

Attachment E - Explore IRP Disaster Recovery Strategy Document

1. Introduction

This is a Disaster Recovery Strategy Document for the Explore IRP system as it is proposed for MDOS and required for the RFP.

The document describes Explore's strategy for recovering daily IRP processing during system outages.

2. Disaster Recovery for Purposes of this Document

A disaster is any interruption to the computer operation that disrupts the critical business functions as defined by the business unit. A maximum allowable time for Explore IRP to be unavailable needs to be established (Explore will work with MDOS to determine this number). Explore is assuming 72 hours for the strategy document.

3. Assumptions

- The document strategy includes the ability to recover from the "worst case" destruction of the Explore IRP operating environment. The worst case includes any non-data processing function that may be in close proximity to the data center or workstations.
- Explore IRP is being hosted at the Explore/USIS data center in Tulsa, OK.
- Explore/USIS operates a backup data center in Grove City, PA.

4. Infrastructure

The IT infrastructure for Explore IRP consists of the following: (Proposed infrastructure has been listed)

Production Environment

Server Requirements	#	Description
Load Balancers (Primary and Backup)	2	
Web Servers	2	Duo Core 2.0 GHz Processors 2GB RAM 18 GB available for OS 50 GB available for Apps/Code/Files Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses HW/SQ Monitoring
Application Servers	2	Duo Core 2.0 GHz Processors 2GB RAM 18 GB available for OS 50 GB available for Apps/Code/Files Microsoft ® Windows 2003 Standard

Vehicle Registration System

		Microsoft ® Windows 2003 Internet Licenses HW/SQ Monitoring Anex 2D Barcode NetAddress 3.5 Active PDF Tool Kit
Active Clustered Database Server	2	Duo Core 2.0 GHz Processors 8GB RAM 18 GB available for OS 300 GB available for Database and Logs Microsoft ® Windows 2003 Enterprise Microsoft ® SQL Server Reporting Services Microsoft ® SQL Server Enterprise Edition 2005 HW/SQ Monitoring
Passive Clustered Database Server	2	Duo Core 2.0 GHz Processors 8GB RAM 18 GB available for OS 300 GB available for Database and Logs Microsoft ® Windows 2003 Enterprise Microsoft ® SQL Server Reporting Services Microsoft ® SQL Server Enterprise Edition 2005 HW/SQ Monitoring

Development, Test and Training Environment

Server Requirements	#	Description
VMWare Web Server/Application Server (should total from below)	1	Duo Core 2.0 GHz Processors 8GB RAM 300 GB available for virtual servers Microsoft ® Windows 2003 Enterprise Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses VMWare ESX 2.x
Virtual Web Server (1 for development, 1 for test environment)	3	1GB RAM 18 GB available for OS 25 GB available for Apps/Code/Files Microsoft ® Windows 2003 Enterprise Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses Anex 2D Barcode NetAddress 3.5 Active PDF Tool Kit
Virtual Application Server (1 for development, 1 for test environment)	3	1GB RAM 18 GB available for OS

Vehicle Registration System

		25 GB available for Apps/Code/Files Microsoft ® Windows 2003 Enterprise Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses
Database Server (includes instances for dev, test, and training environment)	2	Duo Core 2.0 GHz Processors 8GB RAM 18 GB available for OS 750 GB available for Database and Logs Microsoft ® Windows 2003 Enterprise Microsoft ® SQL Server Reporting Services Microsoft ® SQL Server Standard Edition 2005 HW/SQ Monitoring

Explore/USIS has a disaster recovery center in Grove City, PA. The following equipment will be located in Grove City for the purposes of site redundancy.

Server Requirements	#	Description
Web Server	1	Duo Core 2.0 GHz Processors 2GB RAM 18 GB available for OS 50 GB available for Apps/Code/Files Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses HW/SQ Monitoring
Application Server	1	Duo Core 2.0 GHz Processors 2GB RAM 18 GB available for OS 50 GB available for Apps/Code/Files Microsoft ® Windows 2003 Standard Microsoft ® Windows 2003 Internet Licenses HW/SQ Monitoring Anex 2D Barcode NetAddress 3.5 Active PDF Tool Kit
Active Clustered Database Server	1	Duo Core 2.0 GHz Processors 8GB RAM 18 GB available for OS 300 GB available for Database and Logs Microsoft ® Windows 2003 Enterprise Microsoft ® SQL Server Reporting Services Microsoft ® SQL Server Enterprise Edition 2005 HW/SQ Monitoring

5. Disaster Recovery Team

A Disaster Recovery Team needs to be established. The Disaster Recovery Team is responsible for the damage assessment of the Explore IRP system as quickly as possible following a disaster, and reports the level of damage to MDIT Management, as appropriate. This team is also responsible for the recovery of the critical Explore IRP systems, including the operating systems, application software, and data. In general, the responsibilities of this team are:

Pre-Disaster

- Understand role and responsibilities within the MDOS Overall Disaster Recovery Plan and the Explore IRP Disaster Recovery Plan.
- Work together closely to reduce possibility for disaster in the data center
- Train employees in emergency preparedness
- Participate in disaster recovery tests as required

Post-Disaster

- Assess extent of damage to the Explore IRP systems, communication links, etc.
- Estimate time to recover based upon damage assessment
- Identify salvageable hardware and communication equipment
- Apprise management on the extent of damages, estimated recovery time, and salvageable equipment
- Maintain log of salvageable hardware and equipment
- Coordinate with vendors and suppliers in restoring, repairing or replacing salvageable hardware and equipment
- Implement the details of the Explore IRP Disaster Recovery Plan:
 - Restore operating system, applications and network software from backup medium
 - Test and verify operating system, applications and network software
 - Modify configuration to meet alternative site configuration
 - Connecting local and remote users to an alternate site.
 - Communicate progress to management on a timely basis
- Members of the team will be identified in the Explore IRP Disaster Recovery Plan

6. Outage Prevention

The Explore IRP system environment incorporates numerous redundancy features.

- Load balancers are redundant, allowing one to fail with no loss of system capabilities
- Two pairs of web and middle tier servers are included in the production environment. With the use of the load balancers, one set of servers can be lost while the other set will continue to operate.
- There is 3rd party service monitoring of Explore IRP web site availability with real time alerts when the site is unresponsive.
- There is Hardware and Operating System monitoring of disk space, CPU load, and performance.
- At the primary location, SQL Servers are clustered allowing one to pickup processing for the other if one should fail. In addition, the disaster recovery site

~~Vehicle Registration System~~

will also house a SQL server that will be kept up to date using log shipping and can be activated should the primary site be lost.

- Each of the servers has redundant power supplies, RAID arrays for storage, and error correction memory.
- Daily backups of the database are to be retained for one month.
- Backups are rotated to an off-site storage facility.
- In the event of a serious failure of multiple machines, we have the capability of reconfiguring the stage environment for use in production.

7. Notification Process

- Outage identified (by either party).
- The party that identifies the outage will contact the other party.
- Explore will post a System Down notice on the system.
- Explore determines cause for outage and resolution strategy. This may require MDIT assistance.
- Explore notifies MDOS of resolution steps and timeframes.
- If a move to the Disaster Recovery Database (DR) is required, this will be agreed upon and enacted by Explore.
- Explore will switch to DR environment
- Explore notifies MDOS that Explore IRP is available.
- Explore removes System Down notice.
- Preparations are made to switch back to the primary production environment after the necessary corrections are made.

8. Recovery Information

Various types of outages can occur. We have listed the most common outages that are anticipated with related information.

The steps listed in the recovery responsibilities column is meant to be an overview of the high level responsibilities for each event. It is not intended to be an exhaustive listing of every step.

Failure	Impact	Resolution	Recovery Responsibilities
Single Disk Drive on any one of the servers	Will not cause an outage if replaced before another failure occurs.	Procure replacement hard drive and install it.	Explore to maintain replacement parts. Explore to verify replacement was successful.
Single power supply failure on any one of the servers	Will not cause an outage if replace before another failure occurs.	Procure replacement power supply and install it.	Explore to maintain replacement parts. Explore to verify replacement was successful.

Vehicle Registration System

Failure	Impact	Resolution	Recovery Responsibilities
<p>Loss of multiple disk drives in a single RAID array</p>	<p>If the system is web or middle tier, the problem will not cause an outage. The pair of servers will be removed from the load balancing pool until repaired.</p> <p>If the system is SQL server, there will be a system outage.</p>	<p>If web or middle tier, correct the error and add back to load balancing pool. May require restore from backups.</p> <p>If SQL server, a switch to the DR SQL server will be completed.</p>	<p>Explore to maintain replacement parts.</p> <p>Explore to direct and coordinate overall response and verify recovery is complete.</p>
<p>Failure of network interface card on any server</p>	<p>If the system is web or middle tier, the problem will not cause an outage. The pair of servers will be removed from the load balancing pool until repaired.</p> <p>If the system is SQL server, there will be a system outage.</p>	<p>If web or middle tier, correct the error and add back to load balancing pool. May require restore from backups.</p> <p>If SQL server, replace the card using parts from the DR machine or other servers. If no parts are available then a switch to the DR server is required.</p>	<p>Explore to maintain replacement parts.</p> <p>Explore to direct and coordinate overall response and verify recovery is complete.</p>
<p>Failure of one of the load balancers</p>	<p>No outage will occur, the secondary load balancer will pickup for the primary.</p>	<p>Repair primary load balancer and restore it back into the environment.</p>	<p>Explore will replace load balancer and physically install it.</p> <p>Explore to configure new load balancer and verify replacement was successful.</p>

Vehicle Registration System

Failure	Impact	Resolution	Recovery Responsibilities
Failure of both load balancers	Outage will occur.	Since no spare parts will be on hand for the load balancers, we could point the DNS to one of the two pairs of servers until replacement load balancers arrive.	Explore will replace load balancers and physically install them. Explore will change DNS server to point to one of the web paths and change it back to the load balancers when recovery is complete. Explore to configure new load balancers, direct and coordinate overall response and verify recovery is complete.
Application code move causes system failure.	Outage could be partial or complete depending on the type of error.	Whenever possible, restore application to the state it was in prior to the application move, or work on a hot fix for immediate installation.	Explore responsible for overall identification and recovery action.
Database Corruption	Will cause an outage. Most likely the DR environment will be corrupt too.	Will require a restore from database backup and a roll-forward of logs up to the point right before the problem occurred.	Explore will direct and execute the overall recovery effort and verify recovery is complete.
Loss of network capabilities	Will cause an outage	System will be down until the problem can be corrected.	Explore will identify and correct the problem and verify that recovery is complete.

Vehicle Registration System

Failure	Impact	Resolution	Recovery Responsibilities
Loss of data center access (biological threat, gas leak, etc.)	Will not cause an outage by itself since systems are managed remotely. If an event occurs that requires direct access to the servers then an outage would occur at that point.		Switch to Explore Disaster Recovery Center. Explore will continue to keep the system operational while resolution is in process as long as remote capabilities are available.
Data center destroyed	Will cause outage until switch to Explore/USIS disaster recovery center is made.	Switch to Explore/USIS Disaster Recovery Center.	Explore to direct the overall recovery effort and verification that the system is ready to be resumed.

External Interfaces	
Interface	Impact
FMCSA Database	This is used to download the database of valid USDOT# and ICC# holders. Impact TBD.
SMTP Server Fails	Email will not be delivered for events requiring it.
BAM COMET	Vehicle data for fleet additions may not be available.
MDOS ARS	This allows staff to determine when carriers have made payments so that credentials may be issued. Impact TBD.
MDOS Inventory Database	This is used to update plate issuance information. Impact TBD.
MDOT CPAS	CPAS is a real-time interface that facilitates credit card and ACH payments. Without the interface being live, TxIRP will not be able to accept electronic payments. Cash and check will still be available.
IRP Clearinghouse	This is a monthly file transfer with the file needing to be submitted by the 10 th of each month. It is not likely that an outage will prevent this process from occurring.

9. System Build Documentation

Explore will keep a current copy of the system build documents for each of the servers in the escrow account that will hold a copy of the source code.