Legislative Audit Division

State of Montana

Report to the Legislature

June 2006

Information System Audit

Data Center Review

Department of Administration

This report contains five multi-part recommendations addressing:

- Implementing an overall process to ensure threats to the data center are addressed.
- Implementing safeguards over physical security to deter unauthorized access.
- Strengthening safeguards to mitigate water and earthquake-related threats.
- Coordinating disaster recovery efforts.
- Defining responsibilities for data center security and coordination.

Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705

06DP-05

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Joe Balyeat, Vice Chair
Senator John Brueggeman
Senator Jim Elliott
Senator Dan Harrington
Senator Lynda Moss
Senator Corey Stapleton

Representative Dee Brown
Representative Hal Jacobson
Representative Christine Kaufmann
Representative Scott Mendenhall
Representative John Musgrove, Chair
Representative Janna Taylor

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
Tori Hunthausen,
Chief Deputy Legislative Auditor

Deputy Legislative Auditors:
James Gillett
Jim Pellegrini

June 2006

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an information systems audit of Data Center operations at the Department of Administration. Our audit focused on the management and protection of the central data center against physical, logical and environmental threats.

This report contains multi-part recommendations addressing: implementing an overall process to ensure threats to the data center are addressed; implementing safeguards over physical security to deter unauthorized access; strengthening safeguards to mitigate water and earthquake-related threats; coordinating disaster recovery efforts; and defining responsibilities for data center security and coordination.

We wish to express our appreciation to the department for their cooperation and assistance.

Respectfully submitted,

/s/ Scott A. Seacat

Scott A. Seacat
Legislative Auditor

Legislative Audit Division

Information System Audit

Data Center Review

Department of Administration

Members of the audit staff involved in this audit were David P. Nowacki and Dale Stout.

Table of Contents

Appointed and Administrative Officials

Department of Administration	Janet Kelly, Director
	Dick Clark, Chief Information Officer
	Pat Boles, Cyber Protection Officer
	Jeff Brandt, Deputy Chief Information Officer
	Steve Bender, Deputy Chief Information Officer

Executive Summary

A data center is a facility used for housing and protecting computers and communications equipment that stores and processes the data necessary to support business operations. The Department of Administration (DofA) maintains a central data center as a service to state agencies. Information resources residing within the data center are critical servers, systems, and data including the Statewide Accounting, Budgeting and Human Resources System, the Department of Revenue’s IRIS system, and Department of Public Health and Human Services systems. DofA approximates the total value of equipment in the data center at $14 million.

The audit included determining whether DofA has identified logical, physical and environmental threats to the data center, assessed the risk or impact presented by the threats, determined the feasibility of implementing controls to address the risks, implemented appropriate controls, and re-assess risks periodically. Audit work included interviews with DofA personnel, walkthroughs and inspections of the facilities, observations, and review of documentation and equipment configurations. We reviewed safeguards used to prevent unauthorized access to server operating systems and reviewed procedures to update and patch server operating systems. We reviewed physical controls, doorways, card key locks and access systems, monitoring functions, and the physical layout of the data center. Audit work included reviewing controls over environmental threats such as moisture and flooding, fire and heat, earthquakes, power surges and outages, and man-made threats such as food, beverages, physical contact or disruption.

Overall, there is not a process in place to ensure the continuity of data center operations or for management to make an informed decision about the appropriateness, cost effectiveness, and necessity of implementing data center controls. DofA has taken a minimal approach to securing the existing data center, preferring to focus efforts and resources on obtaining a new facility they represent will solve the major problems. DofA performs damage control and remediation as problems arise, but does not eliminate or reduce all known threats proactively. This report contains recommendations addressing: implementing an overall process to ensure threats to the data center are addressed; implementing safeguards over physical security to deter unauthorized access; strengthening safeguards to mitigate water and earthquake-related threats; coordinating disaster recovery efforts; and defining responsibilities for data center security and coordination.

Chapter I – Introduction and Background

Introduction

A data center is a facility used for housing and protecting computers and communications equipment that stores and processes the data necessary to support business operations. The Department of Administration (DofA) maintains a central data center as a service to state agencies. Information resources residing within the data center are critical servers, systems, and data including the Statewide Accounting, Budgeting and Human Resources System, the Department of Revenue's IRIS system, and Department of Public Health and Human Services systems. DofA approximates the total value of equipment in the data center at $14 million.

Scope and Objectives

Agencies rely on DofA to protect the equipment housing their information systems and data. DofA has the responsibility to establish appropriate controls, which protect agency information resources contained within the data center. During past audits agencies have expressed concerns regarding the adequacy of controls over the data center. The scope of this audit included the management and protection of the data center and information resources residing within. The scope also included access controls to operating systems under the control of DofA, patch management and server updates. The scope did not include access controls related to any particular application, database, or system, and excluded network devices such as hubs, routers, switches, and firewalls.

Objective #1:
This objective is to determine whether the department has implemented controls that are commensurate with the identified threats to the information resources: **Has DofA implemented controls to prevent, detect or mitigate risks from physical, environmental, and logical threats to the data center?**

Conclusion: DofA has controls in place for fire and heat, power surges and outages, and operating systems access and updates. In the areas of physical security, moisture and flooding, earthquakes, and incident response, controls are fragmented or nonexistent and can be improved. DofA performs damage control and remediation as problems arise, but does not eliminate or reduce all known threats proactively. Overall, there is not a process in place to ensure the continuity of data center operations or for management to make an informed decision about the appropriateness, cost effectiveness, and necessity of implementing data center controls.

Objective #2:

This objective is to evaluate the condition of the facilities housing the data center, primarily the Mitchell Building: **Does the location of the data center, and the facilities that contain the data center, present significant threats that cannot be reasonably controlled or mitigated by DofA?**

Conclusion: The Mitchell Building presents additional challenges to securing the data center, particularly in the security against physical and water-related threats. DofA has taken a minimal approach to securing the existing data center, preferring to focus efforts and resources on obtaining a new facility they represent will solve the major problems. DofA can do more to mitigate these threats to the data center. For example, moving the data center from the basement level could reduce water related threats, and making structural improvements to the data center walls and locking hallway doors could tighten physical security.

Methodology

We evaluated whether DofA has identified threats to the data center, assessed the risk or impact presented by the threats, determined the feasibility of implementing controls to address the risks, implemented appropriate controls, and re-assessed risks periodically. We interviewed DofA personnel, conducted facility walkthroughs, observed operations, and reviewed documentation and equipment configurations. We reviewed safeguards used to prevent unauthorized access to server operating systems and reviewed procedures to update and patch server operating systems. We reviewed physical controls, doorways, card key locks and access systems, monitoring functions, and the physical layout of the data center. Audit work included reviewing controls over environmental threats such as moisture and flooding, fire and heat, earthquakes, power surges and outages, and man-made threats such as food, beverages, and physical contact.

Our work included gathering information regarding the condition of the Mitchell Building by interviewing key personnel to determine their concerns with the location, determining what has been done to address their concerns, reviewing a 2002 report by an independent security assessment company identifying physical threats to the location, and observing the condition of the building.

To aid in the evaluation of the control environment, we referred to the Information Systems Audit and Control Association's Control Objectives for Information Technology and Control Practices, the Federal Information Systems Control and Audit Manual, statewide information technology (IT) policies, and IT industry standard practices.

Chapter II – Findings and Recommendations

Introduction

Section 2-15-114, MCA, states agencies must "implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data." As guardians of the equipment housing the most critical and sensitive data in the state, DofA has the custodial responsibility to protect the data center with safeguards proportional to the importance of the equipment residing in the data center and the extent of potential loss. Accomplishing this requires identifying what equipment it is protecting, threats to the equipment, potential safeguards, and associated costs to implement the safeguards. The department can then make decisions on controls that will eliminate, reduce, or recover from the identified threats. Our review included the areas of: Planning and Management, Physical Security, Environmental Security, and Recovery and Incident Response. Details regarding controls in these areas and conclusions are in the following sections.

Planning and Management

Planning and management of the data center sets the tone for the level of protection by understanding what equipment and systems reside in the data center, knowing where the responsibility for protection lies, knowing what controls are in place and what are lacking, and mitigating the identified threats to the extent possible.

Identification of Resources, Threats, Risks, Cost Effectiveness Analysis

It is unclear within DofA who is responsible for maintaining an inventory of the servers, systems, and data residing within the data center, and required protection. Inventories of systems and data exist, but are outdated. Recovery staff stated that if the systems in the data center were brought down, the order in which agency systems would be brought back up is unclear. Disaster and Emergency Services at the Department of Military Affairs, using Homeland Security funding, purchased a $100,000 software package in the fall of 2005 that can be used for maintaining an organized inventory of resources residing in the data center, and coordinating and documenting recovery plans for all state agencies. The software has been used on a limited basis, but has not been utilized to its full potential. DofA has access to the software, but it is unclear who is responsible for coordinating with agencies to ensure continuity of operations, and when coordination efforts will start.

DofA has not identified and documented threats to the data center, determined threats that are not addressed by a control, or determined the need for controls to address an existing threat or vulnerability. Physical security threats were disclosed by an independent security assessment report in 2002, but the office responsible for physical security, the Office of Cyber Protection (OCP), was unaware that the report existed. Efforts to implement controls have been limited to damage control and remediation as problems arise rather than a formal proactive approach to determine the adequacy of the control based on risk and cost analysis. Risks, including likelihood of occurrence and potential impact associated with threats, have not been determined or evaluated.

Lacking Overall Approach

DofA does not have a process in place for management to make an informed decision about the appropriateness, cost-effectiveness, and the necessity of implementing data center controls. There is not a consistent understanding throughout the department of the resources the department is responsible for protecting, the threats to each resource, the potential impact associated with the threats, and the levels of risk DofA is accepting. The department does not have a methodology to identify and select cost-effective and appropriate safeguards to reduce these risks. It is unclear which division within DofA is responsible for implementing safeguards. As a result, the security controls for the data center are fragmented, with adequate controls in some areas, and deficient controls in other areas, as identified later in this chapter. Because the department is responsible for protecting equipment that houses some of the data most critical to state government operations, more emphasis should be placed on ensuring threats to all data center facilities, resources and equipment are addressed. An overall approach to planning for and implementing a data center control structure will allow DofA to determine whether funding should be applied in order to safeguard against an identified threat or risk, even in extreme cases where the likelihood of occurrence is low.

<u>Recommendation #1</u>
We recommend the Department:

A. Maintain and update the inventory of equipment, systems, and data residing in the data center.

B. Coordinate with all agencies that have hosted systems in the data center to rank the systems' criticality and establish a priority for the order in which systems will be brought back up.

C. Evaluate existing threats to the data center including the potential impact or harm.

D. Conduct a cost analysis associated with implementing or improving controls.

E. Define the responsibility for, and coordinate with agencies to utilize the existing software package to develop disaster recovery plans.

Physical Security

Physical security involves the protection of the data center from unauthorized access, resulting in direct physical contact with data center equipment such as the hardware, cables and power cords, and physical storage media. The data center currently resides on the basement level of the Mitchell Building, which is publicly accessible during working hours. While it is not unusual for a data center to be located in a public building, this presents additional exposures and greater risks of unauthorized access. For this reason, it is important to have a strong control structure to protect against unauthorized access.

Perimeter Security

For physical security, the department relies on walls and doors that comprise the perimeter of the data center within the Mitchell Building. DofA uses a key card access system to secure the doors. Only individuals with access assigned within the key card database are permitted beyond the data center doors. While a key card system can be an effective control, during our walkthrough we noted that not all of the walls on the perimeter of the data center extend up to the ceiling. We observed instances where suspended ceiling panels could be lifted up and access could be gained by climbing through the space between the suspended ceiling and the true ceiling. Staff informed us that due to cables and pipes above the suspended ceiling, it would not be feasible to extend the wall all the way up to the true ceiling in all areas. Subsequently, no analysis has been performed to determine what could be done to secure the facility, and associated costs. The office responsible for physical security of the data center, the OCP, was not aware partial walls existed, but the facilities and operations personnel were aware of this vulnerability. We also identified additional doors outside the perimeter of the data center in the hallways of the building that could be locked during nonbusiness hours to reduce the window of opportunity to enter the data center, but are left open twenty-four hours a day for convenience.

Background Checks

DofA does not have controls in place to ensure all DofA employees in positions requiring background checks have those checks completed. According to Section 44-5-405(1), MCA, "Personnel, applicants and current employees that work with or in a computer center that processes criminal justice information are subject to a background check." The data center transfers information used by the Criminal Justice Information Network (CJIN) system. We reviewed individuals with data center access and identified 91 individuals without background checks. These individuals consisted of 52 DofA staff and 39 staff from other agencies. There is no process to ensure all employees with the defined job positions have background checks completed or procedures for regularly reviewing employees in the defined job positions to ensure the background checks are completed.

Authorization Documentation

The department has an internal policy to authorize data center key card access. Each person with data center access should have an authorization form on file with justification of which doors need to be accessed, why the access is necessary, and approval signatures from the individual's supervisor as well as the CIO. We reviewed access for all active key cards, to confirm the internal policy was being followed. Authorization forms for individuals with access to the outermost door of the data center were on file for 21 of the 144 active key cards, while the innermost door had 7 of 121 authorization forms on file. OCP personnel explained that due to moving of personnel and office space, the documentation has been lost, and lack of consistent understanding of what forms are necessary to request access also contributed. Some people request access via email or submitting a request to the DofA help desk. Neither of these options complies with the internal policy requirement of an approval signature from the CIO.

Periodic Review of Access

Access should be periodically reviewed to ensure the approved security level is maintained. In February 2006, the OCP conducted a review of data center door access to determine if inappropriate access to the data center exists. OCP stated this would be a quarterly procedure. Their review consisted of confirming access for everyone on the Information Technology Services Division (ITSD) organizational chart and existing authorization documentation on file and, therefore, would not include persons outside of ITSD that did not have appropriate documentation. We conducted a review of all individuals with access to the data center within the keycard database and identified 57 individuals with data center access that were not accounted for in the quarterly review.

Key Card Logs Monitoring

The key card database that manages access to the secured data center doors has the capability to log all activity for the data center doors, including successful and failed login attempts. DofA staff does not consistently monitor data center door activity, and does not review overnight logs. OCP staff has stated there is not enough time to complete all job duties if constant monitoring of data center door activity were to occur. We noted that OCP staff was not always logged-in to the system. During one of our interviews we noted instances where the key card monitoring system logged several unsuccessful login attempts by a contractor. Having the software up and running continuously would increase the likelihood of noting potential inappropriate login attempts. The number of people accessing the data center overnight is minimal, and it would not require an excessive amount of time to review the logs. Even though the data center door access is logged and can be checked at any time, the lack of consistent monitoring does not allow OCP to know who is accessing, or failing to access, the data center as it occurs.

Visitor Logs

The use of visitor key cards is required in policy, but enforcement has not been required. Visitor logs are located outside the perimeter data center doors, but no controls are in place to ensure the logs are filled out or accurate. The logs reside in a publicly-accessible area, and are not reviewed. Without the use of key cards and review of the visitor logs, visitor entry to the data center can occur for any reason and will not be known by OCP, who is responsible for physical access to the data center. DofA does not have controls in place to detect patterns of inappropriate visitor access. For example, we identified two separate entries that reported a visitor entered the data center to have lunch with a family member and to walk a family member home, which according to OCP is not an appropriate reason for entering the data center. According to the entries, the visitor was in the data center for up to two hours. OCP staff stated it is time consuming to review the visitor logs and the visitor cards are not used because it is difficult to enforce their use. We noted that our review of visitor logs for the entire year took less than one hour.

Operator Awareness

DofA ultimately relies upon the data center being manned 24 hours a day for physical security. During our work, we noticed the only notification of someone entering the data center was a mild beep that cannot be heard over the noise made by the data center equipment. The layout of the data center does not allow straight-line visibility to every area of the data center from the operator areas. There is currently no monitoring or surveillance systems installed on the perimeter of the data center. The current controls do not take into account persons accessing the data center by means other than the doors, such as the ceiling. Data center access could be gained without the operators noticing, effectively negating the compensating control of the data center being manned for 24 hours.

Recommendation #2
We recommend the Department:

A. Implement safeguards such as locked doors in Mitchell Building hallways or completed walls on the perimeter of the data center to restrict physical access to the data center.

B. Implement procedures and assign responsibilities for ensuring background checks are complete.

C. Follow policy and maintain required authorization documentation on file for each individual who has key card access to the data center.

D. Conduct a periodic review of all key card access to the data center to confirm appropriateness.

E. Monitor and review the key card activity logs and data center visitor logs for inappropriate or unauthorized access.

F. Develop a system to ensure operator awareness of physical security breaches.

Environmental Security

Environmental security consists of implementing controls to protect against environmental threats such as fire and heat, water, power loss, and natural disasters.

Earthquakes

The Lewis and Clark County Pre-Disaster Mitigation plan states that based on population concentration and seismic activity, Helena is the most vulnerable city in the state to an earthquake. DofA states that one of their primary concerns about data center security is that the Mitchell Building could not withstand a major earthquake. The last major earthquake to hit the Helena area was in 1935, when three earthquakes hit the area. The earthquakes magnitudes ranged from 5.9 to 6.3. Based on past activity, a magnitude 5 or greater earthquake is expected to occur once in a 32-year period, while a magnitude 6 or greater earthquake once in a 192-year period. There is no compensating control to eliminate the threat, such as a hot site containing redundant equipment or mirrored systems they could immediately switch over to in the event of an earthquake. DofA does have a disaster recovery contract, which includes alternate facilities in Philadelphia. This contract is further discussed in the

Recovery and Incident Response section of this chapter. In evaluating mitigating controls that could reduce the impacts to the equipment due to the earthquakes, we determined that data center equipment is not stabilized or bolted to the ceiling or floor to reduce movement. DofA has not implemented controls to ensure business continuity in the event of an earthquake.

Water

The data center resides in the basement of a four-story building, and aside from the suspended ceilings, there is nothing to prevent water from floors above from coming into the data center. Water pipes exist above the suspended ceilings, below the floors, and along the walls of the data center. Measures have been taken to reduce the impact from water related threats. The data center contains raised floors, pumps to reduce the amount of water that accumulates on the floor, and a water detection system was recently installed. Some of the communications and power cables have waterproof conduit to protect them from water damage, but individual servers remain largely unprotected. The potential exists that if a major flood occurs that overrides the pumps' capacity for removing water, the data center could receive severe water-related damage.

The data center and alternate site are not situated such that the susceptibility to natural disasters such as earthquakes is reduced as much as possible. Additionally, the building is constructed in a manner in which the susceptibility to water and flooding is increased due to the basement location and water pipes surrounding the facilities. Controls are in place to reduce, but not eliminate water-related threats.

Recommendation #3
We recommend the Department strengthen safeguards to mitigate the risks associated with earthquake and water-related threats.

Recovery and Incident Response

Recovery and response controls include procedures to compensate for nonexistent or failed controls, which create a problem that requires recovery.

Disaster Recovery

The Statewide Disaster Recovery plan has not been updated since 1995, and is not being used. DofA has a disaster recovery contract with an external vendor that includes facilities located in Philadelphia. The facility does not include redundant systems, and would require down time while DofA personnel acquire back-up tapes, fly to Philadelphia, install the equipment, and re-load the systems and data covered under the contract. Based on annual testing of the disaster recovery contract procedures, the best-case scenario in a controlled, organized, planned test is 64 hours of down time. Disaster recovery is not included with standard service levels for agency systems hosted by DofA. The current disaster recovery contract includes recovering services such as core functionality for the state network, and systems that DofA operates such as SABHRS. Agencies have the option to participate in the disaster recovery contract. Under the current contract, only DofA, the Department of Fish, Wildlife and Parks, the Department of Revenue, the Department of Corrections, and the Department of Justice have elected to be included in the contract. Those agencies are covered for select applications, but not all systems or services. The remaining state agencies would be on their own to recover their systems and applications, and would have to find a way to connect to the core state network once again.

DofA does not have a plan or controls in place to ensure continuity of data center operations in the event of a major disaster. The current disaster recovery contract covers limited agency applications and services. While it is not DofA's responsibility to recover all agencies' data, it is responsible for the protection of equipment in the data center where the data resides. Given the potential impact of a disaster on state government operations, more emphasis should be placed on ensuring the continuity of government.

Recommendation #4
We recommend the Department:

A. Maintain an updated statewide disaster recovery plan.

B. Coordinate with the Governor's office to request that agencies assign a higher priority to disaster recovery.

Why are Security Measures not given a Priority?

We observed the following as underlying reasons for controls lacking in the areas identified above in addition to the department focusing on obtaining a new data center facility.

Services vs. Security

DofA staff noted on several occasions reasons for controls not being in place included a preference to provide convenient services to the agencies as opposed to putting security as a priority. We were informed of instances where security measures were not given a high enough priority or enough time to do what was necessary and on occasions access is granted based on convenience for contractors and agency personnel. Security to the data center, which houses some of the most sensitive and critical data in state government, should be controlled by a principle of least access approach, rather than allowing convenient accessibility.

Security Through Obscurity

DofA relies heavily on a security through obscurity approach, in that there are many known vulnerabilities that exist, and the only security they rely on is the fact that they have not been discovered or threatened. Specifically for physical security, there is little in the area of compensating controls or a layered security approach to reduce the risk of vulnerabilities. Where known control deficiencies exist, compensating controls can be implemented or strengthened in layers to reduce the likelihood of exposure.

Summary

DofA is focused on providing services to agencies, and there are conflicting priorities for data center services between convenience, availability, and security. Because the data center houses some of the most sensitive data in state government, it is important to skew the balance toward security. Due to the organizational structure of the department, several divisions and bureaus have responsibilities related to data center security. General Services Division maintains the physical condition of the facilities; the OCP is responsible for physical security; and several bureaus within the ITSD maintain server and network security within the data center. All of these components are important to data center security, and will remain important regardless of the location of the facility. The overlapping areas of responsibility created barriers to security efforts due to conflicting priorities. The department does not have somebody responsible for data center security as a whole, and for coordinating efforts to ensure the security of the data center.

Recommendation #5
We recommend the Department clearly define and designate responsibility for coordination of all aspects of data center security.

Department Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

BRIAN SCHWEITZER, GOVERNOR | MITCHELL BUILDING

STATE OF MONTANA

(406) 444-2032
FAX 444-2812

PO BOX 200101
HELENA, MONTANA 59620-0101

June 13, 2006

David Nowacki
Senior Information Systems Auditor
Legislative Audit Division
PO Box 201705
Helena, MT 59620-1705

Dear Mr. Nowacki:

We have reviewed the June 2006 Data Center Review audit report and the recommendations contained therein. Our response to the recommendations appears below:

Recommendation #1

We recommend the Department:

A. Maintain and update the inventory of equipment, systems, and data residing in the data center.
B. Coordinate with all agencies that have hosted systems in the data center to rank the system's criticality and establish a priority for the order in which systems will be brought back up.
C. Evaluate existing threats to the data center including the potential impact or harm.
D. Conduct a cost analysis associated with implementing or improving controls.
E. Define the responsibility for, and coordinate with agencies to utilize the existing software package to develop disaster recovery plans.

Response:

We concur:

A. The currently-fragmented inventories of equipment, systems and data will be consolidated, updated and maintained. ***Target date: September 30, 2006.***
B. The Department will work with agencies on "Continuity of Government (COG)/Continuity of Operations (COOP)" plans, and will pay particular attention to their recovery plan for critical systems residing in the data center. Development of a "48 Hour" tactical plan is already underway to assure business priorities are clear during disruptions of systems services. ***Target date (for the "48 Hour Plan"): September 30, 2006.***

"AN EQUAL OPPORTUNITY EMPLOYER"

C. The Department will conduct a threat and impact assessment for the data center by participating in the Capitol complex vulnerability assessment scheduled for July. ***Target date: August 31, 2006.***

D. A cost analysis will be conducted for implementing or improving controls. ***Target date: TBD based on the results of item "C".***

E. The Department will clarify and communicate its responsibilities to its staff and other stakeholders as follows: ***Target date: July 1, 2006.***

   - The General Services Division (GSD) is responsible for coordination of agency disaster recovery planning.
   - The Information Technology Services Division (ITSD) provides software support for the program. The Department has prepared an EPP for technical support of this software the upcoming budget cycle.

Recommendation #2

We recommend the Department:

A. Implement safeguards such as locked doors in the Mitchell Building hallways or completed walls on the perimeter of the data center to restrict physical access to the data center.

B. Implement procedures and assign responsibilities to ensure background checks are completed.

C. Follow policy and maintain required authorization documentation on file for each individual who has card access to the data center.

D. Conduct a periodic review of all key card access to the data center to confirm appropriateness.

E. Monitor and review the card key activity logs and data center visitor logs for inappropriate or unauthorized access.

F. Develop a system to ensure operator awareness of physical security breaches.

Response:

We concur.

A. Department divisions will work together to identify and implement, where appropriate, data center physical access restrictions. ***Target date to identify potential controls: October 31, 2006. Implementation dates will depend on specific improvements identified and their priority sequence in an overall plan.***

B. The Department will implement a procedure that will assure required background checks are performed for individuals and positions that handle sensitive information housed in the data center. ***Target date: September 30, 2006.***

C. The Department will maintain card key authorization documentation as recommended. ***Target date: Immediately.***

D. The Department will formalize the access card review frequency and process. ***Target date: August 31, 2006.***

E. The Department will review the logs as recommended. The Department will also establish and communicate guidelines for visitor access to the data center. ***Target date: July 15, 2006.***

F. The Department will develop a system to ensure data center operators are alerted of physical security breaches. Note: all data center weekend shifts, all midnight shifts, and half the evening shifts are staffed with a single operator. Their duties require them to be away from the console area for significant periods of time. Prompt response to an intruder alert will require additional staff. This gives further weight to an existing EPP for additional operator staffing. The Department will prepare a surveillance equipment plan and EPP request. ***Target date: EPP preparation – July 15, 2005; implementation - TBD.***

Recommendation #3

We recommend the Department strengthen safeguards to mitigate the risks associated with earthquake and water-related threats.

Response:

We concur. During the budget planning process for FY06-07, the Department submitted an EPP for earthquake dampening devices for data center equipment to provide protection during "non-catastrophic" earthquakes. That proposal did not survive the previous budget process. The Department will resubmit that EPP to provide a measure of earthquake protection. ***Target date: July 1, 2006.***

The Department has installed new water-sensing and alert equipment in the data center. ***Completed.***

Recommendation #4

We recommend the Department:

A. Maintain an updated statewide disaster recovery plan.
B. Coordinate with the Governor's office to request that agencies assign a higher priority to disaster recovery.

Response:

We concur:

A. GSD has oversight responsibility for the COG plan. ITSD is responsible for developing and maintaining the disaster recovery plan for ITSD equipment and services. ITSD is also responsible to provide technical support for the software tool used to develop and maintain COOP plans on a statewide basis. ***Target date: on-going. See response to Recommendation#1 (B) for communication tasks.***

B. The Governor's office has placed a high priority on disaster recovery and set expectations for agency participation in COG/COOP planning efforts. ***Target date: on-going.***

Recommendation #5

We recommend the Department clearly define and designate responsibility for coordination of all aspects of data center security.

Response:

We concur. The Department will clearly define and designate responsibility for coordination of all aspects of data center security. ***Target date: July 15, 2006.***

We recognize the magnitude of the challenges associated with implementing these recommendations; however we are committed to implementing the data center recommendations in a manner consistent with the audit.

Thank you and your staff for conducting the audit in a professional manner.

Sincerely,

Janet R Kelly

Janet R. Kelly, Director

cc: Dick Clark - State CIO
Jeff Brandt - Deputy CIO, Enterprise Operations
Steve Bender - Deputy CIO, Enterprise Services
Mike Boyer - Asst. Administrator, Enterprise Operations
Pat Boles - Cybersecurity Officer
Marv Eicholtz - General Services Division Administrator