***Active Directory Deliverables Request List***

**Active Directory Operations**

*Schema Modifications*

ADO.1.1 – List of all schema modifications made during 2/1/2008 - 7/1/2009.

ADO.1.2 - Members of the “Schema Admin” group.

ADO.1.3 - AD network diagram.

ADO.1.4 – Screen shot or command line output to identify the Schema master (cmd> dsquery

server –hasfsmo schema)

ADO.1.5 - The following registry key for the schema master identified in ADO.1.4:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\ Schema Update Allowed

*Performance Monitoring*

ADO.2.1 – List of AD monitoring tools utilized (including whether or not Active Directory

Management Pack is installed).

ADO.2.2 – List of monitoring reports used and an example of each.

ADO.2.3 - Monitoring baseline thresholds established by management.

*Periodic Maintenance*

ADO.3.1 - List of all maintenance tasks performed between 2/1/2008 - 7/1/2009.

Ideally this will be a summary of remedy tickets.

ADO.3.2 - Change control details for a sample of maintenance tickets.

*Backup and Restore*

ADO.4.1 – List of operations master role machines in the root domain, all domain controllers

with operations master role in all child domains, and all global catalog servers.

ADO.4.2 - Backup schedule for all Active Directory components.

ADO.4.3 - List of who can perform backup and restore operations.

*Log Collection*

ADO.5.1 - Screen prints showing the sizes of each log for each domain controller. Should be

three screen shots per server. To perform this, go to “Computer Management\Event

Viewer” then right click on each log and take a screen shot of the “Properties” screen.

ADO.5.2 - Screen prints of the settings located here: “Computer Configuration\Windows

Settings\Security Settings\Event Log\Settings for Event Logs”

ADO.5.3 - Audit policy settings for each domain controller. Go to: Administrative Tools\Local

Security Policy. Capture screen print of Security Settings\Local Policies\

Audit Policy.

ADO.5.4- Additional audit policy settings for each domain controller: Go to: Computer

Configuration\Windows Settings\Security Settings\Local Policies\Security Options\.

Capture a screen print of each option.

*Log Review*

ADO.6.1 - Copies of audit log reports reviewed and all research performed for a sample of 4

weeks. This will include remedy ticket research, emails, etc. The sample 4 weeks are

as follows:

4/21/08 - 4/25/08,

7/14/08 - 7/18/08,

10/6/08 - 10/10/08,

1/5/09 - 1/9/09

ADO.6.2 - Provide proof that audit logs are backed up and maintained for 1 year. This should be

the following:  
  
 1. A backup job that is scheduled for daily back.   
 2. Proof that the following dates are backed up (i.e. a timestamp on a backup file):

2/21/08,

3/3/08,

4/4/08,

4/29/08,

5/5/08

*Antivirus*

ADO.7.1 - Screen print showing installation of antivirus software for each domain controller.

ADO.7.2 - Screen print of configuration to get updates on a regular basis.

ADO.7.3 - Version information for the DAT file (virus signature file) for each domain controller.

**Authentication and Access Controls**

*Segregation of SysAdmin and SecAdmin Duties*

AA.1.1 - Policies and procedures documenting the system and security administration activities.

*Authentication Protocols*

AA.2.1 - Screen prints of the following two registry keys:

HKEY\_Local\_Machine\system\CurrentControlSet\Control\LSA

Value:LMCompatability

HKEY\_Local\_Machine\system\CurrentControlSet\Control\LSA

Value:NoLMHash

*Anonymous Access*

AA.3.1 - Screen print of the following registry setting:

HKEY\_Local\_Machine\system\CurrentControlSet\Control\LSA

Value: RestrictAnonymous

*Local Users and Groups*

AA.4.1 - Listing of each local user account on each domain controller:

net user >> net\_user\_output.txt

AA.4.2 - For each user account listed in AA.4.1 above run the following command to get

account details:

net user [user\_account\_name] >>

net\_user\_[user\_account\_name]\_detail\_output.txt

AA.4.3 - Listing of each local group on each domain controller

net localgroup >> net\_localgroup\_output.txt

AA.4.4 - For each group listed in AA.4.3 above, run the following command to get the group

details:

net localgroup [group\_name] >>

net\_localgroup\_[group\_name]\_detail.txt

AA.4.5 - Policies and procedures regarding the adminstration of local domain controller accounts

and groups.

*File Permissions*

AA.5.1 - The output from the following commands:

cacls C:\Windows\inf >> cacls\_c\_windows\_inf.txt

cacls C:\Windows\NTDS >> cacls\_c\_windows\_ntds.txt

cacls C:\Windows\ntfrs >> cacls\_c\_windows\_ntfrs.txt

cacls C:\Windows\repair >> cacls\_c\_windows\_repair.txt

cacls C:\Windows\security >> cacls\_c\_windows\_security.txt

cacls C:\Windows\system >> cacls\_c\_windows\_system.txt

cacls C:\Windows\system32 >> cacls\_c\_windows\_system32.txt

cacls C:\Windows\SYSVOL >> cacls\_c\_windows\_sysvol.txt

AA.5.2 - The output from the following commands:

net share >> net\_share\_output.txt

For each share identified in the command above, run the following command:

net share [share\_name] >> net\_share\_[share\_name]\_output.txt

*Trusts*

AA.6.1 - Screen prints of all trust and trust properties for all domains and forests (if multiple

exist). The Active Directory Domains and Trust Console can be used to perform this

step.

AA.6.2 - Evidence of trust relationship recertification with appropriate approvals.

*Active Directory Groups*

AA.7.1 - A list of all high-risk global groups. This would include any system administration

groups.

AA.7.2 - A list of all changes made to the high-risk global groups identified in AA.7.1.

AA.7.3 - List of all members of the following groups:

Domain Admins,

Enterprise Admins,

Schema Admins,

Group Policy Creator Owner

AA.7.4 - The output of the following command:

DumpSec.exe /rpt=groups /computer=\\USA /outfile=USA\_groups.txt /saveas=tsv

/noheader

*Active Directory Users*

AA.8.1 - List of all user profile changes made from 2/1/2008 - 7/1/2009.

AA.8.2 - Output of the following:

DumpSec.exe /rpt=users /computer=\\[Domain] /outfile=[out\_file\_name.txt]

/saveas=tsv /noheader

AA.8.3 - List of all active and terminated users as of 7/1/2009.

*Functional/Application Accounts*

AA.9.1 – Inventory of all functional/application IDs that exist either on a domain controller or in

active directory.

AA.9.2 – Any entitlement review reports for functional/application IDs.

AA.9.3 - All functional/application profiles created during 2/1/2008 - 7/1/2009.

*Entitlement Review*

AA.11.1 - Policies and procedures surrounding the entitlement review process. Also, any policies

and procedures around the open share review process.

AA.11.2 – Any entitlement recertification reports.

AA.11.3 - The ACL for a sample of critical shares on the network. Some examples:

\\Bes01psp\Logs (Blackberry call logs, sms logs, pin logs)

\\Dilbert (See: \\Dilbert\H\scripts\Test scripts\telnet\_dump.txt)

\\msg08psp\files

..add more here…

*Group Policy – Domain*

ADP.1.1 - Output from the following command:

DumpSec.exe /rpt=policies /computer=\\USA /outfile=AD\_USA\_Policies.txt

/saveas=tsv /noheader

ADP.1.2 - Perform the following:

1. Open Active Directory Users and Computers, right-click your domain, and then

click Properties.

1. In your properties dialog box for your domain, click the Group Policy tab, select

the Domain Policy GPO, and then click Edit to open the Group Policy Object Editor.

1. Under Computer Configuration, go to the Windows Settings\Security

Settings\Account Policies\Password Policy folder and the 'Account Lockout' folder and take screen prints of these settings.

ADP.1.3 - All domain security policy changes made during 2/1/2008 - 7/1/2009.

*Group Policy - Local and Other*

ADP.2.1 – Screen prints from the gpedit.msc tool

ADP.2.2 – Group policy changes made during the timeframe 2/1/2008 – 7/1/2009.

**Vulnerabilities and Threats Management**

*Services*

ADVM.1.1 - Output of the following command:

sc query type= service state= all

*Legal Banner*

ADVM.2.1 - Screen prints showing legal banner, no auto logon, and that the user name of last

logon user is not displayed.

*Patch Management*

ADVM.3.1 - Output of the MBSA tool.