Secretary of State

FY09 Information Technology Plan

Submitted September 04, 2007

FY09 IT Plan - New Mexico Secretary of State

I. Executive Summary

The Information Technology Division of the New Mexico Secretary of State's Office is committed to providing state-of-the-art technology and infrastructure support to support legacy applications as well as developing new systems that are appropriate to its environment and application demands. We are focused on serving the public and upholding the laws of the state of New Mexico providing day-to-day functionality and support to the agency and the citizens of the state on an on-going basis.

Agency IT staff has worked hard for a number of years to implement the statewide Voter Registration and Elections Management system (VREMS) as mandated by the Help America Vote Act (HAVA) and the Secretary of State Knowledge Base (SOSKB). The implementation of both these centralized systems offer our users and the general public state-of-the-art IT systems.

VREMS and SOSKB

Additional base budget on statewide VREMS and SOSKB will be required for continued support and development of these existing applications and systems environment long term . In particular, the annual support fees for the statewide voter registration system will be approximately $561,304 in FY09 with the current configuration. The recurring annual support fees for the SOSKB environment is estimated at $53,393 in FY09.

Network Equipment Obsolescence Replacement

Obsolescence replacement funds will need to be secured to replace all critical Cisco Catalyst Switch equipment and firewall equipment and software to ensure a reliable and secure infrastructure is in place to continue to support the VREMS, SOSKB and other SOS application requirements. Today, the network hardware and software installed is obsolete and end-of-life. It will be critical to ensure timely replacement of this network hardware to be pro-active before any issues arise as a result of hardware faults and failures. The equipment replacement fund request is estimated at approximately $35,000.

Computer Room Enhancement and Compliance

The SOS is also working to address the environmental and climate control measures necessary to bring its designated Equipment Room up to code and specifications. It is vital to be compliant with all equipment and state standards to ensure business continuity and maximum uptime. The server and network equipment currently residing in this facility is vital and strategic to the SOS application needs and requires proper fire suppression measures are installed, climate control systems, facility monitoring equipment and meets all building code and hardware/software requirements. The SOS has contacted the Legislative Council Services to help address the agency needs but will also request additional funding and support to accomplish this initiative in a timely and efficient manner. Initial estimates for the Phase I improvements are estimated at approximately $500,000.

Dedicated Internet Access Services and Security

Another goal for the SOS Office is to establish added redundancy capability for access to the global Internet. While the SOS will maintain its primary connection to the Internet through a shared connection at GSD, the SOS also requires a dedicated 6Mbps connection to the Internet to ensure backup and redundancy options exist to support its end-user community and general public access. The recurring cost for the dedicated connection is estimated at approximately $3,311 per month based on a 1-year term, or approximately at $39,732 annually.

Political Financial Reporting System (PFRS)

The SOS continues to pursue the re-design and implementation of a strategic Political Financial Reporting System (PFRS), based on agency and legal requirements to ensure accurate and timely reporting on an on-going basis. The system will allow candidates and political committees to file campaign reports as required by law. It is estimated in FY09 that approximately $175,000 will be required to design and enhance the PFRS to meet reporting requirements and successfully implement electronic filing of campaign reports going forward.

II Agency Overview

Statement of Agency Mission:

The mission of the Office of the NM Secretary of State is to carry out its constitutional and statutory mandates by administering elections and governmental ethics in accordance with state and federal law; and to maintain and provide access to the laws, official acts and other instruments that are vital to the efficient operation of New Mexico State Government. It is also the mission of the Office of the NM Secretary of State to file and maintain records vital to the interest of commerce and industry and in accordance with statutory requirements.

B. Statement of Agency Goals:

I. AGENCY GOALS BY ACTIVITY:

1. BUREAU OF ELECTIONS AND ETHICS ADMINISTRATION

To increase public confidence in the conduct of elections and in the electoral process; to successfully implement and carry out the provisions of the "Help America Vote Act;" to provide education and training to local election officials; to educate voters about their rights and responsibilities; to ensure compliance with governmental ethics laws through education and enforcement; to successfully implement electronic filing of campaign reports; to adopt any administrative rules necessary to comply with statute and ensure that the purpose of the Election Code is achieved.

2. COMMERCIAL RECORDINGS:

To increase accessibility to public records through good records management systems and electronic availability; to provide easier means to file trademarks and service marks, partnership registrations, and agricultural liens.

3. ADMINISTRATION/ INFORMATION SYSTEMS:

Provide administrative management and support to all agency functional areas including personnel, maintenance and supplies, information management, public relations and overall fiscal and budgetary services. Information Systems is focused on improving and developing state-of-the-art information technology hardware and software support and infrastructure so the agency can more efficiently carry out its duties and better serve public demand for information and services.

C. Agency Description:

The Office of the Secretary of State has approximately 41 employees all working at the Capitol North Annex on Don Gaspar, just north of the Round House.

The Office of the Secretary of State is organized into three activities, which are the Elections and Ethics Administration, Commercial Recordings, and Administrative Support, which includes Information Systems.

A.

III. IT Plan Implementation for FY06-FY07

A. Description of IT Plan Implementation in prior FY06

Major FY06 goals were the implementation of VREMS and SOSKB. Significant progress was made with each project, however, additional technological advancements need to be made to further advance agency initiatives.

VREMS is a single statewide voter registration system, housed at GSD/ISD and used by all 33 New Mexico Counties and the Secretary of State's Office. January 1, 2006 was the federally mandated deadline for having a fully operational statewide voter registration system. We successfully met that deadline. All 33 New Mexico counties used PowerProfile to administer the June 2006 Primary Election.

Significant VREMS project costs in FY06 included: $23,500.00 to Bency and Associates to perform a post implementation review that was completed in July 2006; and $11,210.00 to our vendor, Elections Systems & Software for the implementation of a distributed database solution for San Juan County.

ISD charged us $100,000 in FY06 to house the VREMS hardware. This is for space, power, cooling, security, and network connectivity. These rates have been costly as we could get hosting services for less than a third of the ISD cost from the private sector. ISD has told us our costs would drop to $37,000 a month in FY07 which would have proven to be much more palatable, however, the costs need to be re-assessed based on the latest service rates posted and the MOU resolved with GSD. Oracle annual support fees were another $100,000, a staggering amount. We plan to see if there is any way we can restructure those fees to bring them down. Federal HAVA funds provided almost all FY06 VREMS spending. Federal money is exhausted in the first half of FY07. The state must step forward to fund the maintenance of this critical application going forward.

Our second important project is the Secretary of State Knowledge Base (SOSKB) developed by the North Carolina Secretary of State in conjunction with Office Automation Solutions (OAS). We worked hard in FY06 on the project to upgrade the Campaign Reporting module of SOSKB, spending $76,500 on this project in FY06. The ability for filers to upload files directly into SOSKB and the public query of campaign reports over the Internet were made operational for the 2006 General Election reporting period.

I. B. IT Strategic Plan Initiatives

The projects mentioned in section A., above, advance the objectives identified in the State IT Strategic Plan. The new statewide voter registration system is a clear step toward an enterprise IT model. VREMS means one standard voter registration system replacing the 11 previous brands of systems installed in 33 different counties. VREMS "consolidates common IT services" by sharing one common statewide database, housed at ISD in Santa Fe (common hosting/data

center model). VREMS will also "enhance delivery of services to clients". Voter registration data will have fewer errors and duplicate registrations because of the integration of 34 independent systems into one statewide system. Data integrity will also be improved because of a "cross-agency approach". VREMS data will be updated by receiving data from the Vital Records, JID, and MVD databases.

Implementation of SOSKB significantly "enhances the delivery of services to constituents." SOSKB will allow, for the first time, public queries of campaign reporting data.

IV. Environment and Infrastructure

A. Current IT Environment, Organization Structure, Strategies, and Goals:

Agency IT staff has been focused on implementation of the statewide voter registration and SOSKB since 2000. The voter registration system involves increased and on-going responsibilities and workload for IT to ensure a stable environment. The Agency IT environment has suffered due to organizational changes and lack of manpower. It is critical that the IT Division be sufficiently staffed and cross trained to ensure legacy and strategic systems are maintained on an on-going basis in order to properly administer, deploy and secure the Agency's IT assets.

Current IT staff at the Office of the Secretary of State now consists of an IT Director, two Computer Specialists, and two IT Generalists One of the Computer Specialists runs the GIS system and works very closely with the Bureau of Elections. The Information Systems Department is a part of the Administrative Support Division.

Title	Total Number of Staff
IT Director	1
Computer Specialist	2
IT Generalist	2

Existing network infrastructure is aging (end-of-life) and prompt equipment obsolescence replacement will be key to maintaining a current, reliable and strategic network infrastructure to support existing and future application development and services.

Equipment room environmental considerations and improvements are being assessed and planned to ensure adequate security, cooling, power and reliability criteria are satisfied. Critical server and network equipment installed need to be situated in an equipment room that meets all building code and manufacturer specifications to ensure warranty and maintenance guarantees are satisfied and to maintain network reliability factors the agency demands.

Plans, policies and work-flow process documentation have not been kept current in the past, but with focus on developing standard operating procedures and training manuals for each division within the SOS, adequate documentation will be established to ensure business continuity and cross training at all levels.

a) Contingency Strategy

Continuity and Disaster Recovery Plan (DRP) instructions are written and include programmatic and computer components. We have one plan that deals exclusively with the statewide voter

registration system and another for the rest of the Agency. The two plans will be discussed separately.

Voter Registration and Election Management System (VREMS) Disaster Recovery Plan

The VREMS Disaster Recovery Plan, attached as Attachment A-1, has been created to provide information necessary for the continuity, restoration, and recovery of critical data and systems that facilitate the technical operation of VREMS. Data is routinely backed up and copies maintained at an off site location. A hot site system is maintained in Bellevue, NE and can be used in the event of a disaster. The hot site can also be used when the primary system is offline due to a significant failure or during a system upgrade that renders the primary system inaccessible.

A project is currently underway to implement additional security measures prior to the November 2006 general election. The "VREMS Disaster Recovery Plan" will be updated at that time to include detailed processes and test procedures. A mock disaster will be simulated, the test results analyzed and changes incorporated into the plan.

In summary the disaster recovery strategy for VREMS pertains specifically to a disaster disabling operations at the main data center where the primary VREMS system is located. If the estimated outage is relatively short, recovery will be initiated under normal recovery procedures. If the outage is estimated to be longer, then the Secretary of State's office will activate the disaster recovery process.

For example if a serious system failure occurred today, such as a catastrophic fire where the VREMS primary system is located (SIMMS datacenter), the disaster recovery plan would be activated and VREMS functionality would be accessed on the hot site system. Since the VREMS application is web based and accessible via the Internet, users would access the hot site system by placing the address of the hot site system (url) in their web browser. The Secretary of State's office would work with GSD/ISD to locate another facility where the primary VREMS system could be recovered. If GSD/ISD had difficulty providing another location that was suitable, the agency would explore facilities available from other agencies and third-party vendors. During this time VREMS operations would continue on the hot site system.

Because the election process is cyclical in nature, the consequences of a serious VREMS system failure vary according to the time of the failure. The most serious time frame would be the month leading up to a major Federal election when early and absentee voting is taking place and counties need to print their poll books. A system failure of an hour would be difficult and with increasing consequences as the duration of the outage continued. This system has the highest priority in terms of minimizing down time and speedy recovery from system failure.

A copy of the Voter Registration System Disaster Recovery Plan is attached as Attachment A-1

Agency Disaster Recovery Plan

Hard copies are stored in the Server Room, at Records and Archives, with DRP team members, and on a portable hard drive at Records and Archives.

- *Current status:* A contingency plan is in place and documented.
- *Last Updated:* July 2003
- *Last Tested:* November 1999 when server hardware failed. Critical database and login functions were restored to another server within hours. The failed server was retired from use. All files were restored from backup tapes to the replacement server. The new server was on-line within 3 days.
- *Summary:* Following is the Table of Contents from our DRP plan:

  Section 1:
  Overview
  Executive Summary
  Assumptions
  Scope and Limitations

  Section 2:
  Document Maintenance

  Section 3:
  Disaster Recovery Action Plan

The consequences of Agency system failures are far less than that of the voter registration system. The most significant outage would be to the Uniform Commercial Code system, as the time of filing determines priority in bankruptcy cases. Another application where system failure would be significant is Political Finance Reporting System in the days leading up to filing dates. This is the system candidates and political committees use to file campaign reports as required by law. Most of the systems, such as Notary, Trademarks, Partnerships, etc. could be down a number of days with minimal consequences.

A copy of the Agencies' Disaster Recovery Plan is attached as Attachment A-2

b) Executive Summary of the Agency's Security Program and Security Architecture

The security architecture of both VREMS and the rest of the Agency configuration was designed to strike a balance between the centralization of IT services, simplicity, effective security, and the need for flexibility at the agency level.

Agency databases, especially VREMS, contain confidential and sensitive data such as social security numbers, birth dates and other. Therefore access to the systems is restricted and monitored.

The SOS utilizes layered security architecture. This approach incorporates effective security measures and controls that provide protection against risks and vulnerabilities. The current system design utilizes traditional user authentication and network security safeguards.

The layers of security have been incorporated into VREMS include:

- **Limited access through firewall technologies** - A Cisco PIX firewall and Intrusion Detection System (IDS) have been implemented in the past to restrict the type of network traffic, control the destination to specific servers (IP addresses) and applications (TCP Ports), and mitigate certain types of attacks. IT recommends upgrading the Cisco PIX firewall with similar security policies using an ASA 5510 Security Appliance.
- **SSL/NLS** – The initial communication between a user's workstation and the VREMS login screen is facilitated via a web browser (Internet Explorer). The connection utilizes 128-bit encryption.
- **Citrix ICA Client** - The Citrix Independent Computing Architecture (ICA) Client is a web browser plug-in that facilitates the display and user's interaction with the VREMS application. It is the program that allows the client to access the VREMS application in a World Wide Web environment. This connection utilizes 128-bit encryption.
- **Citrix Secure Gateway** – The Secure Gateway manages the Citrix authentication and authorization and is responsible for creating a secure channel for the Citrix ICA protocol over SSL. The data exchanged between the clients and the Citrix enabled applications is transmitted over the secure channel.
- **User authentication** - Username/password authentication is being utilized to control user access to the data contained within VREMS. The authentication is used by Citrix and the VREMS application. Transmission of both the username and password occurs over a 128-bit encrypted connection. Strong password complexity is enforced and passwords expire and must be changed at set intervals.
- **Physical Security** – Security at the Simms Building in Santa Fe includes restricted entry to the server room using badge and key pad technology. Racks are kept locked except when hardware is being physically accessed by IT staff. The server room is equipped with video monitors and security personnel monitor the premises 24 X 7.

The layers of security have been incorporated into other Agency systems include:

- **Physical Security** - Key pad access to the server room at all times. Only IS staff has the code. This is reset when there is a staffing change or a reason to believe the code has been compromised. During non-office hours an LFC issued ID badge is required to enter the building then a key to enter the front doors. A list is kept of who has this restricted access.
- **IPX** - The Novell servers are IPX and no gateways from the windows network are currently open.
- **Limited access through firewall technologies** - A Cisco PIX firewall has been implemented to restrict the type of network traffic, control the destination to specific servers (IP addresses) and applications (TCP Ports), and mitigate certain types of attacks. Again, IT recommends upgrading the Cisco PIX firewall with similar security policies using an ASA 5510 Security Appliance.

- **SSL** – Verisign SSL certificates are used on the IIS server for certain applications. The connection utilizes 128-bit encryption
- **User Authentication** - Username/password authentication is being utilized. Passwords expire and must be changed at set intervals.
- **Enterprise Security** – Another layer of security is afforded us as a part of the greater state network. We are the beneficiaries of such GSD/ISD security hardware and software systems as an additional firewall; email protection; Internet monitoring and restriction through WebSense; and Intrusion Detection.

Security Assessment:

An assessment of the VREMS architecture was recently performed to identify security threats and vulnerabilities that could be mitigated utilizing state-of-the-art advances in security technology. Various threats are intrinsic to all networked applications and are of particular importance to a voter registration and election management system.

Some of the key threats and considerations include:

- Session interception
- Man-in-the-middle
- Unauthorized access
- Identity spoofing
- Repudiation
- IP spoofing
- Denial of service
- Application layer attacks
- Trust exploitation
- Overall attack surface

Products that utilized three different technological approaches were reviewed for effectiveness in mitigating VREMS vulnerabilities. The products were evaluated on their ability to limit risk, implementation considerations, flexibility and cost effectiveness.

A product has been selected that will reduce the attack surface of VREMS and provide identity management and control. An implementation plan has been developed and the product is currently in the procurement phase. The goal is to have the product implemented prior to the November 2006 general election so that system access can be monitored. Details of the assessment can be found in the "VREMS Security Technologies" document.

c) Overview of the Agency's Records Retention Plan Regarding Internet/Email Policies.

The Agency Internet Policy is a well thought out document that aims to educate the Agency staff about the Internet and Agency policies and procedures for using the Internet. It lists exactly what is allowed and what is not allowed on the Internet. The plan includes an Internet Access

form that each employee completes and is kept on record in their file. The employee signs the form indicating that s/he is subject to disciplinary action if s/he does not abide by the Internet policies and procedures.

The Agency Email policy needs to be updated on an on-going basis.

d) Major IT Issues and Concerns:

We are particularly concerned about annual maintenance for the new statewide voter registration system. We had federal money for annual maintenance for FY07 but need state funds for FY08 and FY09 . A supplemental Request for $390,000 is included in this IT plan to cover the anticipated shortfall. (how much has been allocated in this FY08 and what is estimated for FY09?) – review numbers below for FY08 and detail what is being requested for FY09.

The anticipated maintenance cost for the voter registration system for FY08 is $750,000 in FY08. This money will need to come wholly from state funds. Typically agency budgets are limited to a small percentage increase annually, say 5%. We will need a total agency budget increase of close to 20% just to cover PowerProfile annual maintenance. The voter registration system is a critical, high profile system that must be funded annually.

Another important concern is the amount of work there is to be done. It is very difficult with a staff of five (when we are fortunate enough to be fully staffed with competent people) to provide day-to-day support to the agency and now the thirty three New Mexico Counties, provide the required IT operation of software and hardware, fulfill the ever growing burden of reporting and paperwork, stay abreast of new technologies in the IT world, and move ahead on new projects. Another slant on this is: the more IT technology we implement, the more there is to maintain, and the less time there is to move ahead. Making that transition with the same staffing as we have had for years is a push. Complicating the problem of doing more and more with the same resources is the problems of hiring and maintaining competent IT staff members. Without a competent IT staff, nothing gets done.

Both the LFC VREMS audit and the post implementation IV&V performed by Bency and Associates have underlined the critical need of additional FTE support for the VREMS project. We now administer and support a statewide voter registration system with the same number of staff members that has traditionally supported just the SOS office. At this point, not everything is getting done. Fortunately, the 2006 Legislature appropriated $180,000 to staff these positions. At the time of this writing our HR person finally got the jobs posted using SHARE and we hope to have the positions filled soon. The next critical need is to make these new positions permanent.

e) Status and Established Goals of the Agency IT Infrastructure

Our building is wired with both copper (Cat 5) and fiber to desktop cabling. An assessment of the existing wiring and cabling will be done to ensure all cabling is consistent with the State Wiring Standard. The 6 Cisco 3550 24-port switches will need t be replaced as they are end-of-

life and no longer on a maintenance contract. The Cisco Catalyst 2950 switch which serves as the DMZ is still in effect.

Agency Infrastructure has been improved as a result of the voter registration system project. The VREMS database is housed at ISD necessitating a good broadband connection to ISD. We installed our own Ethernet data circuit with ISD that bypasses LCS as a part of the VREMS project. This change speeds us up some and reduces the number of points of possible failure.

We do have a number of infrastructure concerns and desires regarding the VREMS system:

1) GSD/ISD is our single ISP connection today and is a shared access. The SOS will implement its own ISP connection based on a 6Mbps dedicated access service ensuring a redundant ISP connection of its own.
2) We need redundant fiber lines from ISD in Santa Fe out to the rest of the world.
3) GSD/ISD needs to implement a hot site that is on the state backbone to meet the needs of the voter registration system and other critical state systems.
4) More broadly, broadband infrastructure in the countryside needs to continue to be upgraded to enhance county connections to the voter registration system.

f) Resource Sharing and Cross Agency Collaboration:

The Office of the Secretary of State participates in significant inter-agency collaboration as a result of the VREMS project. Deceased voters are removed from the voter file based on an update file received from Vital Records. We receive felon information from JID. The next software release in September will allow us to verify SSNs via data from the MVD database.

We are very involved in collaboration with and between counties. The VREMS project places all 33 county databases into one large database housed in Santa Fe. The SOS statewide voter database is now the on-line database utilized by the 33 counties. This streamlines many operations that took weeks or months to complete manually. For example, resolving duplicate voter registrations in multiple counties and voter residence moves from one county to another now can happen in a matter of seconds.

g) Maintenance and Upgrade Strategies of Applications, Databases and Hardware.

The Agency network has two separate network operating systems. Legacy COBOL applications plus file and print functions are run on four dual Pentium file servers running Novell Netware 4.3. Our goal is to gradually migrate to a Windows 2003 Server NOS as we retire legacy applications and replace them with Windows applications. As part of the SOSKB project we purchased Windows Servers to run SQL Server and IIS Web Services. We will be able to run all SOSKB modules on these servers. We have 50 personal computers, including laptops, and 32 printers. We are currently predominately a Windows XP shop with a few older Windows 2000 machines.

We have just a few legacy database applications left to migrate to SOSKB: Trademark, Ethics, and Notaries. These legacy programs are 16-bit DOS COBOL applications with embedded SQL

calls to Pervasive (formerly known as Btrieve) databases. These applications were written in-house. All mission critical applications except VREMS will be migrated to SOSKB. SOSKB is written in Visual Basic using a SQL Server backend.

We have a goal of replacing 12 Agency personal computers, one quarter of the total, each year. This goal is important as old computers limit our software options and reliability becomes more and more of a problem as they reach the end of their useful lives. New workstations are purchased loaded with Windows OS and we add standard core office products plus Enterprise Norton Anti-Virus software.

We have a goal of replacing 20% of VREMS hardware each year. We have already used Federal money to upgrade VREMS servers from Windows 2000 to 2003 and to upgrade Citrix to the latest release. It is critical that state funding be available to upgrade software in the future as the need arises.

#	Executive Business Continuity Plan (BCP) Scorecard	Yes	No	Unknown
1.	Do you have a written business continuity of operation plan (COOP)?	X		
2.	If so, have you fully tested it?		X	
3.	If tested, did you pass your test?			
4.	Have you quantified and ranked the business and financial risk of outages to all vital functions?	X	X	
5.	Are you prepared to address liabilities and fiduciary responsibilities in case of a disaster?	X	X	
6.	Are business continuity plans kept current and updated for business changes?	X	X	
7.	Do you perform back-ups faithfully and include every server and hard drive?	X		
8.	Do you regularly send your back-ups to a safe, off-site archive?	X		
9.	Have you standardized back-up solution on a proven media?	X		
10.	Does business continuity and disaster recovery readiness have support of top management in your organization?	X		

B. Technical Inventory:

The Online Inventory has been updated

V. Information Technology Funding Requests

See Attached C-1 and C-2 Forms

Business Case for Funding Maintenance of the Voter Registration and Election Management System (VREMS)

I. Executive Summary

VREMS is central to the Secretary of State's mission and allows New Mexico election officials register voters and conduct elections. It fulfills the mandate of the Help America Vote Act (HAVA) to provide a statewide voter registration system. This application is mission critical.

The problem is that the Agency base budget has not been increased to cover the significant costs associated with maintaining this system and Federal funds are all but gone.

VREMS implementation costs were $6,600,000. Annual maintenance costs are approximately $561,000 a year, just over 11% of implementation costs, well within industry standards.

It is imperative that VREMS be properly maintained. This means it is imperative that the Secretary of State's supplemental request of $390,000 for FY07 be granted and future base budget requests be authorized.

II. Business Problem and Opportunity

The maintenance cost for the voter registration system is $750,000 annually. We have Federal money for VREMS annual maintenance for the first ½ of FY07 but need state funds for the second ½ of FY07 forward. Typically agency budgets are limited to a small percentage increase annually, say 5%. We will need a total agency budget increase of close to 20% just to cover PowerProfile annual maintenance.

III. Proposed Project Objectives/Performance Metrics

On October 29, 2002, President Bush signed HR 3295, the Help America Vote Act ("HAVA"). This federal legislation created many new mandates for state and local governments. One of the key provisions is that each "...state shall implement a uniform, official, centralized, interactive, computerized statewide voter registration list defined, maintained, and administered at the State level."

The Voter Registration and Election Management System (VREMS) is New Mexico's fulfillment of that mandate. VREMS is a web-based system that meets HAVA requirements, with additional functions supporting election management. New technologies supporting features like document imaging of voter registration cards are also included. VREMS replaces the (non-HAVA compliant) legacy systems that have previously been in use at the 33 New Mexico counties. Most of the counties connect to the centralized system via the public Internet and some have private ATM connections. Citizens can also access the public portion of the voter website (VoterView).

IV. Business Risks

1) Without annual maintenance payments, the system would not run at all. For example, it pays for the annual costs of using the software that allows VREMS to operate. These include the Oracle database, Red Hat OS, and Citrix. Annual Maintenance payments to GSD/ISD pay for server room floor space, electricity, air conditioning and Internet Access that allow counties to connect into the system.

2) Without annual maintenance payments, VREMS could not be properly secured. Private information such as voter SSNs would be at risk. Without proper security, election outcomes cannot be guaranteed. Annual maintenance fees pay for security items such as SSL certificates, security audits, the Identity security solution, and server administration that includes keeping computers updated with security patches.

3) Without annual maintenance payments we could not afford help desk services. Helpdesk services are essential to help the counties and the SOS to use PowerProfile to register voters and run elections. Our users simply would not be able to operate the system without the ability to contact experts, when needed, to advise and troubleshoot.

4) Without annual maintenance payments we could not pay for the facilities and services that would allow us to recover from disasters and system failures. Most importantly this means the hot site in Nebraska that is an exact duplicate of the hardware and software configuration at the Simms building in Santa Fe.

5) Without annual maintenance fees, we could not keep VREMS current. Hardware must be replaced on a regular basis to ensure productivity and reliability. Software must be updated to conform to changes in state and federal law. Software updates also increase productivity and the service provided to our constituents.

V. Alternative Solutions

There is no alternative solution to paying annual maintenance costs other than abandoning the system in violation of federal and state law. There are, however, certainly ways to reduce those recurring costs. GSD/ISD recently reduced by 2/3s the cost of hosting our system at the Simms building. Areas where we believe there is good potential to reduce annual maintenance costs include Hot Site host fees and Oracle database fees.

Cost Analysis –A list of recurring costs is as follows:

Annual Maintenance Estimates for PowerProfile Enterprise Edition			
Item	**Cost per Unit**	**# Units**	**Total**
Oracle Support Renewal (per processor)	$12,000.00	8	$96,000.00
GSD/ISD Oracle License Maint.	$1,600.00	5	$8,000.00
Citrix Licenses	$50.00	170	$8,500.00
Red Hat Linux Advanced Server	$1,588.50	4	$6,354.00
Distributed Solution / Synchronization Maint.	$9,000.00	1	$9,000.00
ES&S Annual Maintenance	$118,385.00	1	$118,385.00
ES&S In-State Support Rep	$126,720.00	1	$126,720.00
ES&S Remote Administration of Servers	$16,800.00	1	$16,800.00
GSD/ISD Primary Data Center Space Rental	$36,929.52	1	$36,929.52
Security Audit	$20,000.00	1	$20,000.00
Dialup Backup Accounts	$1,000.00	1	$1,000.00
Cisco Smartnet Annual Support	$9,632.86	1	$9,632.86
USPS city / zip database for mailing verification	$538.00	1	$538.00
SSL Certificates:	$2,500.00	1	$2,500.00
Voter View Public Web Lookup Support	$8,700.00	1	$8,700.00
Identity Security Solution:	$12,245.00	1	$12,245.00
Software Customization / Upgrade Costs	$20,000.00	4	$80,000.00
Total:			**$561,304.38**

a. Benefits

Benefits of paying the recurring costs listed above include:

1) We can ensure the continued operation of VREMS. This means ensuring that New Mexico election officials can fulfill their missions to conduct fair and honest elections.

2) We can properly secure VREMS to ensure that private information remains private, elections are not tampered with, and servers and data are secure.

3) We can provide our users with the help desk experts to advise and troubleshoot

4) We can retain the facilities and services that would allow us to recover from disasters and system failures. Most importantly this means the hot site in Nebraska that is an exact duplicate of the hardware and software configuration at the Simms building in Santa Fe.

5) We can keep VREMS current and thus ensure hardware is efficient and reliable; software conforms to changes in state and federal law; user productivity and service to our constituents is enhanced.

VI. Recommendation

Based on the information presented, it is clear that annual maintenance costs for VREMS must be properly funded. This means granting the supplemental request of $390,000 for FY07 and the base budget request of $750,000 for FY08.

Base Budget IT Project Form									
Project Name	Appropriation Section, Subsection, or Grant (base or other)	Start Date mm/dd/yy	End Date mm/dd/yy	Cost by funding source (in thousands)		Certified by OCIO or ITC? (15-1C-8B NMSA 1978) Date last certified?	Independent validation and verification (IV&V) and vendor name	Project Manager	FY08 Total Estimated Costs (all funding sources)
				FY06 Actuals (all funding sources)	FY07 Appropriations (all funding sources)				
Voter Registration and Election Mgmt. - VREMS	2002 107-252 HAVA (U.S) 2000 Spcl. 5-8-7 2001 64-14-11 **2003 76-7-9**	01/01/99	6/30/2007	22.1 IV&V	128.7 **- System Acceptance**	No: Grandfathered in	Post Implementation IV&V: Bency & Associates	David Caldwell	0.0
Secretary of State Knowledgebase (SOSKB)	2002 4-7-13 200383-2-P **2002 110-46 (Cap. Project)**	01/01/2002	6/30/2007	76.5	321.8	Yes 4/1/2006	Yes Bency & Assoc.	Trena Watson	0..0

Compliance Spreadsheet: Agency and Project Identification

Lead Agency Name: Secretary of State **Agency Code:** 370

Program Name(s): Bureau of Elections **Contact Peron:** Daniel Ivey-Soto

Information System Name: Voter Registration & Election Management System (VREMS)

Contract **Person:** Daniel Ivey-Soto **Contact Phone Number:** 827-3600

		Compliance with IT Consolidation: Please note that the Secretary of State is an elected official and therefore not required to comply with Governor's mandates.			**Investment Protection: Business Continuance & Disaster Recovery Plans**	
Compliance Requirements						
	Y	IT functions of the project have been reviewed by the Agency CIO or IT Lead so that duplication and redundancy are minimized.		Y	Project is actively addressing security and data integrity issues.	
	Y	This project reports to a Secretary or Director who is a single point of accountability for IT within the Agency.		Y	Project is actively addressing disaster recovery and business continuance issues and records retention	
	N	This project has been reviewed by GSD for participation in existing or future common IT functions usable across multiple Agencies.		Y	Project is actively addressing privacy issues.	
	Y	Project has planned for or conducted a pilot test of applicability and operability in an actual business environment.		Y	Project is actively addressing regulatory compliance issues.	
	Y	Project has planned for or conducted a proof of concept of the technology to be used.		Y	Project is, wherever possible, acting as a supplier and user of shared technical resources with the State.	
	N	Project has addressed governance to identify decision points and accountability to ensure successful implementation.		Y	Project is working with other state agencies to maximize savings through participating in bulk purchases and licensing of standardized components and solutions.	
	Y	A risk profile has been created and is being updated at the start of each phase of the project.		Y	If already in service, the project manager has performed a recent gap analysis against current State security, privacy, architecture, DR and BC requirements and standards.	

	Compliance with the Enterprise IT Strategic Plan		Compliance with the Framework For Enterprise Architecture Plan
Y	An IV&V provider has been selected and is ready to provide independent quality assurance.	Y	Project is in compliance with the current IT Enterprise Architecture Standards for the State.
Y	This project "uses" existing common IT functions from other agencies.	Y	Data and information managed by the project are being handled and protected as an enterprise asset.
Y	This project could benefit from not-yet-existing common IT functions usable across multiple Agencies.	Y	Project is, wherever possible, participating as a supplier or user of re-usable enterprise architecture components.
Y	Project has identified common (sharable) business functions and data.	Y	Project is accessing risks and engineering security into every layer of project implementation.
N	Project is using middleware, where appropriate, to enhance access to all data.	Y	Project has planned for or conducted a proof of concept of the technology to be used.
Y	Any common services "provided" by this project to other agencies or external parties are provided at competitive rates.	Y	Project is collaborating between IT and business leaders during analysis and review to provide advice on technologies.
Y	Project is actively addressing security and data integrity issues.	Y	Project owners are taking responsibility for initiating analysis and review.
Y	Project has given thorough and appropriate consideration to common hosting and data center models.	Y	Project has considered application of COTS (commercial off-the-shelf).
Y	Project has given thorough and appropriate consideration to open source components.	Y	Project is managing a separation of presentation logic, business logic and data access to maximize reusability of components.
Y	Project has given thorough and appropriate consideration to common, distributed and remote support models.	Y	Project is actively addressing system management issues.
Y	Project is implementing and participating in state-wide approaches to business continuity and disaster recovery solutions.	Y	Project is actively addressing privacy issues.
Y	Project is actively participating in any appropriate state-wide or group purchases of products, software or services to minimize costs.		
Y	Project is complying with business case and other project planning and ROI evaluations appropriate to the size and cost of the project.		

Compliance Spreadsheet: Agency and Project Identification

Lead Agency Name: Secretary of State **Agency Code:** 370

Program Name(s): Multiple programs **Contact Peron:** Patricia Herrera

Information System Name: Secretary of State Knowledgebase (SOSKB)

Contract **Person:** Patricia Herrera **Contact Phone Number:** 827-3600

		Compliance with IT Consolidation: Please note that the Secretary of State is an elected official and therefore not required to comply with Governor's mandates.			**Investment Protection: Business Continuance & Disaster Recovery Plans**	
Compliance Requirements						
	Y	IT functions of the project have been reviewed by the Agency CIO or IT Lead so that duplication and redundancy are minimized.		Y	Project is actively addressing security and data integrity issues.	
	Y	This project reports to a Secretary or Director who is a single point of accountability for IT within the Agency.		Y	Project is actively addressing disaster recovery and business continuance issues and records retention	
	N	This project has been reviewed by GSD for participation in existing or future common IT functions usable across multiple Agencies.		Y	Project is actively addressing privacy issues.	
	Y	Project has planned for or conducted a pilot test of applicability and operability in an actual business environment.		Y	Project is actively addressing regulatory compliance issues.	
	Y	Project has planned for or conducted a proof of concept of the technology to be used.		Y	Project is, wherever possible, acting as a supplier and user of shared technical resources with the State.	
	Y	Project has addressed governance to identify decision points and accountability to ensure successful implementation.		Y	Project is working with other state agencies to maximize savings through participating in bulk purchases and licensing of standardized components and solutions.	
	Y	A risk profile has been created and is being updated at the start of each phase of the project.		Y	If already in service, the project manager has performed a recent gap analysis against current State security, privacy, architecture, DR and BC requirements and standards.	

	Compliance with the Enterprise IT Strategic Plan		Compliance with the Framework For Enterprise Architecture Plan
Y	An IV&V provider has been selected and is ready to provide independent quality assurance.	Y	Project is in compliance with the current IT Enterprise Architecture Standards for the State.
Y	This project "uses" existing common IT functions from other agencies.	Y	Data and information managed by the project are being handled and protected as an enterprise asset.
Y	This project could benefit from not-yet-existing common IT functions usable across multiple Agencies.	Y	Project is, wherever possible, participating as a supplier or user of re-usable enterprise architecture components.
Y	Project has identified common (sharable) business functions and data.	Y	Project is accessing risks and engineering security into every layer of project implementation.
N	Project is using middleware, where appropriate, to enhance access to all data.	Y	Project has planned for or conducted a proof of concept of the technology to be used.
Y	Any common services "provided" by this project to other agencies or external parties are provided at competitive rates.	Y	Project is collaborating between IT and business leaders during analysis and review to provide advice on technologies.
Y	Project is actively addressing security and data integrity issues.	Y	Project owners are taking responsibility for initiating analysis and review.
Y	Project has given thorough and appropriate consideration to common hosting and data center models.	Y	Project has considered application of COTS (commercial off-the-shelf).
Y	Project has given thorough and appropriate consideration to open source components.	Y	Project is managing a separation of presentation logic, business logic and data access to maximize reusability of components.
Y	Project has given thorough and appropriate consideration to common, distributed and remote support models.	Y	Project is actively addressing system management issues.
Y	Project is implementing and participating in state-wide approaches to business continuity and disaster recovery solutions.	Y	Project is actively addressing privacy issues.
Y	Project is actively participating in any appropriate state-wide or group purchases of products, software or services to minimize costs.		
Y	Project is complying with business case and other project planning and ROI evaluations appropriate to the size and cost of the project.		

State of New Mexico
Voter Registration and Election Management System
Disaster Recovery Plan

***** Restricted Distribution *****

Version History

14 JUN 2006	0.1 (Draft)	Lawrence White
23 JUN 2006	0.2	Lawrence White

PLAN TESTING SUMMARY

1. Verify that the hot-site system is operational
2. Simulate a disaster at the primary VREMS datacenter
3. Notify the VREMS help desk of the disaster and provide instructions for users to connect to the hot-site until further notice. Let the users know that some of the transactions performed just before the simulated outage may not have been committed to the hot-site system. Those tasks may have to be performed again on the hot-site system.
4. Send an email to each County with the notice in #2 above. Some Counties may be called on the telephone to simulate an outage of the State's email system.
5. Ensure that users can connect to and authenticate with the VREMS system at the hot-site
6. Verify that users can perform their required tasks
7. Test completion: Notify the Counties that the test is complete. Have them disconnect from the hot-site system and connect to the primary VREMS system.
8. Ensure that all users are disconnected from the hot-site system
9. Evaluate the results of the test

SCOPE

This document contains detailed information about the New Mexico Voter Registration and Election Management System, security measures, and controls implemented to provide protection against risks and vulnerabilities. This document is classified as "confidential" and distribution is restricted. This document is under version control and dated for tracking modifications and approvals.

INTRODUCTION

On October 29, 2002, President Bush signed HR 3295, the Help America Vote Act ("HAVA"). This federal legislation created many new mandates for state and local governments. One of the key provisions is that each "...state shall implement a uniform, official, centralized, interactive, computerized statewide voter registration list defined, maintained, and administered at the State level."

The Voter Registration and Election Management System (VREMS) is New Mexico's fulfillment of that mandate. VREMS is a web-based system that meets HAVA requirements, with additional functions supporting election management. New technologies supporting features like document imaging of voter registration cards are also included. VREMS replaces the (non-HAVA compliant) legacy systems that have preciously been in use at the 33 New Mexico counties. Most of the counties connect to the centralized system via the public Internet and some have private ATM connections. Citizens can also access the public portion of the voter website (iPower).

It is important to note that VREMS contains voter information that includes social security numbers, birth dates and other confidential and sensitive data. Therefore access to the system needs to be restricted and monitored. The current system design utilizes traditional user authentication and security safeguards. As with any system, back office processes and appropriate staff training are integral components to ensure the system is safe and secure from unauthorized use.

DESCRIPTION

Business continuance describes the processes and procedures to ensure that essential functions can continue during and after a disaster. Business continuity planning seeks to prevent interruption of mission-critical services and to reestablish full functioning as swiftly and smoothly as possible.

Business continuity planning and disaster recovery are two related initiatives each with their own goals. Business continuity's goal is business process stability. That plan is developed by business unit representatives in partnership with information technology representatives. The goal for disaster recovery planning is technical recovery. The disaster recovery plan is developed and managed by information technology representatives.

This document is the disaster recovery plan for the State of New Mexico's Voter Registration and Election Management System (VREMS). In the event that VREMS is negatively impacted by a man made or natural disaster, this plan is will be used as a guide by New Mexico Secretary of State Staff for the recovery of VREMS computing and network facilities. This disaster recovery plan identifies resources and procedures that can be used in the event of a disaster.

A security assessment of the current VREMS architecture was performed to identify any security threats and vulnerabilities that could be mitigated utilizing state-of-the-art advances in security technology. The assessment and recommendations are contained in the New Mexico Voter Registration and Election Management System (VREMS) Security Recommendations document dated April 21, 2006.

OBJECTIVE

The purpose of the disaster recovery plan is to provide for the continuity, restoration and recovery of critical data and systems that facilitate the technical operation of VREMS. The New Mexico Secretary of State's Office is responsible for this system and needs to ensure that critical data is routinely backed up and copies maintained at an off site location. This document covers the steps necessary for building, testing and maintaining the disaster recovery plan.

The data backup section and disaster recovery section of this plan applies to all personnel who are responsible for the operation of VREMS. This includes System Administrators, Network Managers, Application Administrators, etc. These sections pertain to datacenter equipment and supporting infrastructure necessary for the operation, maintenance and security of VREMS.

DISASTER RECOVERY

The disaster recovery plan can be defined as the on-going process of planning, developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption.

Contingency planning is a critical step in the process of implementing a comprehensive disaster recovery program. Contingency plans contain detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption.

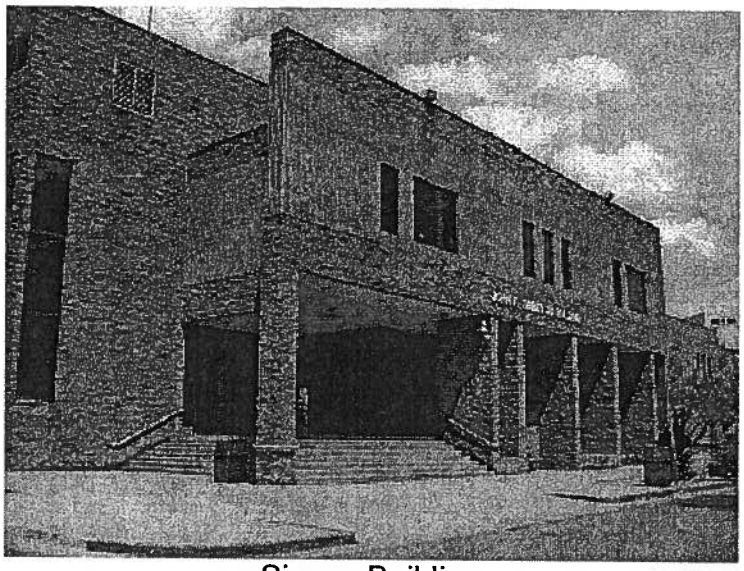
There are five main components of an IT contingency plan. The Supporting Information and Plan Appendices provide essential information to ensure a comprehensive plan. The Notification/Activation, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency. The VREMS contingency plan is being written to provide a clear, concise, and easy to implement plan in the event of an emergency. Checklists and step-by-step procedures will be developed for clarity and ease of tracking.

Figure 2-1 Contingency Planning as an Element of Risk Management Implementation
Source NIST Special Publication 800-34

DATACENTER LOCATIONS

The primary VREMS data processing center is located in the State of New Mexico's John F. Simms Building at:

715 Alta Vista Street
Santa Fe, NM 87502-0110



Simms Building
Front View
Figure 1

A secondary site has been established that functions as a hot-site. This site is used when there is a problem utilizing the primary site and for testing purposes. The secondary site is located at:

CoSentry
1001 Fort Crook Road North
S4uite 1321
Bellevue, NE 68005
402-492-7800

BACKUP

The New Mexico Secretary of State's office is responsible for the backup of VREMS data. The responsibility for backing up any data held on the workstations of individual

VREMS users falls entirely to the user. VREMS users should consult their departmental IT lead or system administrator about local backup procedures.

All VREMS backups must conform to the following best practice procedures:

- Data, operating systems and utility files must be backed up. This includes patches, fixes, updates and disk controller (RAID) configurations.
- It is highly recommended that image backups be created of key disk partitions for all servers. The images will include snapshots of the operating system and registry settings. In the event of a server failure, the server can be restored from the image backup. Once the images have been loaded, backups of the data can be restored.
- Records of what is backed up and to where must be maintained.
- Records of software licensing should be backed up.
- The backup media must be labeled, accurate records of backups performed must be maintained and include details such as which backup set they belong to.
- Copies of the backup media, together with the backup record, should be stored safely in a remote location. The remote location needs to be at a sufficient distance away from the primary datacenter to escape any damage from a disaster at the primary site.
- Backup logs need to be monitored for errors. Tests of restoring data from backup should be performed bi-annually to ensure the viability of the backup system during a disaster. These tests should include the use of the hot-site systems.

The functionality of VREMS has been duplicated at the hot-site in Bellevue, NE. Data is replicated between the primary and hot-site systems at regular intervals. In the event of a failure at the primary site, VREMS users can connect to the hot-site to continue operations. Tasks that were performed just before a primary system failure may have to be repeated on the hot-site system. The primary system will be synchronized with the hot-site system when the primary system has been restored. At this point in time the data on both the primary and secondary systems should contain the same information.

RECOVERY PROJECT TEAM

A project team should be created with representatives from each of the following functions. In some cases a single person may represent multiple areas. The team will include representatives from the New Mexico Secretary of State's Office (IT project management), the New Mexico General Services Department/Information Systems Division (primary datacenter and network infrastructure) and Election Systems and Software (VREMS system administration including application and help desk).

- Project Manager: Responsible for disaster recovery activities. This includes updating, testing and deploying the disaster recovery plan
- Facilities Management
- Local Area Network Operations

- Wide Area Network Operations (Data and Voice Communications)
- Email Administration
- Systems Administration
- Database Administration
- Information Systems Security

If possible do not have all of the IT people working in the same place. If something happened to their building, those resources could be unavailable. This would significantly impact the ability to get the system up and running again.

A notification procedure such as calling trees should be established. Contact information for business partners, contractors, consultants and vendors need to be readily at hand.

OTHER CONSIDERATIONS

It is recommended that a backup Internet Service Provider (ISP) be established at the Secretary of State's Office. In the event of a primary datacenter disaster (Simms Building), Internet communications with the Secretary of State's Office could be severed. An alternate ISP would allow IT personnel to establish a network connection with the hot-site and also use an external email system. A plan to operate at a remote site should also be created in the event that access to the Secretary of State's Office is not possible.

A quick-ship program should be considered with vendors to help ensure that any equipment replacement can occur as quickly as possible.

A disaster recovery database could be created that includes critical technical information such as configuration information and backup versions and dates. The database could also contain contact information for IT personnel and vendors. The database could automatically replicate to the hot-site system and be available in the event of a disaster at the primary site.

PLAN TESTING SUMMARY

1. Verify that the hot-site system is operational
2. Simulate a disaster at the primary VREMS datacenter
3. Notify the VREMS help desk of the disaster and provide instructions for users to connect to the hot-site until further notice. Let the users know that some of the transactions performed just before the simulated outage may not have been committed to the hot-site system. Those tasks may have to be performed again on the hot-site system.
4. Send an email to each County with the notice in #2 above. Some Counties may be called on the telephone to simulate an outage of the State's email system.
5. Ensure that users can connect to and authenticate with the VREMS system at the hot-site
6. Verify that users can perform their required tasks

7. Test completion: Notify the Counties that the test is complete. Have them disconnect from the hot-site system and connect to the primary VREMS system.
8. Ensure that all users are disconnected from the hot-site system
9. Evaluate the results of the test

PLAN REVIEW AND UPDATE

This plan shall be reviewed and updated on an annual basis. The plan may have to be reviewed sooner if special events or circumstances dictate.

RELATED FEDERAL, STATE AND LOCAL REFERENCES

VREMS users and administrators are bound by all applicable laws, rules, policies, and procedures. This plan is not intended to limit the applicability of any law or policy and does not preclude New Mexico State Government agencies and related organizations from implementing additional or more stringent safeguards.

REFERENCES

NIST Special Publication 800-34
CIO Executive Council - Eight Best Practices for Disaster Recovery

Exhibit A-2

Secretary of State Agency Disaster Recovery Plan

Table of Contents

The following is the Table of Contents for the disaster recovery plan document. Each section listed will be discussed in more detail in the sections that follow.

Section 1: Overview

Executive Summary

The purpose of this document is to outline the disaster recovery procedures for the Office of the New Mexico Secretary of State (NMSOS) at 325 Don Gaspar, Santa Fe, NM 87503. At this site, the NetWare server infrastructure is currently providing authentication services, file/print and database services. Two separate Windows 2000 domains are attached to the Novell system, voter and secure.

Within the Voter domain

In the event of a site disaster, recovery of 4 NetWare servers and 1 O'Reilly web server will be required for business continuity. SOSF - login authentication; SOSD - database; SOS2 - secondary database; SOSL - images; WIN95 O'Reilly webserver.

This document provides a workable network disaster recovery plan for NMSOS NetWare file and print services and the SOS Web Page. This document will provide a set of guidelines for a network technician to follow during a disaster recovery situation. These guidelines will streamline the recovery process and minimize the number of decisions required during the recovery. It is estimated that the recovery procedures outlined in this document will require thirty hours to be carried out. Fail-back procedures are also specified for reinstating the complete network environment after the disaster is over.

Assumptions

Access to hardware and software required for recovery
Access to all required backup tapes
Replacement hardware is functional
Required connectivity and cabling is available
Network technician is familiar with the basics of networking in general, as well as the software and hardware contained within this plan

Scope and Limitations

The steps outlined in this document assume that this is a plan to recover whatever is necessary within the walls of the data center: servers, NDS, connectivity between the servers, and data. In the event of a disaster, it is assumed that access to the main site is not available. The printing environment at the recovery site will therefore probably not be the same as it was in the production environment. Due to this, the recovery of the printing environment will be dependent on the equipment available at the recovery site. This document assumes that the specifics are not known and therefore the recovery printing environment will need to be configured manually

When changes are made to this document, changes are logged to a table contained within the document.

Section 2: Document Maintenance

DISASTER RECOVERY PLAN CHANGES LOG

Date	Name	Description
Sept 2002	Trena Watson	Initial creation of document.

Section 3: Disaster Recovery Action Plan

Step 1 - Preparation

Step 1.1. Verify Hardware. The first step in recovering the NetWare server environment is to verify that you have all the components necessary before starting the procedures.

Step 1.2 Obtain Media.

After each section is a checklist table to be used throughout the entire recovery plan. Once each step is complete, the network engineer can check the task as completed and record the time. This will help adjust recovery time estimates for future recoveries.

Checklist for Step 1: Preparation	Done	Date/Time
Step 1.1 - Verify Hardware Verify that the necessary hardware is available and in working condition.		
Verify that all servers complete POST (Power-On Self Test) properly and count the correct amount of memory.		
Verify the configuration of disk arrays on each server.		
Verify power to connectivity hardware (routers/switches).		
Step 1.2 - Obtain Media		
Contact Records & Archives		

Step 2 - Recovery

Step 2.1 - Prepare Hardware. The first step in the recovery phase is to prepare the recovery hardware. SOS2, use Compaq's Scripting Toolkit: http://www.compaq.com/manage/toolkit.html. This toolkit contains utilities which allow you to configure the hardware resources, configure the array, create and populate the configuration partition, create and format the DOS partition, and start the installation. At the completion of this step, your hardware should be configured and ready for NetWare to be installed.

Step 2.2 - Configure NetWare and NDS on the Recovery Servers. This step contains the instructions necessary to recreate the server environment. At the end of this step, the NetWare servers are installed into a skeleton NDS tree that matches your production environment.

Recreate the first server alone. The tree has the original name and the server is located in the original context. This server will hold the Master NDS replica.

The remainder of the servers are recreated simultaneously. The next two servers installed will automatically receive Read/Write replicas of NDS. There is a key in the response file that you can specify whether this server will get a replica. However, it is referring to a replica of the [Root] partition, as no other partitions have been created yet.

> Note: It is important to recreate each server with exactly the same name and Server ID. If not, you will not be able to recover trustee assignments later. Also, it is very important to reinstall servers into the same context as in the production system.

Install all of the server and connection licenses at this time. The license installation may also be automated with the scriptable installation. It is important to install the licenses now because if you forget to do so later, you may encounter application authentication problems. At this point, you will need to patch the servers to the latest level approved by your organization. To speed the patch installation, have available a copy of the expanded service pack on a CD for each server. This way you can install the patches to all the servers simultaneously. During a disaster recovery, you'll want to save as much time as possible wherever you can.

Next, recreate all data volumes on each server. Assign all name spaces that were assigned to the original server.

Before moving on to the next step, verify the current environment. At this point, you should have all the servers recreated and located in the same context as they were in the production environment. Verify that all of the volumes have been recreated and the proper name spaces have been assigned. Also triple-check the server names, server IDs, and addresses. It is easy to make a typo while under the pressure of a disaster recovery.

Step 2.3 - Restore NDS. Before NDS or file system data can be restored, the same User ID that submitted the backup job must exist in this new tree, with the same password and rights as it had before. Be sure to record this User ID, password, and any security equivalences in the maintenance section of this document. This reference must be maintained up-to-date if any aspect of the User ID is changed in the production environment.

Next, restore your SMS-compliant backup program on the server with the master NDS replica. Verify that the TSA agents (TSANDS and TSA500) are loaded and that SMDR is configured (SMDR NEW).

Veritas BackupExec v8.5 stores the catalog on each tape, which can be restored instead of rescanning the entire tape. This will save you critical time during the recovery phase. Insert and restore the catalog of the tape that contains the backup of NDS.

The first step to NDS recovery is to restore the schema extensions. To verify that the schema has been expanded, use the Schema Manager to record the number of object classes and attributes. Submit the schema restore job. Compare the number of classes before and after the schema restore. If the schema recovery fails and your recovery environment has applications that are dependent on specific classes, you will have to reinstall the application programs to extend the schema.

The next step is restoring the actual NDS objects. It is very important to choose only those object types that you will need during the fail-over phase. Restore the specific classes that you need during the recovery, such as User and Group objects. Do not restore objects that already exist in the recovered environment. Below is a list of some of the objects that you should not restore.

Security container
OU containers that already exist
Server objects
Volume objects
License containers and objects
Printer objects (unless they are required)
SMS objects
Application objects that are recreated during installation (BackupExec and NetShield are two examples)
Admin and Backup user objects

Once NDS is restored, verify that there are no unknown or renamed objects. These may be present if you restored an object that already exists. Verify time synchronization and NDS replication on all servers that have replicas.

Once the NDS restoration has been verified, you may set bindery contexts on servers that require them.

Step 2.4 - Restore File System. To restore the file system data, first restore your backup programs on the remainder of the servers and verify that the TSA agents are loaded. Then proceed with the data restoration.

Identify the most critical data and create the first job to restore this data.

> Note: If the restore job submission is in flowchart format you are be able to show the relationships and dependencies of backup jobs.

It would ease recovery efforts to do full backups of each server each night; however SOS IS policy is a full backup monthly.

Step 2.5 - Set Up Printing. As mentioned previously, this document assumes a complete site disaster. If this is the case, the printing environment during the recovery is probably not going to be the same as it was in the production environment. The restored configuration will be

determined by the equipment on hand at the recovery site. As the printing environment will have to be manually recreated, specific instructions are not included in this plan.

Be aware that some legacy applications--usually those that run within a DOS window--may require LPT ports to be captured.

	Done	Date/Time
At this point, all of your servers should be properly recovered in the NDS tree and have their data restored. But before you stop to celebrate, you need to verify that everything is actually correct. Move on to Step 3		

3. **Checklist for Step 2: Recovery**

Step 2.1 - Prepare Hardware define the array
configure the hardware
configuration of any switch connectivity hardware

Step 2.2 - Configure NetWare and NDS on the Recovery Servers

Step 2.3 - Restore NDS

Step 2.4 - Restore File System

Step 2.5 - Set Up Printing

Step 3 - Verification

All of your planning and efforts may be for naught if the right users can't access the right information. It is important to check the accuracy of the recovered environment.

Step 3.1 - Verify NDS. First, verify that time is synchronized on all servers in the tree. Next, verify that NDS is healthy by running DSREPAIR's "Repair Local Database" option on each server that holds a replica. Verify that there are no errors.

Step 3.2 - Verify File System. Verify that the file system has been recovered by spot-checking file system and trustee assignments. If you have the tools to do so, include a trustee report with this plan. In the event of an error during the NDS restore, you may need this report to manually recreate trustee assignments. Also, check backup logs for restore errors.

Sep 3.3 - Verify Login Scripts. Verify that login scripts are correctly mapping drives. They are a critical component that may be overlooked in the event of an NDS restore problem.

Note: Remember to comment out references to resources that do not exist in the recovered environment. For example, remove references to printers and mappings to servers that may not be part of the recovery procedure.

Step 3.4 - Verify Applications. If any applications were running on your servers, make a note to verify their proper functionality. Examples of a critical application that may be running on a NetWare server are applications dependent on the Pervasive database.

Done Date/Time

Checklist for Step 3: Verification

Step 3.1 - Verify NDS

Step 3.2 - Verify File System

Step 3.3 - Verify Login Scripts

Step 3.4 - Verify Applications

Step 4 - Fail-back Plan

Once the disaster has been handled, you'll be ready to restore the original production environment in its entirety. This section outlines the general steps to take when restoring the production environment.

Step 4.1 - Recover Original Server Environment. If the disaster destroyed the original production servers, follow these steps. If the original servers are recoverable, move to Step 4.2. If not, rebuild the servers and connectivity hardware following the same procedures in Step 2. Use the same tapes that were used during the recovery to restore the file system to the new production servers. This will give you the starting point from which the recovery mode began.

Step 4.2 - Restore Changes Made During Recovery Mode. Unless major changes have been made to the NDS tree while in recovery mode, NDS does not have to be backed up and restored to the new production system. Perform differential backups of the recovery servers to capture all data that has been modified. Restore this differential data to the new production environment.

Step 4.3 - Verification. Follow the same procedures as in Step 3 above to verify the production environment's proper operation. The only exception may be the printer restoration. Since you are recovering the original production site, the printers should be recovered as they originally were. If the physical site is recoverable, you can restore the NDS printer objects from tape. If the physical site is completely recovered, you will have to redefine the printers manually.

Checklist for Step 4: Fail-back Plan **Done Date/Time**

Step 4.1 - Recover Original Server Environment

Step 4.2 - Restore Changes Made During Recovery Mode

Appendix A

VENDOR SUPPORT CONTACT TABLE

Vendor	Product	Support Number	Support ID
Dell http://premier.dell.com/premier	PowerEdge Servers	1-800-981-3355	
Compaq http://www.compaq.com/manage/toolk	ProLiant Server	1-800-231-9977	
Novell	Netware 4.2	1-800-858-4000	
Veritas	BackupExec v8.5	1-800-634-4747 1-800-531-7750 Express Routing Code:	

Form C1

Information Technology Base Operating Budget, Special and Supplemental requests[1] Informational Purposes Only[2]			
Agency Name:	Office of the Secretary of State	Agency Code:	370
Project Start Date:	08/29/2007 – Obsolescence Replacement Network Equipment		
Project & Appropriation Funding Type[3]:	Base Request Operational Support of IT Normal Hardware Replacement ☒ Standard Software Upgrade ☐ or Software/Hardware Maintenance ☒	Supplemental Request Cost before July 1, 2008 Operational Enhancements ☐ or Completion of IT Projects ☐	Special Request Costs on or after July 1, 2007 Operational Enhancements ☐ or Completion of IT project ☐

Project Cost (dollars in thousands)

	FY06 & Prior	FY07 Actual	FY08 OpBud	FY09 Request	FY10 Estimate
General Fund				35.0	
Other State Funds					
InterAgency Transfers/ Internal Service Funds					
Federal Funds					
Total	0.0	0.0	0.0	35.0	0.0

Expenditure Categories (dollars in thousands)

	FY06 & Prior Actuals	FY07 Actual	FY08 OpBud	FY09 Request	FY10 Estimate
Personal Services & Employee Benefits					
Contractual Services					
Professional Services					
IT Services				35.0	
Other					
Travel					
Maintenance					
Supplies/Inv. Exempt					
Operating Costs					
Capital Outlay					
Other Financing Uses					
Total	0.0	0.0		35.0	0.0

Agency Cabinet Secretary/Director	CIO or IT Lead	Budget Director
Mary E. Herrera, Secretary of State	Phyllis Vigil-Herrera	Dianne Brown
Phone number	Phone number	Phone number
505-827-3600	505-827-3661	505-827-3600
Date	Date	Date

[1] Please see DFA's FY09 Appropriation Request Preparation Manual for Base Operating Budget instructions.
[2] **Base budget** information is strictly used for informational purposes only.
[3] **Follow the FY09 Funding Request Flow Chart.** Submit one form per funding type.

Form C1

Information Technology Base Operating Budget, Special and Supplemental requests[1] Informational Purposes Only[2]			
Agency Name:	Office of the Secretary of State	Agency Code:	370
Project Start Date:	08/29/2007 – Dedicated Internet Access Services 1-yr term		
Project & Appropriation Funding Type[3]:	Base Request Operational Support of IT Normal Hardware Replacement ☐ Standard Software Upgrade ☐ or Software/Hardware Maintenance ☐	Supplemental Request Cost before July 1, 2008 Operational Enhancements ☐ or Completion of IT Projects ☐	Special Request Costs on or after July 1, 2007 Operational Enhancements ☐ or Completion of IT project ☐

Project Cost (dollars in thousands)					
	FY06 & Prior	**FY07 Actual**	**FY08 OpBud**	**FY09 Request**	**FY10 Estimate**
General Fund				39.7	
Other State Funds					
InterAgency Transfers/ Internal Service Funds					
Federal Funds					
Total	**0.0**	**0.0**		**39.7**	**0.0**

Expenditure Categories (dollars in thousands)					
	FY06 & Prior Actuals	**FY07 Actual**	**FY08 OpBud**	**FY09 Request**	**FY10 Estimate**
Personal Services & Employee Benefits					
Contractual Services					
Professional Services					
IT Services				39.7	
Other					
Travel					
Maintenance					
Supplies/Inv. Exempt					
Operating Costs					
Capital Outlay					
Other Financing Uses					
Total	**0.0**	**0.0**	0.0	39.7	**0.0**

Agency Cabinet Secretary/Director	**CIO or IT Lead**	**Budget Director**
Mary E. Herrera, Secretary of State	Phyllis Vigil-Herrera	Dianne Brown
Phone number	Phone number	Phone number
505-827-3600	505-827-3661	505-827-3600
Date	Date	Date

[1] Please see DFA's FY09 Appropriation Request Preparation Manual for Base Operating Budget instructions.
[2] **Base budget** information is strictly used for informational purposes only.
[3] **Follow the FY09 Funding Request Flow Chart.** Submit one form per funding type.

Form C1

Information Technology
Base Operating Budget, Special and Supplemental requests[1]
Informational Purposes Only[2]

Agency Name:	Office of the Secretary of State	Agency Code:	370
Project Start Date:	08/29/2008 – Server Replacement		

Project & Appropriation Funding Type[3]:	Base Request Operational Support of IT Normal Hardware Replacement ☐ Standard Software Upgrade ☐ or Software/Hardware Maintenance ☐	Supplemental Request Cost before July 1, 2008 Operational Enhancements ☐ or Completion of IT Projects ☐	Special Request Costs on or after July 1, 2007 Operational Enhancements ☐ or Completion of IT project ☒

Project Cost (dollars in thousands)

	FY06 & Prior	FY07 Actual	FY08 OpBud	FY09 Request	FY10 Estimate
General Fund				120.0	
Other State Funds					
InterAgency Transfers/ Internal Service Funds					
Federal Funds					
Total	**0.0**	**0.0**	**0.0**	**120.0**	**0.0**

Expenditure Categories (dollars in thousands)

	FY06 & Prior Actuals	FY07 Actual	FY08 OpBud	FY09 Request	FY10 Estimate
Personal Services & Employee Benefits					
Contractual Services					
Professional Services					
IT Services					
Other					
Travel					
Maintenance					
Supplies/Inv. Exempt					
Operating Costs				120.0	
Capital Outlay					
Other Financing Uses					
Total	**0.0**	**0.0**		120.0	**0.0**

Agency Cabinet Secretary/Director	**CIO or IT Lead**	**Budget Director**
Mary E. Herrera, Secretary of State	Phyllis Vigil-Herrera	Dianne Brown
Phone number	Phone number	Phone number
505-827-3600	505-827-3661	505-827-3600
Date	Date	Date

[1] Please see DFA's FY09 Appropriation Request Preparation Manual for Base Operating Budget instructions.
[2] **Base budget** information is strictly used for informational purposes only.
[3] **Follow the FY09 Funding Request Flow Chart.** Submit one form per funding type.

Form C1

Information Technology
Base Operating Budget, Special and Supplemental requests[1]
Informational Purposes Only[2]

Agency Name:	Office of the Secretary of State	Agency Code:	370
Project Start Date:	08/29/2007 – Network Upgrade/Support		

	Base Request	Supplemental Request	Special Request
Project & Appropriation Funding Type[3]:	Operational Support of IT Normal Hardware Replacement ☐ Standard Software Upgrade ☐ or Software/Hardware Maintenance ☐	Cost before July 1, 2008 Operational Enhancements ☐ or Completion of IT Projects ☐	Costs on or after July 1, 2007 Operational Enhancements ☐ or Completion of IT project ☒

Project Cost (dollars in thousands)

	FY06 & Prior	FY07 Actual	FY08 OpBud	FY09 Request	FY10 Estimate
General Fund				146.6	
Other State Funds					
InterAgency Transfers/ Internal Service Funds					
Federal Funds					
Total	**0.0**	**0.0**	**0.0**	**146.6**	**0.0**

Expenditure Categories (dollars in thousands)

	FY06 & Prior Actuals	FY07 Actual	FY08 OpBud	FY09 Request	FY10 Estimate
Personal Services & Employee Benefits					
Contractual Services					
Professional Services					
IT Services				146.6	
Other					
Travel					
Maintenance					
Supplies/Inv. Exempt					
Operating Costs					
Capital Outlay					
Other Financing Uses					
Total	**0.0**	**0.0**		146.6	**0.0**

Agency Cabinet Secretary/Director	**CIO or IT Lead**	**Budget Director**
Mary E. Herrera, Secretary of State	Phyllis Vigil-Herrera	Dianne Brown
Phone number	Phone number	Phone number
505-827-3600	505-827-3661	505-827-3600
Date	Date	Date

[1] Please see DFA's FY09 Appropriation Request Preparation Manual for Base Operating Budget instructions.
[2] **Base budget** information is strictly used for informational purposes only.
[3] **Follow the FY09 Funding Request Flow Chart.** Submit one form per funding type.

Form C2

Information Technology Data Processing - Computer Systems Enhancement Fund or Capital Outlay[1]					
Agency Name:	Office of the Secretary of State-Data Processing Development related to VREMS			Agency Code:	370
Project Start Date:	07/01/2008				
Multi-Agency Project	Yes ☐	No ☐	List agencies participating:		Enter agency names and codes
Project Type and Specifics:	Computer Systems Enhancement Fund New System Development ☒ Buy (purchase COTS) ☐ or Build (internal resources) ☐		Capital Outlay Agency IT Infrastructure ☐		

Project Cost (dollars in thousands)					
	FY06 & Prior	FY07 Actual	FY08 OpBud	FY09 Request	FY10Estimate
General Fund				150.0	
Other State Funds					
InterAgency Transfers/ Internal Service Funds					
Federal Funds					
Total	0.0	0.0	0.0	150.0	0.0

Expenditure Categories (dollars in thousands)					
	FY06 & Prior Actuals	FY07 Actual	FY08 OpBud	FY09 Request	FY10 Estimate
Personal Services & Employee Benefits					
Contractual Services				150.0	
Professional Services					
IT Services					
Other					
Travel					
Maintenance					
Supplies/Inv. Exempt					
Operating Costs					
Capital Outlay					
Other Financing Uses					
Total	0.0	0.0	0.0	150.0	0.0

Agency Cabinet Secretary/Director	CIO or IT Lead	Budget Director
Mary E. Herrera, Secretary of State	Phyllis Vigil-Herrera	Dianne Brown
Phone number	Phone number	Phone number
505-827-3600	505-827-3661	505-827-3600

[1] **Capital Outlay Information Technology** project requests are strictly for informational purposes only.

Form C2

Information Technology Data Processing - Computer Systems Enhancement Fund or Capital Outlay[1]					
Agency Name:	Office of the Secretary of State-Computer Rm Enhancements and Compliance			Agency Code:	370
Project Start Date:	07/01/2008				
Multi-Agency Project	Yes ☐	No ☐	List agencies participating:		Enter agency names and codes
Project Type and Specifics:	Computer Systems Enhancement Fund New System Development ☐ Buy (purchase COTS) ☐ or Build (internal resources) ☐		Capital Outlay Agency IT Infrastructure ☒		
Project Cost (dollars in thousands)					
	FY06 & Prior	FY07 Actual	FY08 OpBud	FY09 Request	FY10Estimate
General Fund				500.0	
Other State Funds					
InterAgency Transfers/ Internal Service Funds					
Federal Funds					
Total	0.0	0.0	0.0	500.0	0.0
Expenditure Categories (dollars in thousands)					
	FY06 & Prior Actuals	FY07 Actual	FY08 OpBud	FY09 Request	FY10 Estimate
Personal Services & Employee Benefits					
Contractual Services					
Professional Services					
IT Services					
Other					
Travel					
Maintenance					
Supplies/Inv. Exempt					
Operating Costs					
Capital Outlay				500.0	
Other Financing Uses					
Total	0.0	0.0	0.0	500.0	0.0
Agency Cabinet Secretary/Director		CIO or IT Lead		Budget Director	
Mary E. Herrera, Secretary of State		Phyllis Vigil-Herrera		Dianne Brown	
Phone number		Phone number		Phone number	
505-827-3600		505-827-3661		505-827-3600	

[1] **Capital Outlay Information Technology** project requests are strictly for informational purposes only.