COUNTY OF MILWAUKEE
INTEROFFICE COMMUNICATION

Date : April 17, 2014

To : Supervisor Marina Dimitrijevic, Chairwoman, County Board of Supervisors
Supervisor Willie Johnson, Jr., Co-Chairman, Finance, Audit & Personnel Committee
Supervisor David Cullen, Co-Chairman, Finance, Audit & Personnel Committee

From : Chris Lindberg, Chief Information Officer, Information Management Services Division

Subject : Assessment of Milwaukee County Data Centers and Recommended Action

Background

Milwaukee County currently hosts all core computing and network services in two separate mechanical equipment rooms in the County Courthouse complex. (See Appendix 1 for historical background). These facilities were developed with no clear course in mind other than to operate and provide computing services at high availability to Milwaukee County Government at reasonable cost. Recognizing the need for redundancy and fail-over of business critical applications, a project was instituted in 2010 whose primary purpose was to establish redundancy and failover between the two data centers in the event of failure in one of the two data centers. This approach was later transitioned into a data center refresh project early in 2013 with the intent of building out transitional capabilities until a full disaster recovery/business continuity plan could be developed, funded and executed. That work was put on hold after the Courthouse fire in 2013.

The fire that occurred in the Milwaukee County Courthouse in the summer of 2013 was contained and extinguished before direct fire damage to the information technologies resident within the Courthouse complex occurred. However, power failures and inadequacies in cooling resulted in ambient temperatures rising above 100 F in the Courthouse data center for a sustained period of time.

Had the fire progressed to the point where IT facilities were involved, IT services to Milwaukee County would have been interrupted completely with full restoration likely taking weeks, if not months, to accomplish. Simply put, Milwaukee County nearly suffered a complete and sustained outage of all IT services.

As a result, IMSD engaged a firm (Reliable Resources, Inc.) to assess the current state of data center facilities in Milwaukee County and make recommendations for ensuring business continuity/disaster recovery in the event of a disaster or large outage. This company specializes in the design and construction of data centers for small, medium and large organizations in both the private and public sectors.

Findings of the Assessment

The challenges that the Milwaukee County data center operations and management team are faced with are many and include:

- Redundancy and/or failover is only partially in place. While some features of the two data centers are configured for automatic backup and failover in the event of a disaster, that work was not completed, nor could be, based on inherent cooling and power constraints. In addition, one of the two data centers has already reach capacity limiting IMSD's ability to move forward with automatic backup and failover.
- Both data centers are located in close proximity to each other. Good disaster recovery planning and execution requires geographic dispersion to accommodate the effects of a "smoking hole" (e.g., explosion, tornado) disaster.
- Opportunities and demand will continue to grow and drive growth and changes in how IMSD services are provided. The data center must be very agile in order to respond to these dynamic requirements.
- Increasing requirements for the power and cooling demands of new technology platforms which exceeds the capacity of the existing data center facilities.
- Currently, both data centers operationally share primary data center functions. These data centers will reach their power & cooling capacities in the next several years in the current non-redundant system mode of operations.

Other relevant issues identified include:

- Milwaukee County Facilities is an organization capable of managing facilities of varying sizes and complexities but completely lacks expertise in the management of data centers. This is not a criticism or short-coming of Facilities. Rather, it reflects that environmental management of data centers is a highly specialized field of expertise and requires significant investment.
- The Courthouse fire clearly exposed power supply issues with the Milwaukee County Courthouse complex as it pertains to data center operations. Dual and geographically dispersed pathways for power are necessary utilities for data center operations.

Data center strategy options that were analyzed in their ability to meet growth projections included:

1. Expand capacity of the existing Courthouse data center.
2. Renovate BHD location studio space (or another existing facility) to provide sufficient capacity and capabilities.
3. Build a new data center on a suitable site to provide sufficient capacity and capabilities.
4. Relocate to a co-location data center vendor to provide sufficient capacity and capabilities. The co-location vendor will provide floor space, power and cooling in support of the county owned and managed information technology equipment. The county would continue to provide all information technology platform support staff.
5. Contract with a suitable managed hosted services vendor for one or both data center applications. The managed services vendor will provide floor space, power, cooling, information technology equipment and the management of the facility infrastructure and information technology platforms up but including applications.

The option for Milwaukee County to continue with the status quo is not a viable option for

meeting the disaster recovery/business continuity requirements or growth projections beyond 2014. Compounding the problem is the fact that the existing Courthouse data center is already operating at its capacity constraints.

Strategy Analysis for Milwaukee County

Chart 1 identifies the cumulative costs to year 2020 vs. the associated level of risk for the following articulated scenarios where the colocation outsourcing strategies providing the primary data center functions and the MER data center located in the Criminal Justice Facility providing the secondary data center function, and the outsourcing strategies that incorporate a co-location vendor or a Managed Services vendor providing both the primary and secondary data center functions.

Specific scenarios included:

1. **Current State:** Continue investments into the current Courthouse data center.
2. **Second Location Retrofit/Courthouse**: Expand existing MER data center operating as secondary data center and renovation of existing space within Second Location facility (e.g., BHD) operating as primary data center.
3. **Courthouse/Second Location New:** Build a new second location data center operating as primary data center and expand existing Courthouse data center operating as secondary data center.
4. **Colo/Colo:** Co-location vendor solution for both primary and secondary data centers.
5. **HMS/HMS:** Hosted Managed Services (HMS) vendor solution for both primary and secondary data centers.

Next Steps

IMSD believes the best strategy for Milwaukee County data centers is the migration to hosted managed services vendor (*Scenario 5 on Chart 1*). This model consists of the County migrating most of the processing, storage and network hardware together with the management services to a managed services vendor. The vendor would own and manage the servers and storage hardware that would be located in the vendor's facility. The costs would include the following services by the vendor:

- Power
- Cooling
- Connectivity to the network
- Bandwidth
- Hardware support
- Operating system maintenance and support
- Networking support and engineering
- Data backup and restore
- Automatic failover capabilities, where required and or mandated.

The vendor selected through the RFP process would have to have its data centers located on US soil and meet hybrid HIPAA and CJIS requirements.

This strategy:

- Has the lowest initial, 5 and 10 year total cost of ownership (*See Chart 1*).
- Addresses risks with redundancy and disaster recovery (*See Chart 1*).
- Addresses issues associated with loss of experience and expertise due to looming retirements.
- Eliminates requirement for DAS Facilities to manage data center facilities and environmentals.
- Paves the path for the development and implementation of a business continuity strategy that mitigates risks in a manner aligned with criticality and cost impact.
- Provides accurate costs with respect to application development and operations that can be used to assess business value creation aligned with investment decisions and strategies.

Pursuit of this strategy would require issuing a Request for Proposal to pre-qualified vendors. The major associated risk with this strategy is the development of appropriate Service Level Agreements (SLAs) that would assure the performance of the vendor in maintaining availability of all County applications. These SLAs would be addressed through the RFP and ensuing contract.

Adoption of this strategy will increase operational costs but decrease on-going capital investments associated with technology refreshes.

Respectfully submitted by

Chris Lindberg, Chief Information Officer
Information Management Services Division

cc: Supervisor Jason Haas, Vice Chair, Finance, Personnel and Audit Committee
Kelly Bablitch, Chief of Staff, County Board of Supervisors
Raisa Koltun, Director of Legislative Affairs, County Executive's Office
Don Tyler, Director, DAS
Josh Fudge, Budget Director, DAS
Steve Cady, Research Analyst, County Board
Janelle Jensen, Committee Clerk, Finance and Audit Committee
Dan Laurila, Fiscal Management Analyst, DAS
Laurie Panella, Deputy Chief Information Officer, IMSD
Nicholas Wojciechowski, Chief Technology Officer, IMSD
Rich Foscato, IT Director of Applications
Marlinda Sisk, Fiscal and Budget manager, IMSD

Strategy Comparisons

Scenario	1	2	3	4	5
Description	Current State	2nd Retrofit/ Courthouse	Courthouse/ 2nd Loc. New.	Colo/Colo	HMS/HMS
Captial Expenses	$ -	$ 3,800,000	$ 7,100,000	$ 2,000,000	$ -
One-Time Operating Expense					
Technology Migration Costs	$ -	$ 400,000	$ 500,000	$ 1,000,000	$ 400,000
Annual Operating Expenses					
Data Center Support Staff (County)	$ 660,500	$ 660,500	$ 660,500	$ 660,500	$ 210,000 [1]
IS Technology Refresh Costs (average)	$ 1,500,000	$ 1,500,000	$ 1,500,000	$ 1,500,000	$ - [1]
Outsourcing Fees/Costs	$ -	$ -	$ -	$ 350,000	$ 600,000
Overhead (utilities ... (utilities, services, maintenance, etc)	$ 100,000	$ 250,000	$ 250,000	$ 750,000	$ -
Software Maintenance	$ 500,000	$ 750,000	$ 750,000	$ 750,000	
Total Annual Operating Expenses	$ 2,760,500	$ 3,160,500	$ 3,160,500	$ 4,010,500	$ 810,000
Annual Depreciation	$ -	$ 280,000	$ 280,000	$ 180,000	$ -
1 Year Cumulative Costs (TCO)	$ 2,760,500	$ 7,640,500	$ 11,040,500	$ 7,190,500	$ 1,210,000
5 Year Cumulative Costs (TCO)	$ 13,802,500	$ 21,402,500	$ 24,802,500	$ 23,952,500	$ 4,450,000 [2]
10 Year Cumulative Costs (TCO)	$ 27,605,000	$ 38,605,000	$ 42,005,000	$ 44,905,000	$ 8,500,000 [2]
Facility Characteristics					
Construction/Implementation Timeline		MER: 7 mo. 2nd Loc: 8 mo.	MER: 7 mo. 2nd Loc: 12 mo.		
Maintenance Cycle	Annual				
Facility/Contract Life Cycle	MER: 10 years G2A: 1 year	15 years	15 years	5 years	5 years
Data Center Classification	MER: Tier 1 G2A: Tier 1-	MER: Tier 3- 2nd Loc: Tier 3	MER: Tier 3- 2nd Loc: Tier 3-	Tier 3	Tier 3
Eliminates Single Points of Failure	No	Yes	Yes	Yes	Yes
Eliminates Electrical Utility Failure	Yes	Yes	Yes	Yes	Yes
Diverse Communications Routing	Yes	Yes	Yes	Yes	Yes
Concurrent Facilities Repairs	No	Yes	Yes	Yes	Yes
Utilizes Existing Private Fiber Infrastructure	Yes	Yes	Yes	No	Yes
Risks					
Eliminate Exposure to Site/Adjacent Risks	MER: No G2A: No	MER: No 2nd Loc: Yes	MER: No 2nd Loc: Yes	Yes	Yes
Risk of Modifications to "live" Data Center		MER: No 2nd Loc: Yes	MER: No 2nd Loc: No	No	Yes
Physical Separation between Data Centers	4 hour wall	> 4 miles	< 4 miles	< 15 miles	< 15 miles
Shared Tenant Buildings	Multi-use Multi-use	Multi-use Multi-use	Multi-use Single tenant	Single use Multi tenant	Single-use Multi tenant

[1] Based on current internal staffing in IMSD. Scenario 5 assumes internal staff reassignments and/or reductions totalling 2-3 FTEs.

[2] Anticipated escalation of contract renewal costs not included

Appendix 1:

History of Milwaukee County Data Centers

Milwaukee County's first foray into a data center model began in 1987 with the purchase of a new Amdahl mainframe computer that was physically located into Schlitz Park, replacing an earlier IBM model that had been housed in the Courthouse Annex. IMSD did not yet exist as a centralized entity at this point and services were managed by administrative services. Early in the 1990's, the Milwaukee County Justice Information Services Division (JISD) began the development of the Criminal Justice Information System (CJIS) which ran on the new Amdahl hardware. Data center facilities were managed through a leasing agreement with ownership of the Schlitz Park complex.

In November of 1993, the new Milwaukee County Criminal Justice Facility (CJF) opened and a new data center was created in a Mechanical Equipment Room (MER) to accommodate video editing/inmate appearance hardware, jail telephone system, and other networking infrastructure. IT staff consisted of mostly sworn MCSO deputies (Information Technology Unit and Special Project Unit). IMSD still had not been formed as the primary IT division, but a study had been underway since the mid-1990s that recommended consolidating and centralizing IT services. In 1998, Advantage was installed on the mainframe hosting CJIS, production was fully implemented in 1999. Following Y2k IMSD continued to consolidate departmental IT units between 2000 and 2004. All IT related services for MCSO were assumed by IMSD in 2004 and oversight of the MER data center followed.

In late 2005, the mainframe housed at Schlitz Park was retired and replaced with a newer IBM enterprise server located in the City of Milwaukee data center. Early in 2006, the Courthouse telephone systems were relocated from the Annex into the G2A data center which was originally designed to house only the telephone systems. Mid 2006 to 2010, IMSD expanded G2A to include file servers and other information technology hardware. It is important to note that this expansion was not engineered to meet classic data center requirements. It was essentially a consolidation effort.

In 2010, IMSD initiated required investments into higher capacity information technologies which drove expansion back into the MER facility. The concentration of these high performing/capacity information technologies required significant investments in facilities for power, HVAC, uninterruptible power supplies and other environments. The overall intent of these investments into the MER and G2A rooms was to provide high availability services and create primary and backup data centers for disaster recovery purposes. While those investments maintained reasonable reliability of current day operations and accommodated growth in capacity, they never fulfilled the requirements for high-availability, fail-over and disaster recovery.

Appendix 2:

Data Centers Explained

A data center is a facility used to house computer systems and associated components, such as local and wide-area networks, telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and various security devices. Large data centers are industrial scale operations using as much electricity as a small town.

IT operations are a crucial aspect of most organizational operations around the world. One of the main concerns is business continuity; companies rely on their information systems to run their operations. If a system becomes unavailable, company operations may be impaired or stopped completely. It is necessary to provide a reliable infrastructure for IT operations, in order to minimize any chance of disruption. Information security is also a concern, and for this reason a data center has to offer a secure environment which minimizes the chances of a security breach. A data center must therefore keep high standards for assuring the integrity and functionality of its computer environment. This is typically accomplished through redundancy of many data center components such as networking cables and providers, cooling, and power, which includes emergency backup power generation.

The Telecommunications Industry Association (TIA) is a trade association accredited by ANSI (American National Standards Institute). In 2005 it published ANSI/TIA-942, Telecommunications Infrastructure Standard for Data Centers, which defined four levels (called tiers) of data centers in a thorough, quantifiable manner. TIA-942 was amended in 2008 and again in 2010. TIA-942:Data Center Standards Overview describes the requirements for the data center infrastructure. The simplest is a Tier 1 data center, which is basically a server room, following basic guidelines for the installation of computer systems. The most stringent level is a Tier 4 data center, which is designed to host mission critical computer systems, with fully redundant subsystems and compartmentalized security zones controlled by biometric access controls methods.

The German Data center star audit program uses an auditing process to certify 5 levels of "gratification" that affect Data Center criticality.

Tier Level	Requirements
1	• Single non-redundant distribution path serving the IT equipment • Non-redundant capacity components • Basic site infrastructure with expected availability of 99.671%
2	• 2 Meets or exceeds all Tier 1 requirements • Redundant site infrastructure capacity components with expected availability of 99.741%
3	• Meets or exceeds all Tier 1 and Tier 2 requirements • Multiple independent distribution paths serving the IT equipment

	• All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture • Concurrently maintainable site infrastructure with expected availability of 99.982%
4	• Meets or exceeds all Tier 1, Tier 2 and Tier 3 requirements • All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems • Fault-tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of 99.995%

The difference between 99.671%, 99.741%, 99.982%, and 99.995%, while seemingly nominal, could be significant depending on the application.

Whilst no down-time is ideal, the tier system allows the below durations for services to be unavailable within one year (525,600 minutes):

- Tier 1 (99.671%) status would allow 1729.224 minutes
- Tier 2 (99.741%) status would allow 1361.304 minutes
- Tier 3 (99.982%) status would allow 94.608 minutes
- Tier 4 (99.995%) status would allow 26.28 minutes