STATE OF MICHIGAN
DEPARTMENT OF CORRECTIONS
LANSING

JENNIFER M. GRANHOLM
GOVERNOR

PATRICIA L. CARUSO
DIRECTOR

March 20, 2008

Bryan Weiler
Support Services Division
Office of State Budget
George W. Romney Building
111 South Capitol, 5th Floor
Lansing, MI 48913

Dear Mr. Weiler:

In accordance with the State of Michigan, Financial Management Guide, Part VII, attached please find a preliminary summary table and corrective action plans to address the recommendations that were directed at the Department of Corrections within the Office of the Auditor General's audit report of the:

Offender Management Network Information System

Questions regarding the preliminary summary table or corrective action plans should be directed to Connie MacKenzie, internal audit liaison, at 517 241-7342.

Sincerely,

DEPARTMENT OF CORRECTIONS

Signature Redacted

Patricia L. Caruso, Director
Attachment
PC/22/cm

c: S. DeBor
C. MacKenzie
D. Schrantz
K. Koppsch-Woods

Offender Management Network Information System
Department of Corrections
Preliminary Summary of Agency Responses to Recommendations
May 2002 through July 2007

1. Findings/Recommendations DOC complied with:

   None

2. Findings/Recommendations DOC will comply with by:

1a, 1g	09/08
1b, d, and f	12/08
1c	06/09
1e	12/09
2d	12/09
3	12/08
4a	07/08

3. Findings/Recommendations DOC disagreed with:

   None

Offender Management Network Information System
Department of Corrections
Preliminary Corrective Action Plan
May 2002 through July 2007

1. OMNI Access

The auditors again recommended that DOC establish a comprehensive information systems security program and effective access controls over OMNI.

Agency Preliminary Response:

DOC agrees and will comply.

Regarding item a., in 2006, DOC began taking steps to establish an information security officer position within the Automated Data Systems Section (ADSS) that would establish security policies, standards and operating procedures to safeguard OMNI data. Due to severe State budgetary constraints, the position was not approved; however, the position was recently approved and is being established.

Regarding item b., DOC will develop an appropriate profile for DIT application development staff.

Regarding item c., DOC will require correctional facilities to identify authorized requestors who will have the authority to request new user access or modifications to a user's access. As part of the duties of the information security officer, DOC will implement policies to assist DOC staff in determining the appropriate access particular to a user's job function.

Regarding item d., DOC will implement policies and procedures to suspend access for inactive OMNI user accounts and remove access for terminated employees. DOC will work with DIT to develop a routine process to identify OMNI accounts not accessed during a specified timeframe and will request the access be automatically suspended pending further review. DOC will work with the Bureau of Human Resources to develop procedures to identify employees who have separated from DOC and to remove access to OMNI in a timely manner.

Regarding item e., DOC will take steps to improve assignment of appropriate OMNI profiles based upon an employee's job responsibilities and audit all non-DOC OMNI users to confirm documentation is available within ADSS to validate user access for business needs. DOC has started a process to suspend access to a user's existing account when a request for a new account at a different work location is received.

Regarding item f., DOC has reduced the number of security administrators to 10 and will work to further limit the number of ADSS security administrators with the development of a security unit. In addition, DOC will explore the establishment of audit trails for all users with administrator access.

Regarding item g., DOC began corrective measures in 2007 by retaining logs of security background checks and security agreements for non-DOC OMNI users. DOC will conduct an audit to confirm that security verification documentation is available within ADSS for all non-DOC OMNI users.

2. OMNI Database and Operating System Security

The auditors recommended that DIT and DOC fully establish security controls over the OMNI databases and operating system.

Agency Preliminary Response:

Regarding item d., DOC agrees and will comply. DOC will coordinate with DIT to ensure that a complete data dictionary is developed for the OMNI databases.

3. OMNI Audit Trails

The auditors recommended that DOC fully develop and monitor audit trails for OMNI data.

Agency Preliminary Response:

DOC agrees and will comply by coordinating with DIT to incorporate automatic audit trails within tabs that contain confidential data, such as social security numbers, and by integrating audit trails that will generate reports that are accessible by DOC independent of DIT. Further, DOC will explore expanding the security within OMNI to allow DOC the ability to either block a user from viewing an offender's record or allow only certain users access to view an offender's record.

4. Change Control Process

The auditors recommended that DIT and DOC develop a comprehensive change control process for OMNI.

Agency Preliminary Response:

Regarding item a., DOC agrees and will comply by modifying its change request forms to include the name of the person who requested the change, the name of the person within the Automated Data Systems Section (ADSS) who is requesting the change to be implemented, and the name of an ADSS manager who approved the request. Upon staff providing test acceptance in the test application environment, an ADSS manager will document his/her authorization to implement and notify DIT that the change is authorized for implementation.