
| Other Peripherals Driver | | |
| BIOS Update | | |
| | | |
| Programs: | | |
| Microsoft Office 2003 (Corporate Edition) Complete Installation | | |
| MS Office 2003 Service Pack 1 (SP1) | | |
| MS Office 2003 Critical Updates | | |
| MS Visio Viewer | | |
| Windows Media Player 10 | | |
| Adobe Acrobat Reader 7.0 | | |
| Macromedia Flash 7 | | |
| Yahoo Messenger 6.0 | | |
| MSN Messenger 6.2 / Its security update | | |
| Real Player light | | |
| Nero Burner (if burner exist) | | |
| Winzip | 9.0 SR-1 | |
| | | |
| SpyWare Programs: | | |
| MS AntiSpyware (Beta) | | |
| Ad Aware | | |
| | | |
| Anti Virus Program: Only one | | |
| Norton Anti-Virus (Corporate Edition) | | |
| AVG 7.0 (Free Edition) | | |
| | | |
| Other Settings: | | |
| Install the Arabic Support & Keyboard | | |
| Set the non-Unicode for Arabic (Saudia Arabia) | | |
| Set the Arabic As Default Language | | |
| Enable Remote Access | | |
| Enable Remote Desktop | | |
| Enable Auto Update | | |
| Enable Firewall on the NIC card | | |
| | | |
| Pre-Image Settings: | | |
| Delete the prefetch files | | |
| Delete the Temp Files | | |
| Delete the temp internet files, cookies & the History | | |
| Run SysPrep with the Reseal option | | |

CD-Key: QVY8V-V2QPQ-MCQ43-VHWQX-X9G7M

Check : www.officeupdate.com
 check: download.microsoft.com
 Check : www.microsoft.com
 Check: www.adobe.com
 Check : www.flash.com
 Check: messenger.yahoo.com
 Check: messenger.msn.com

Check: download.microsoft.com

Check: www.grisoft.com

