NORTH DAKOTA LEGISLATIVE MANAGEMENT

Minutes of the

LEGISLATIVE AUDIT AND FISCAL REVIEW COMMITTEE

Wednesday, October 17, 2012
Roughrider Room, State Capitol
Bismarck, North Dakota

Representative Dan Ruby, Chairman, called the meeting to order at 9:00 a.m.

Members present: Representatives Dan Ruby, Dick Anderson, Patrick Hatlestad, RaeAnn G. Kelsch, Keith Kempenich, Joe Kroeber, Andrew Maragos, Corey Mock, David Monson, Chet Pollert, Bob Skarphol, Dwight Wrangham; Senators Joan Heckaman, Jerry Klein, Judy Lee, Terry M. Wanzek

Members absent: Representatives Tracy Boe, Gary Kreidt, Lonny B. Winrich; Senator Randel Christmann

Others present: See Appendix A

It was moved by Representative Maragos, seconded by Representative Skarphol, and carried on a voice vote that the minutes of the July 26, 2012, meeting be approved as distributed.

The Legislative Council staff distributed a memorandum entitled *Summary of Audit Reports Not Selected for Presentation*, which provides a summary of audit reports that are available but not selected for presentation at the October 17, 2012 Legislative Audit and Fiscal Review Committee meeting. Chairman Ruby suggested committee members review the memorandum to determine if any of the reports included in the memorandum should be presented at the next committee meeting.

The Legislative Council staff distributed a memorandum prepared in response to a request at the committee's July 2012, meeting entitled *Whistleblower Laws and Rules*, which provides a summary of state laws that are commonly referred to as whistleblower protection laws and administrative rules adopted to address the laws.

NORTH DAKOTA NETWORK AND SECURITY AUDIT

Mr. Mark Shaw, Executive Director, Cyber and Intelligence Solutions, ManTech International Corporation, Vienna, Virginia, provided information (Appendix B) regarding vulnerability assessment and penetration testing of the Information Technology Department. He said ManTech International Corporation performed a vulnerability assessment and penetration test of the Information Technology Department's statewide computer network from May to August 2012. He said the assessment and penetration testing consisted of the following three major project tasks:

Project Task	Description
External vulnerability assessment	An external vulnerability assessment is intended to provide an organization with information on the overall security and risk of the computer network from an external point of view. External assessment procedures focus on performing Internet research, discovering systems connected to the Internet, and probing systems to discover misconfigurations and vulnerabilities.
Internal vulnerability assessment	An internal vulnerability assessment is intended to provide an organization with information on the overall security and risk of the systems and network from an internal point of view. Internal assessment procedures focus on examining systems for vulnerabilities, misconfigurations, and implementation flaws that may expose the system and network to additional risk.
Penetration testing	Penetration testing is intended to provide an organization with information on the overall security and risk of its network from an external or an internal point of view. Penetration testing focuses on gaining access to systems under an organization's control.

Mr. Shaw said vulnerabilities discovered were assigned a risk identifier that was relative to the network or system under test. He said the three risk levels used are defined as follows:

- High-risk - A high likelihood of compromise of system-level access exists. If exploited, this vulnerability may allow total control of the system.
- Medium-risk - A vulnerability exists that may provide access to critical data or user-level access to a system. This vulnerability may lead to further exploitation.
- Low-risk - A vulnerability exists that may disclose information but does not directly lead to the exploitation of a system.

Mr. Shaw provided the following summary of the findings and recommendations:

Project Task	Findings
External vulnerability assessment	There were 11 unique vulnerability findings, including six high-risk, four medium-risk, and one low-risk. The findings are classified into two categories-- misconfigured systems or applications and operating systems or software applications that were missing critical security patches.
Internal vulnerability assessment	There were 28 unique vulnerability findings, including 22 high-risk, 4 medium-risk, and 2 low-risk. The findings are classified into two categories-- misconfigured systems or applications and operating systems or software applications that were missing critical security patches.

Penetration testing	In regards to direct penetration testing, the project team completed five penetration testing scenarios for further explorations based on the findings of the external vulnerability assessment. Upon a detailed review of each system and publically available exploits for the identified vulnerabilities, the project team determined none of the proposed scenarios were viable for execution. In regards to a "phishing" exercise, the project team executed a scenario based on the recent rollout of the ConnectND talent management suite. The project team sent "phishing" e-mails to 545 state employees claiming to be from the administrator of the ConnectND system. The first report by a state employee of the "phishing" e-mail to the Information Technology Department service desk was within 10 minutes of the e-mail. The Information Technology Department simulated a block of the malicious domain within 25 minutes of the e-mail and sent notification to state employees within 50 minutes. The project team collected 63 sets of valid credentials from employees that did not realize the e-mail was a "phishing" exercise.

Mr. Shaw provided the following general recommendations:

- Implement formal patch management program - Multiple systems were found to be missing critical operating system and application security patches. A baseline should be established to document deployed operating systems and application software installed on each system in the environment. Application software that is not mission critical should be removed. Regular review should be completed to ensure all operating system and application security patches are deployed in a timely manner.
- Internal segregation of critical servers and development systems - Segregate servers deemed to be hosting critical data or services from the internal network by hosting these servers on a separate subnet strictly controlled by access-lists. Development servers should also be completely isolated on a separate subnet with no access to other state resources.
- Require use of encrypted protocols for remote management - Large numbers of systems on the state's internal network were noted using unencrypted protocols for remote access and management of systems. Security best practices recommend the use of encrypted protocols for remote access and management.
- Restrict access to protocols for remote management from the Internet - IP-based access controls should be put in place to restrict access to known and trusted IP addresses that have a legitimate need to connect to remote access services.

Mr. Shaw said the findings are typical of organizations with an enterprise the size of the state of North Dakota. He said these results show an improvement over the assessment conducted in 2009.

Representative Skarphol suggested information be presented at a future meeting on information

presented by Mantech to the Information Technology Department at the audit exit meeting.

AUDITS OF STATE AGENCIES, BOARDS, AND COMMISSIONS

Chairman Ruby called on Mr. Ed Nagel, Director, State Auditor's office, who presented the audit report for the Aeronautics Commission for the years ended June 30, 2011 and 2010. Mr. Nagel reviewed the auditor's responses to the committee guidelines and said the report includes one internal control finding relating to fraud risk assessment. He said the finding relating to fraud risk assessment is a prior recommendation not implemented.

Mr. Nagel presented the audit report for the Department of Commerce for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report identifies one area for operational improvement relating to usage of the purchasing card.

Mr. Nagel presented the audit report for the Commission on Legal Counsel for Indigents for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report does not include any findings or recommendations.

Mr. Nagel presented the audit report for the Council on the Arts for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report includes one finding of noncompliance with legislative intent relating to reimbursement for meals.

Mr. Nagel presented the audit report for the Department of Corrections and Rehabilitation for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report includes two internal control findings relating to pharmacy inventory and the safeguarding of assets and recording of transactions at Roughrider Industries. He said the report includes two findings of noncompliance relating to sales to inappropriate vendors and improper use of public funds.

Representative Ruby asked that the Attorney General's opinion relating to the termination of the Roughrider Industries Director be provided to committee members.

Mr. Nagel presented the audit report for the State Department of Health for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report does not include any findings or recommendations.

Mr. Nagel presented the audit report for the Insurance Commissioner's office for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report includes one finding of noncompliance relating to collection of petroleum tank registration fees.

Mr. Nagel presented the audit report for the Labor Department for the years ended June 30, 2011 and

2010. He reviewed the auditor's responses to the committee guidelines and said the report does not include any findings or recommendations.

Mr. Nagel presented the audit report for the Office of Administrative Hearings for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report does not include any findings or recommendations.

Mr. Nagel presented the audit report for the Parks and Recreation Department for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report includes one internal control finding relating to controls over state park revenues and two findings of noncompliance with state procurement guidelines and deposit of state park fund revenues.

Representative Skarphol suggested information be provided to appropriation committees during the next legislative session regarding findings and recommendations made in agency audits.

Mr. Nagel presented the audit report for the Public Service Commission for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report includes one internal control finding relating to recording of receipts, one finding of noncompliance relating to fixed assets inventory, and one area for operational improvement relating to inspection fees.

Mr. Nagel presented the audit report for the State Treasurer's office for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report does not include any findings or recommendations.

Mr. Nagel presented the audit report for the Tax Commissioner's office for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report does not include any findings or recommendations.

Mr. Nagel presented the audit report for the Veterans' Home for the years ended June 30, 2011 and 2010. He reviewed the auditor's responses to the committee guidelines and said the report includes two internal control findings relating to improper coding and lack of approval for adjustments to resident accounts.

Mr. Don LaFleur, Audit Manager, State Auditor's office, presented the information system audit report for ConnectND Campus Solutions. He said the report includes two recommendations relating to limiting developer's access to the production environment and not developing test accounts in the production environment.

Chairman Ruby called on Mr. John Mongeon, Brady, Martz & Associates PC, Certified Public Accountants, who presented the audit report for the Ag PACE fund for the years ended June 30, 2012 and 2011. Mr. Mongeon reviewed the auditor's responses to the committee guidelines and said the report contains an unqualified opinion and does not include any findings or recommendations.

Mr. Mongeon presented the audit report for the PACE fund for the years ended June 30, 2012 and 2011. He reviewed the auditor's responses to the committee guidelines and said the report contains an unqualified opinion and does not include any findings or recommendations.

Ms. Mindy Piatz, Brady, Martz & Associates PC, Certified Public Accountants, presented the audit report for the North Dakota Building Authority for the years ended June 30, 2012 and 2011. She reviewed the auditor's responses to the committee guidelines and said the report contains an unqualified opinion and does not include any findings or recommendations.

DEPARTMENT OF HUMAN SERVICES' ACCOUNTS RECEIVABLES

Chairman Ruby called on Mr. Paul Kramer, Fiscal Administrative Division, Department of Human Services, to present information (Appendix C) on the status of the department's accounts receivables pursuant to North Dakota Century Code (NDCC) Sections 25-04-17 and 50-06.3-08. Mr. Kramer said the total amount written off by the Department of Human Services for fiscal year 2012 was $6,508,234, of which $856,799 related to the human service centers, $5,612,659 related to the State Hospital, and $38,776 related to the Developmental Center at Westwood Park.

In response to a question from Representative Skarphol, Mr. Kramer said he would provide information to the committee regarding a 10-year summary of the accounts receivables status, the oldest accounts with a receivable balance, and the total number of accounts with a receivable balance at each human service center, the State Hospital, and the Developmental Center.

DISCOUNTING OF OIL PRODUCED ON NORTH DAKOTA STATE LANDS

Chairman Ruby called on Mr. Jeff Engleson, Deputy Commissioner and Chief Financial Officer, Department of Trust Lands, to present information (Appendix D) on the discounting of oil produced on North Dakota state lands. Mr. Engleson said historically, the benchmark price for North Dakota oil has been 90 percent of the West Texas Intermediate (WTI) price in Cushing, Oklahoma. He said a price below 90 percent of WTI for North Dakota oil means the oil is being sold at a discount and a price higher than 90 percent means North Dakota oil is being sold at a premium. He said the benchmark reflects the most common market forces, such as the extra cost of shipping, that make North Dakota oil worth less than WTI oil.

Mr. Engleson said North Dakota prices should be lower than WTI and Brent prices for the following reasons:

- North Dakota oil is not close to national (WTI) or international (Brent) markets.

- North Dakota has limited marketing opportunities due to an oil glut in Cushing, Oklahoma.
- Pipeline capacity issues create competition with Canadian oil for pipeline space.

Mr. Engleson said over the last three years, the average monthly price of oil received by the Department of Trust Lands has ranged from a premium of $8 to a discount of $8. He said from February 2012 through April 2012, North Dakota oil was selling at a discount with the largest discount being $8 in March 2012. He said new rail shipping facilities have allowed for a price stabilization during the spring and summer of 2012. He said rail shipping capacity in North Dakota was 275,000 barrels of oil per day at the end of 2011, over 400,000 barrels of oil per day during the summer of 2012, and could reach 730,000 barrels of oil per day by the end of 2012.

Mr. Engleson said recent estimates indicate the Department of Trust Lands has received a premium of over $3.9 million over the past three years for oil produced on state lands.

FUND SOURCE INFORMATION IN PEOPLESOFT

Chairman Ruby called on Mr. LaFleur to present information (Appendix E) on fund source information in PeopleSoft. Mr. LaFleur identified the following ways to identify fund source information from PeopleSoft when commingled funds are used:

- Use project numbers to track the revenue and expenditures from a specific revenue source.
- Identify a program number for each revenue source to track expenditures from the specific revenue source.
- Use unused chart fields and user defined fields available in PeopleSoft to track expenditures from a specific revenue source.

NORTH DAKOTA UNIVERSITY SYSTEM SHADOW SYSTEMS

Chairman Ruby called on Mr. Randall Thursby, Chief Information Officer, North Dakota University System, to present information (Appendix F) on North Dakota University System shadow systems. Mr. Thursby said a shadow system is a system that can duplicate or substitute the work of a central system such as ConnectND. He said PeopleSoft has much functionality but is unable to meet all of the reporting needs of the University System.

Mr. Thursby said the University System has a policy that information technology projects must have approval from the Chief Information Officer of the University System if the project interfaces with a major system hosted by the University System, impacts University System communications network, or impacts University System resources.

In response to a question from Representative Skarphol, Mr. Gordy Smith, Audit Manager, State Auditor's office, said accounting and auditing standards provide guidance on how to determine if a separate entity should be considered a component unit and, if it is a component unit, whether it should be blended or discreet for financial reporting purposes. He said a blended component unit's financial information would be included with the primary agency's financial information, and a discreet component unit's financial information would be listed separately from the primary agency.

In response to a question from Representative Skarphol, Mr. Thursby said the University System of Georgia requires all funding from foundations to be provided to the University System Board prior to distribution to a specific campus. He said the University System of Georgia does not allow any officers of the university to serve on foundation boards. He said athletics are paid for by donations or other fees related to the athletic activity. He said the state of Georgia allows foundations to use the same accounting system that universities use to allow for greater transparency in the use of the funds.

Representative Skarphol asked Legislative Council staff to prepare an analysis of how selected other states' university systems operate compared to North Dakota's university system regarding relationships with foundations, inclusion of foundations as component units of universities, and the ability of university employees to serve on foundation boards.

COMMITTEE DISCUSSION AND STAFF DIRECTIVES

It was moved by Senator Wanzek, seconded by Representative Skarphol, and carried on a voice vote that pursuant to Section 54-35-02.2 the committee accept the following reports presented to the committee:

1. **North Dakota network and security (September 28, 2012)**
2. **Aeronautics Commission (June 30, 2011 and 2010)**
3. **Department of Commerce (June 30, 2011 and 2010)**
4. **Commission on Legal Counsel for Indigents (June 30, 2011 and 2010)**
5. **Council on the Arts (June 30, 2011 and 2010)**
6. **Department of Corrections and Rehabilitation (June 30, 2011 and 2010)**
7. **State Department of Health (June 30, 2011 and 2010)**
8. **Insurance Commissioner's office (June 30, 2011 and 2010)**
9. **Labor Department (June 30, 2011 and 2010)**
10. **Office of Administrative Hearings (June 30, 2011 and 2010)**
11. **Parks and Recreation Department (June 30, 2011 and 2010)**
12. **Public Service Commission (June 30, 2011 and 2010)**

13. **State Treasurer's office (June 30, 2011 and 2010)**
14. **Tax Commissioner's office (June 30, 2011 and 2010)**
15. **Veterans' Home (June 30, 2011 and 2010)**
16. **ConnectND campus solutions (September 18, 2012)**
17. **Ag PACE fund (June 30, 2012 and 2011)**
18. **PACE fund (June 30, 2012 and 2011)**
19. **North Dakota Building Authority (June 30, 2012 and 2011)**
20. **Reports available but not selected for presentation:**
    a. **Board of Addiction Counseling Examiners (June 30, 2011 and 2010).**
    b. **Board of Clinical Laboratory Practice (June 30, 2011 and 2010).**
    c. **Board of Architecture (June 30, 2011 and 2010).**
    d. **Board of Occupational Therapy Practice (June 30, 2011).**
    e. **Soybean Council (June 30, 2011 and 2010).**
    f. **Education Standards and Practices Board (June 30, 2010).**
    g. **Marriage and Family Therapy Licensure Board (December 31, 2011) (financial statements only).**

It was moved by Representative Skarphol, seconded by Representative Kelsch, and carried on a voice vote that the Chairman and the staff of the Legislative Council be requested to prepare a report and to present the report to the Legislative Management.

Chairman Ruby thanked the committee members and the Legislative Council staff for their work during the interim.

No further business appearing, Chairman Ruby adjourned the meeting at 12:55 p.m.

_____
Becky Keller
Senior Fiscal Analyst

_____
Allen H. Knudson
Legislative Budget Analyst and Auditor

ATTACH:6