7

STATE OF MICHIGAN
DEPARTMENT OF ENVIRONMENTAL QUALITY
LANSING

DEQ

JENNIFER M. GRANHOLM
GOVERNOR

STEVEN E. CHESTER
DIRECTOR

August 23, 2007

Mr. Michael J. Moody, Director
Office of Financial Management
Department of Management and Budget
P.O. Box 30026
Lansing, MI 48909

Dear Mr. Moody:

Attached please find our revised corrective action plan to address the recommendations in the Performance Audit (761-0590-05) of the Selected General and Application Controls of the Department of Environmental Quality (DEQ). The period for this audit is March 1, 2003, through July 31, 2006. We previously presented a preliminary plan to your office on July 10, 2007, but since then the DEQ has reconsidered our department's ability to implement appropriate corrective actions related to finding number 1. DEQ believes that additional resources, and the hiring of an Information Systems Security Officer, is necessary to effectively implement recommendations of the OAG related to finding number 1.

The following is the audit response summary to the recommendations:

1. Citations complied with: 5
2. Citations which DEQ agrees with and will comply:
    a. Will comply with: 2, 3, 4
    b. Budget considerations: 1
3. Citations DEQ disagrees with: n/a

Please contact me if you have any questions concerning this plan.

Sincerely,

Signature Redacted

Richard T. Lowe, Director
Audit Services Bureau
Department of Management and Budget
517-335-0972

Attachment

c: Ms. JoAnn Merrick, Senior Executive Assistant to the Director, DEQ
Mr. James Kasprzak, DEQ
Mr. Ken Theis, DIT
Ms. Palmer Giron, DIT
Ms. Linda Pung, DIT

# Department of Environmental Quality
# Final Corrective Action Plan

## Performance Audit (761-0590-05) of the

## SELECTED GENERAL AND APPLICATION CONTROLS

## March 1, 2003 through July 31, 2006

### Finding Number 1: Security Program and Security and Access Controls

*Recommendation:*
We recommend that DEQ, in conjunction with DIT, establish and implement an information systems security program and security and access controls over data and data systems.

*DEQ Final Response:*
DEQ agrees with the recommendation and noted that the findings identify similar weaknesses in several of our department's application systems. DEQ issued a draft information systems security plan in 2006. The plan contains several recommended improvements for implementing an overall information system security program, including establishment of a central security function/advisory team, establishment of new policies and procedures, and ongoing risk assessment practices. However, DEQ has not been able to effectively implement the plan due to resource constraints.

DEQ believes that the hiring of an Information Systems Security Officer is necessary to effectively implement the information systems security plan. This will require additional funding and a hiring exception. Also, future risk assessments may identify system enhancements that are necessary to remediate security weaknesses, which may result in the need for additional funding. Consequently, DEQ is currently unable to identify a realistic date for implementation of this recommendation. DEQ will initiate discussions with the SBO as part of the FY 2009 budget development process to better assess realistic time lines for implementing these recommendations.

DEQ staff already revoked ERNIE user access for departed employees. For the Navision system, the department has recently implemented several significant security improvements, including: completing a reaccreditation review, revocation of unnecessary privileged access, limiting Navision super users to two staff, and reassigning Navision security duties to the OFM central security function. Significant progress has also been achieved related to logging and monitoring of Navision transaction activity.

Related to the LABWORKS application, DEQ Laboratory management has restricted developer access to production data, removed unnecessary privileged access rights, instituted an annual reaccreditation of user privileges, is developing monitoring procedures for logged activity, and has developed an audit trail of changes made outside of LABWORKS. Also, the LABWORKS vendor has informed DEQ Laboratory management that password encryption will be available in a future release of the application.

## Finding Number 2: Server Security

*Recommendation:*
We recommend DIT establish effective security and access controls over the server operating systems.

*DEQ Final Response:*
Both DEQ and DIT agree with the recommendation and both departments will work to establish appropriate controls as part of implementing an information security plan. Despite the noted risks, DIT informed us that it is not aware of any instances in which the confidentiality, integrity, or availability of DEQ information was compromised.

DIT has taken several steps to address these issues. All servers have been moved to the secure hosting center. Select servers have already been hardened to comply with the requirements of the Payment Card Industry, with all operating system patches and security patches in place, maintained, and monitored on a monthly basis for full compliance. All high-risk application-level vulnerabilities have also been identified and remedied. A similar project for additional servers will begin later this summer, and periodic scans for vulnerabilities will become a routine feature of the hosting environment. All DEQ related servers are scheduled to be hardened in compliance with this project by May 2008. In addition, to further enhance security for select services, server access at the level of the operating system will be available only to a small number of approved administrators and only through the use of "two-factor authentication" via an RSA SecurID system. Implementation of this enhancement is expected before June 2008 and full compliance with this recommendation will be achieved by August 2008.

## Finding Number 3: Change Management Controls

*Recommendation:*
We recommend DEQ and DIT establish effective change management controls.

*DEQ Final Response:*
DEQ and DIT agree with this recommendation and both departments will work to establish appropriate controls as part of implementing an information security plan. DIT is currently in the process of adopting formal Software Engineering Methodologies across the state enterprise (see www.michigan.gov/suite for details.) In conjunction with Project Management Methodologies, SEM provides a formal, documented, and repeatable framework for the full lifecycle management of a software or application project, including formal change control. Constraints based on the current freezes in hiring, training, and purchasing have slowed the implementation of this project. Initiation of this effort will commence in DEQ by October 2007.

## Finding Number 4: Backup and Recovery Controls

*Recommendation:*
We recommend that DEQ and DIT evaluate the criticality of DEQ's data and data systems to implement effective backup and recovery controls.

*DEQ Final Response:*
DEQ and DIT agree with this recommendation and are working together to establish appropriate backup and recovery controls, including data classification, as part of implementing an information security plan. Progress has already been achieved with regard to backup and recovery. For example, DIT has engaged Sun Microsystems Inc. to manage and monitor backup and recovery tasks for hosted servers, under a contract with specific stipulations regarding performance and service levels. Implementation of this service for all hosted DEQ servers (and data) is expected by November, 2007.

## Finding Number 5: Data Integrity

*Recommendation:*
We recommend that DEQ fully ensure the integrity of data for Navision and LABWORKS.

*DEQ Final Response:*
DEQ agrees with the recommendation but also notes that, although some invalid data was identified during the audit, several of the data fields are used for informational purposes and because of compensating controls, the identified data inconsistencies had minimal adverse impact to DEQ processes. However, the finding identified opportunities for improvement.

DEQ has already implemented several corrective actions related to the Navision and LABWORKS applications. For Navision, a combination of system enhancements and queries are being used to prevent (or identify on an interim basis) inconsistent data. For LABWORKS, several new queries are used to identify potential inaccurate data or instances where a separation of duties was not achieved. In addition, an audit trail is now in place for all changes made outside of the LABWORKS application (e.g., to associated spreadsheet files). Also, DEQ Laboratory management continues to rely on several "review" activities to identify and follow-up on potentially inconsistent or inaccurate data.

DEQ believes that this recommendation has been implemented.