



MLDS CENTER

Maryland Longitudinal Data System

Address 550 West Baltimore Street
Baltimore, MD 21201
Phone 410-706-2085
Email mlds.center@maryland.gov
Website mldscenter.maryland.gov

MEMORANDUM

TO: MLDS Governing Board
FROM: Ross Goldstein
DATE: December 6, 2024
SUBJECT: MLDS Center FY 25 Budget

Purpose

The purpose of this agenda item is to provide the Board a mid-fiscal year update on the MLDS Center's FY 2025 budget.

Background

The Governing Board reviewed and approved the Center's FY 25 annual budget during the June 2024 meeting. There have been no changes to the budget or the Center's spending plans to date, with one exception. The proposed change is to authorize up to \$50,000 to hire a technical writer/information technology security consultant to review and revise the MLDS Center's *Data Security and Safeguarding Plan (DSSP)*. Under Education Article § 24-704(g), the Governing Board was required to establish a DSSP prior to the incorporation of any data into the system. The plan must address the following:

1. Authorized access and authentication for authorized access;
2. Privacy compliance standards;
3. Privacy and security audits;
4. Breach notification and procedures; and
5. Data retention and disposition policies;

The original DSSP developed by the Board has been in place since the initial implementation and development of the MLDS. Since that time there have been a lot of changes to the system and its operations and management. One important change is the role the Department of Information Technology plays in managing the system's security profile. In addition, Center staff have implemented security operations that are not reflected in the DSSP. Accordingly, the goal of the contract is to engage a technical writer/security consultant to:

1. Conduct a comprehensive review of:
 - a. The DSSP and related documents;
 - b. The role of DoIT's enterprise system management;
 - c. The Center's current system security procedures and operations; and
 - d. The *State of Maryland Information Technology Security Manual*.
2. Revise DSSP to be up-to-date, include current best practices, and be in full alignment with DoIT requirements and the IT Security Manual.

Action

We request the Governing Board approve the proposed, additional expenditure.