

2010 NASCIO RECOGNITION AWARD NOMINATION

The Government Cloud Protection Program: Disaster Recovery Services Transformed for the Perfect Storm



**State of Michigan
(Red Card)**

**Information Technology Applications that are
associated with Critical Agency Business Functions
April 2010**

Life Threatening if Application is not available			
Critical Application Name	Business Function	Agency	Hosting Location
ED Syndromic Surveillance	Public Health Syndromic Surveillance Database	Community Health	State Hosted
EPIC for Labs (LIMS)	EPIC for Labs	Community Health	State Hosted
Hospital Pharmacy System (CERNER)	Hospital Pharmacy System	Community Health	State Hosted
MI Disease Surveillance System (MDSS)	Local, State, and National Disease Surveillance	Community Health	State Hosted
Newborn Screening (NBS)	Screens for life-threatening and/or disabling disorders	Community Health	State Hosted
Remedy Bioterrorism Tracking	Storage of Potential Bioterrorism Data	Community Health	State Hosted—Remote
Corrections Management Information System (CMIS)	Offender (Convicts, Parolee, etc) Management	Corrections	State Hosted
Offender Management Network Information System (OMNI)	Offender (Convicts, Parolee Management)	Corrections	State Hosted
Service Worker Support System (SWSS)	Service Worker Support System	Human Services	State Hosted
Criminal History Record (CHR)	Law Enforcement Communication with State, Local, Federal, etc.	State Police	State Hosted
Law Enforcement Information Network (LEIN)	Law Enforcement Communication with State, Local, Federal Agencies.	State Police	State Hosted
MI Criminal Justice Information Network (MICJIN)	Law Enforcement Communication with State, Local, Federal, etc agencies.	State Police	State Hosted
Michigan, Women Infants & Children (MI-WIC)	WIC Eligibility and Food Benefit System	Community Health	State Hosted



Nomination Category:
Risk Management Initiatives

Name of State Agency:
State of Michigan
Department of Technology, Management & Budget (DTMB) formerly (MDIT)

Project Manager:
Carol Steele Sherman
(517) 241-4449
Shermanc@michigan.gov

Name of Project Sponsor:
Daniel J. Lohrmann
Jason Nairn

Video Link: [Http://www.michigan.gov/mdit-smc](http://www.michigan.gov/mdit-smc)
State of Michigan, Service Management Center Training Video.

B. Executive Summary: Michigan has consolidated data centers, information, and telecommunications into a significant “government cloud” that supports all essential functions of the State. These enhancements have saved hundreds of millions of dollars, but risks have increased – creating the potential of a “perfect storm” to disrupt critical business operations. The Government Cloud Protection Program addresses both traditional and emerging risks in a comprehensive and holistic manner. This program sets a new standard for ensuring that end-to-end government technology is reliable despite unprecedented change.

Problem Statement: From the events of 9/11/2001 to the 2003 Blackout of the Northeast, from ice storms in 2008 to the 195,580 daily email and spam attempts in 2009, Michigan is bombarded by a wide variety of threats to operational stability. As technology solutions became more vital to achieve business results, our corresponding state of readiness grew to meet these expectations. From 13 Terabytes of storage in 2001 to 4.4 petabytes and “storage as a service” in 2010; our data has expanded at exponential rates. Information has become the central asset of government. Other challenges include regulatory requirements for applications, email, storage and electronic records. On top of that, we face cable cuts, hardware failures, network changes, computer viruses, organized criminal activity and hackers seeking financial gain. In addition, Michigan has seen historic budget shortfalls over the past decade. This created another “*storm*” to traverse, and yet, we have been directed by our Governor to safeguard our mission critical data and functions. An unprecedented aspect of the threats is that some of them are disguised as opportunities, i.e. stealth threats. This new norm places an emphasis on streamlining government, finding savings and cost control – likely to be accentuated after the 2010 elections with a new Governor.

Solution: Michigan developed policies, procedures and strategies to address risks inherent with consolidation opportunities. This program enabled upgrading the monitoring and management of essential business functions, establishing disaster recovery (DR) plans for the protection of critical information in our government cloud. Despite revenue cuts, we significantly improved risk management.

Significance: The solution has the potential to be a national model for the reduction of risks associated with consolidation, shared services and managing cloud computing environments. The processes and practices established create new opportunities to reach local partners, address emerging federal cloud computing requirements and offer important risk reduction to complex enterprise technology architectures.

Benefits: The program achieves significant improvements in governance, procedures, operations and risk management outcomes. The program:

- Brought together all stakeholders to agree to use a comprehensive Continuity of Government/Disaster Recovery solution within our government cloud.
- Prioritized and documented all critical State business functions and mapped resources, processes, IT dependencies, networks and relationships.
- Created the State of Michigan “**Red Card**” as the definitive list of critical business functions and corresponding applications for State Government.
- Cost avoidance returned over \$46.1 million to our clients in the last 5 years. Funding for this project came entirely from those efficiencies.

C. Program Description:

Governor Jennifer Granholm directed the Michigan Department of Technology, Management and Budget to begin work on the development of a comprehensive plan to ensure that critical government services could and would continue to function in the event of an emergency. This effort culminated in the *Michigan Continuity of Government Initiative* - a program to address the need for comprehensive planning to ensure that all essential functions of Michigan State Government continue, despite man-made or natural emergencies. State departments worked together to create business continuity plans for their agencies.

Problem Background – An early DR challenge for Michigan was the East Coast power outage. About 2.3 million households and businesses were affected by the blackout, including almost all of Metro Detroit, Lansing, and the surrounding communities in southeast Michigan. Many of our State agencies were without power for days. While our consolidated Data Center continued to function with a backup diesel generator, the IT equipment not located in the data center was unable to function without power. In addition, the Office of the Auditor General (OAG) performed an audit in 2006 where the agency was cited with a material finding because IT had not established an *integrated and comprehensive* process to oversee and direct the State's DR planning efforts. Upon further review, many of the critical IT applications that served the State of Michigan were also cited with over 40 OAG findings due to the lack of DR planning for critical business functions. This reality check highlighted the limitations and risks of solely relying on a few mainframe DR plans, and a list of critical IT applications and business functions.

Our **Government Cloud Protection Program** was catalyzed by this Michigan Continuity of Government Initiative and the DR project team began work on this project in the fall of 2006. The understanding of the problem and development of solutions went through a three phase evolution, a maturation and transformational process – first addressing traditional threats and then engaging the transformational challenges now facing public sector risk management and developing agile, transferable solutions. The plan started with the identification of critical government functions and corresponding computer systems and networks in the State. We set out to develop comprehensive plans and Information Technology Information Library (ITIL) based incident processes to sustain technical operations during emergencies in a consolidated environment.

To address these deficiencies, our project staff was tasked with gathering and analyzing information to prepare a strategy to sustain critical business functions for the State of Michigan. The project goals were:

- Creation of policy, funding and staffing models for disaster recovery.
- Identification of a single, prioritized and definitive list of critical business functions and the identification of all IT systems that support those functions.
- Identification of all IT assets that support the business functions along with a priority for recovery that aligned to the State's business needs.
- The development of a model DR plan and process for consolidating into one location and operationalizing the information relating to DR.
- Creation of an online dashboard reflecting the health of critical applications.

Scope of Problem: Eight critical mainframes, 3,900 servers, 4.4 petabytes of data, 55,000 PC's, thousands of applications, and an extensive number of routers and network segments, none of which were associated with a single business function. Two early employee retirement programs had drained a large number of IT workers from State Government. The State had a few DR plans but they resided on someone's desk, in a file cabinet and one in the trunk of an employee's car, all of them in varying formats. Some had been tested, the majority had not been. We had a list of critical applications that were associated with critical business functions for some agencies, but only one or two people had that list. We had a robust and redundant private dark fiber network between our hosting centers, and the storage infrastructure in place to replicate data from one hosting center to another, but only a handful of our systems used it.

In the meantime, Michigan was undergoing a severe budget crisis, the economy had changed drastically and many of the business and citizens we served were leaving our State, reducing our revenue. Michigan consolidated technology staff and systems, but this also created the DR "stealth threats" associated with relying on consolidated infrastructure and sharing systems and networks. (Note: Michigan closed our 36th Data Center in 2009 – consolidating into three generator-protected core facilities which form the basis for our government cloud initiatives going forward). At the same time, government transformation brought new business functions and delivery models to State Government, and new functions required new IT applications. Our critical application portfolio list was growing and evolving on a daily basis.

Phase I: Conduct Assessment: *Understand opportunities and threats.* After the internal review of the audit findings was complete, DTMB built a plan to move forward with this project. The DTMB Director wanted assurance that the other State Department directors fully understood their risks. In many cases, the agency hadn't purchased the required infrastructure, the architecture wasn't adequate or the physical location of redundant hardware wasn't separated into different hosting centers ensuring uptime or data safety. The report that identified the recovery time expected by the agency vs. the achievable recovery time became the backbone of this deliverable. This project would gather data about where the critical applications resided physically and logically; and a collection of other information about the application. It included a report on the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO), along with application dependencies and relationships.

The Impact Analysis Summary (IAS) report included a red/yellow/green risk score card and a list of options to bring more reliability, and resiliency to each application environment. The Red Card classified each of the critical business functions into one of three categories: life threatening, life threatening depending on the disaster and non-life threatening. These cards were provided to staff to bring awareness of applications, but the cards also helped bring awareness to State Government of the DR Project. These Red Cards are now distributed across government and are a symbol of what applications and business functions are most important to the State. They also help prioritize recovery efforts and our daily work. However, the Red Cards were but a necessary starting point. An effective, sustainable solution needed to go beyond technology and applications, and required changes in policies, strategies and operations.

Phase II: Finding the path to Reliability, Resiliency and Recoverability in a Government Cloud. The DR team began by white boarding the Impact Analysis Summary (IAS) requirements that would be delivered and working backwards to understand what data would be required to complete the IAS. The audience was the Agency, which meant it would have to be written from a business function perspective and explain the technical content in a manner that the agency understood. The DR team met with the individuals associated with the application to gather the data for each application. An IAS report was developed for each application. Once the assessment was complete, it was delivered to the Agency business owner by an IT executive. To preserve the relationships with support staff, we committed to store the information, so we would never have to ask for it again.

Phase III: Transform Delivery Models - Reliability, Resiliency, Recovery and “Relationships”. To preserve relationships the team decided on an off-the-shelf package to manage the DR plans, data and recovery procedures gathered during Phase II. The solution selected was an industry standard - widely used by federal and state governments and companies in the private sector. The software solution was purchased in October 2008 and became fully operational in February of 2009. Public and private sector partners were consulted to ensure that best practices were being deployed and that federal requirements were being met. This centralized solution became an important basis for our government cloud facility. Data gathered from the project was loaded into the tool, along with data for all State and leased facilities that house State functions, contact information for over 55,000 State employees and our many business partners. Prior to implementation of the tool, we had to locate staff by telephone during an incident. That manual process took a team an hour to call 40 DTMB staff, often with only a 50% success rate. Today, one person can reach hundreds of mobile staff in less than 3-4 minutes with up-to-date information on incidents that are impacting our State’s ability to provide critical services. The next step in the process was to implement the tools and provide training and access to continuity planners and IT staff to build and test their plans. The DR team built templates for pandemic plans, IT Services along with plans for building evacuations, and essential business functions. We have assigned a service criticality and gathered data for **all 4,500** of our critical IT devices, across the State. The service criticality strategy and related information has been integrated into all of our ITIL based management processes. Our Service Management Center uses this information every day for the prioritization of our work and all incident, change, and problem management processes. See video link: [Http://www.michigan.gov/mdit-smc](http://www.michigan.gov/mdit-smc).

D. Significance:

This project has the potential to be a national model for the reduction of risks associated with consolidation, shared services and managing cloud computing environments. The processes and practices established create new opportunities to reach local partners, address emerging federal cloud computing requirements and offer important risk reduction to complex enterprise technology architectures. Stealth threats, or those risks that arise from cost-cutting and efficiency efforts, can be reduced by following the methodology established here. In addition, hardware, software and broadband network centralization are known to provide more reliable and efficient enterprise operations, but single points of failure and DR risks must be addressed to ensure government can run

7x24x365. As the federal and state governments move more and more data into cloud computing environments, this project will serve as a guide and a checklist of the risks faced and options available to clients. Other significant aspects include:

Policies / Strategies

- Met Governor's mandate, Federal requirements, and DTMB requirement to incorporate modernized DR into existing processes;
- Aligned with Federal, CIO and NASCIO priorities, including: budget and cost control; security enhancement tools; cloud computing; consolidation; virtualization; shared services and solutions;
- Developed strategies and operational approaches for more effectively managing "stealth threats" and the implications of cloud computing to business operations.

Processes:

- The best practice, a centralized, well documented and innovative use of existing technologies, solutions and processes – included for all three phases – is transferable to other jurisdictions regardless of level of DR maturity;
- Created new opportunities to consolidate operations and share solutions by migrating to a single DR/CoG solution under the Executive branch with other branches of Government and locals poised to leverage the same solution;
- Creation of policy, funding and staffing model for DR and a process for operationalizing the information by clearly identifying systems risk factors/ solutions;
- The DR team created the data collection process with an eye on repeatability and sustainability. Testing on an annual basis is now performed on a regular schedule.

Operations:

- Identification of a single, prioritized and definitive list of critical business functions and all IT systems that support critical business functions, along with a priority for recovery of those functions that aligned to the State's business needs;
- Accurate network topology diagrams (previously unavailable). We documented the topology, relationships and dependencies within each application to validate the components necessary for the applications to function and the priority order to restore them;
- Communication during an incident or disaster has been enhanced by the acquisition of *Notifind* as a part of the Continuity Management software suite;
- Creation of an online dashboard reflecting the health of critical applications.

Peace of mind - It is hard to put a price on recoverability, but our project has accomplished this for the State. We have a much better understanding of our highest priority business functions, and we understand the criticality of our entire infrastructure that supports our Agencies applications.

E. Benefit of the Project:

The future of government technology relies upon our ability to deliver efficient, reliable enterprise solutions using multiple channels, which include traditional and cloud computing delivery mechanisms. Our modernized and transformed management of complex interdependencies has enabled Michigan to increase and expand its risk management capabilities, the range of benefits and beneficiaries:

- **Beneficiaries:** The Red Card is used by all Agencies (55,000 State employees) as the definitive list of critical functions and applications for State Government;
- With instantaneous and consistent communication and a DR plan for recovery in times of crisis; our citizens, our businesses, our clients and other Michigan government jurisdictions benefit with new delivery models, better uptime, quicker problem resolution and lower overall costs.
- **Baseline DR Benefits:** Michigan has participated in several federally organized mock cyber attacks, and several very real virus attacks that basically stopped all email traffic for two of our State Agencies for several days. The information for our critical applications and data from this solution was an essential asset during the virus remediation, and the cyber exercises;
- Our staff and our client agencies now understand what it will take to recover their functions in a disaster, and we are poised to take advantage of new approaches like software as a service (SaaS), virtualization, and IT progressively being delivered as a utility service out of our Government Cloud;
- Incident Management processes have improved and recovery times have decreased due to the information now documented in our Configuration Management Database.
- **Cloud Era Benefits:** Developed strategies and operational approaches for more effectively managing “stealth threats” and the implications of cloud computing to business operations;
- Created new opportunities to consolidate operations and share solutions by migrating to a single DR/CoG solution under the Executive Branch with other branches of Government and locals poised to leverage the same solution;
- The data collected has allowed us to make better use of technology like virtualization by sharing systems, applications and hardware so the RTO/RPO of our most critical applications was enhanced at little to no cost to the Agencies. These tools are enabling us to systematically resolve over 40 outstanding audit criticisms on DR.
- **Savings and Efficiencies:** The Data Center returned \$7 Million in 2005, \$6.6 million in 2006, \$9 million in 2007, \$12.8 million in 2008 and 10.5 million in 2009 for a total of over \$46.1 million to our clients in the form of actual rate reductions and credits for Data Center services, and still funded this project at no cost to any of Michigan’s agencies. These benefits were due to the efficiencies gained from consolidation.
- By consolidating the Continuity of Government and DR Planning with the Agencies, we have also realized an additional savings of \$120,000 per year in operational cost avoidance. Homeland Security grants in excess of \$800,000 for generators were acquired by the DR project to increase the reliability of two of our consolidated hosting centers for our Government Cloud space;
- Prior to modernization, a manual process took a team an hour to call 40 DTMB staff, often with only a 50% success rate. Today, one person can reach hundreds of mobile staff in less than 3-4 minutes with up-to-date information on incidents that are impacting our State’s ability to provide critical services.

The State of Michigan can’t control whether our State is affected by a natural disaster, power outage or terrorist attack, but we have proactively ensured that our government cloud services are *reliable and resilient*, and we are prepared to *recover* those services with minimal impact and data loss.