

# Operational Services Division

## *Findings on Reportable Conditions*

### **Finding Number 12: Electronic Data Interchange (EDI) Controls Need To Be Improved**

Controls over the Electronic Data Interchange (EDI) application need to be enhanced. Throughout the previous year and continuing into the next few years, the EDI effort will be expanded by adding additional vendors. This is a critical time in the development of EDI for Massachusetts and the framework for future development and maintenance should be established. In prior audits, the following areas were noted as needing improvement:

- Data and program files were currently not protected by either physical or logical security controls; as a result, unauthorized access may be obtained.
- Formal systems development and maintenance procedures were not in place to manage the change management process. Programmers should not be able to make direct changes to production that management may not be aware of.
- Current business continuity planning activities did not encompass the EDI application.
- A Service Auditor's Report (SAS 70) from the EDI vendor had not been obtained.

Accordingly, we made recommendations to address each of the areas cited above. In our follow-up to the implementation of the recommendations, we were advised that (1) a SAS 70 report had been obtained for 1997 and a request for the 1998 report has been made, (2) the change over to the more secure server has not yet taken place and testing is in process, (3) all changes to the EDI application are tested before they are moved to production and (4) the EDI system is backed up nightly. (*Fiscal year 1996; 1997 Report Finding 10*)

### **Recommendation:**

We recommend that testing of the more secure server be continued and the change over take place as soon as possible. We continue to recommend that only authorized individuals have the ability to make changes to programs and data and the business continuity plan encompass the EDI application.

### **Department corrective action plan:**

The Operational Services Division (OSD) would like to thank the auditors for their time and attention. OSD will take corrective action as follows:

1. Testing of the more secure server has been completed and it was moved into production concurrent with the MMARS Year 2000 upgrade on December 7<sup>th</sup> 1998.

2. Access to the system is limited to staff whose duties include EDI system monitoring/maintenance as a primary or backup responsibility.
3. By February 1999, continuity planning will be reviewed and revised to ensure it adequately includes the new EDI System.

[Next](#)

---

[Privacy Policy](#)

Any questions? Send e-mail to: [comptroller.info@state.ma.us](mailto:comptroller.info@state.ma.us).

Copyright 1999-2001, Massachusetts Office of the Comptroller, all rights reserved.