OFFICE OF THE CHANCELLOR

December 12, 2012

1807
University of Maryland, Baltimore

1856
University of Maryland, College Park

1865
Bowie State University

1866
Towson University

1886
University of Maryland Eastern Shore

1898
Frostburg State University

1900
Coppin State University

1925
Salisbury University

1925
University of Baltimore

1925
University of Maryland Center for Environmental Science

1947
University of Maryland University College

1966
University of Maryland, Baltimore County

The Honorable Martin O'Malley
Office of the Governor
100 State Circle
Annapolis, Maryland 21401

Dear Governor O'Malley:

Under the terms of Chapter 190 of the Acts of the General Assembly of 2010, the Governing Board of the Maryland Longitudinal Data System is required to submit an annual report to the Governor and the Maryland General Assembly.

I am pleased to be given the opportunity to provide you with this report, which is enclosed, and hope that you find it useful and informative.

I am happy to address any questions you may have and look forward to continuing our work together in building Maryland's future through high quality education.

Sincerely yours,

WE Kirwan

William E. Kirwan
Chancellor

Enclosure

cc: President Thomas Miller
Speaker Michael Busch
John Ratliff, Office of the Governor
MLDS Governing Board
Caroline Boice, DLS
Jordan Butler, DBM
Sarah Albert, DLS

3300 Metzerott Road | Adelphi, MD 20783 | TEL: 301-445-1901 | FAX: 301-445-1931 | www.usmd.edu

A Report to the Maryland General Assembly and Governor Martin O'Malley

Regarding

The Development of the Maryland Longitudinal Data System & Maryland Longitudinal Data System Center

December 2012

Introduction

Under the terms of Chapter 190 of the Acts of the General Assembly of 2010, the Governing Board of the Maryland Longitudinal Data System (MLDS) is required to submit an annual report to the Maryland General Assembly containing the following:

1. An update on the implementation of the Maryland Longitudinal Data System (MLDS) and the activities of the Maryland Longitudinal Data System Center (hereafter, Center);
2. A list of all studies performed by the Center during the reporting period;
3. A list of currently warehoused data that are determined to be no longer necessary to carry out the mission of the Center;
4. Any proposed or planned expansion of data maintained in the database; and
5. Any other recommendations made by the Governing Board.

The following sections provide an overview of the Maryland Longitudinal Data System (MLDS), an update on the activities of the Governing Board, a report on requirement 1 – an update on the implementation of Maryland's Longitudinal Data System and Center, and a report on requirement 4 – planned data to be included in the MLDS. Reports on requirements 2, 3 and 5 listed above are not included in this report as the System and Center are not yet operational.

Overview of the Maryland Longitudinal Data System

This section includes information on the MLDS governance and an overview of the technical and data characteristics of the MLDS.

System Governance

Pursuant to Chapter 190 of the 2010 Acts of the Maryland General Assembly, the eleven (11) member Maryland LDS Governing Board met to organize and direct Maryland's LDS development. Dr. William Kirwan, Chancellor of the University System of Maryland, served as the Chair of the Governing Board in 2012.[1] Governor O'Malley charged the Board with creating the P-20-W Maryland LDS Center per Chapter 190 and the Board voted to accept the charge in December of 2010.

To coordinate staff-level work, the Board created the LDS Interagency Workgroup. This Workgroup includes representatives from all the participating agencies and provides coordination on technical and policy issues. Current planning is for this group to serve an advisory role to the Center staff when the Center is established and fully staffed. In addition,

[1] Full membership roster is included as **Appendix A**.

the Office of the Attorney General assigned Assistant Attorney General Elizabeth Kameen to advise the Board on issues surrounding the creation of this System and Center.

The Maryland State Department of Education (MSDE) is leading the project management efforts and is overseeing the build-out of the MLDS technology which will be used by the Center. MSDE coordinates this effort through the Interagency Technical Workgroup and various ad hoc workgroups with all of the involved agencies.

Overview of Technical and Data Characteristics of MLDS

The State of Maryland is in the process of developing a plan to construct a statewide data warehouse that contains longitudinal data in a P-20-W spectrum (P-20-W refers to Pre-Kindergarten through graduate school and/or the workforce). The MLDS will incorporate data collected by the Maryland State Department of Education (MSDE), the Maryland Higher Education Commission (MHEC), and the Maryland Department of Labor, Licensing and Regulation (DLLR).

The primary purpose of the MLDS is to address the critical policy questions that will inform education stakeholders at all levels in order to improve the quality of education in the state. In addition, the implementation of a P-20-W LDS will be a key factor in achieving the requirements identified by United States Department of Education in the America Competes Act, the assurances for State Fiscal Stabilizations Funds, and the Data Quality Campaign's 10 State Actions. It will also be critical in meeting the requirements of other state initiatives including Complete College America (CCA). Included below are an initial list of questions the system will be designed to address, areas for which policy questions will be developed and a list of federal assurances.

Critical Education Policy questions:

1. Are Maryland students academically prepared to enter postsecondary institutions and complete their programs in a timely manner?
2. What percentage of Maryland high school exiters go on to enroll in Maryland postsecondary education?
3. What percentage of Maryland high school exiters entering college are assessed to need to take developmental courses and in what content areas?
4. How likely are students placed in developmental courses to persist in postsecondary education and transfer and/or graduate?
5. Are community college students able to transfer within state to 4-year institutions successfully and without loss of credit?
6. What happens to students who start at community colleges and do not go on to 4-year institutions?

7. What are the differences in performance, retention, and graduation, including time to degree, of students who initially matriculate at a Maryland community college and transfer to a Maryland 4-year institution versus those who initially matriculate at a Maryland 4-year?
8. What are the differences in performance, retention and graduation, including time to degree, of students beginning in dual enrollment programs, at 2-year institutions and at 4-year institutions?
9. Which financial aid programs are most effective in improving access and success (i.e., retention and graduation) for Maryland students?
10. What are the characteristics of 2-year institutions that are allowing students to persist most effectively and either graduate or transfer?
11. Which 4- year institutions are graduating students most effectively and in the timeliest fashion?
12. What are the educational and labor market outcomes for individuals who use federal and state resources to obtain training at community colleges or other postsecondary institutions?
13. What economic value do noncredit community college credentials have in the workplace?
14. Are exiters of Maryland colleges successful in the workforce?
15. How do all of the policy questions vary by different critical subgroups* and backgrounds?

** including Race/Ethnicity, Gender, Age, Income level (defined by FARM eligibility/Pell Status), ESL status, Special Education status, Major discipline area, Geographic origin.*

Federal Assurances and Other Requirements

1. Incorporation into SLDS of student level exit, transfer in, transfer out, drop out or complete P-16 program information.
2. Creation of capacity in K-12 data systems to communicate with higher education data systems.
3. An audit system assessing data quality, validity, and reliability in SLDS.
4. Information on successful transition from secondary to postsecondary school, including whether students enroll in remedial coursework.
5. Other information as deemed necessary to address alignment and adequate preparation for success in postsecondary education and workforce.
6. Provide, for the State, for each LEA in the State, for each high school in the State and, at each of these levels, by student subgroup, the number and percent that enroll in an IHE within 16 months of receiving a regular high school diploma.

7. Provide, for the State, for each LEA in the State, for each high school in the State and, at each of these levels, by student subgroup, the number and percent who enroll in a public IHE within 16 months of receiving a regular high school diploma, the number and percent who complete at least one year's worth of college credit (applicable to a degree) within two years of enrollment in the IHE
8. The Number of High School Graduates with Postsecondary Enrollment

System Location

In order to provide cost savings and ensure the highest levels of security for the data, the information system for the MLDS is being developed in the Department of Public Safety and Correctional Services (DPSCS) data center. This is also the location of the MSDE PK-12 LDS and the MHEC data system upgrade. By locating the system development at DPSCS considerable cost avoidance has been realized through co-service agreements. No decision has been made on the ultimate location of the data system, but the security and ongoing savings opportunity will make DPSCS an attractive option as the long-term location of the system.

System Capabilities and Requirements

The MLDS is being constructed to meet all the requirements specified in Chapter 190 and provide critical data support for policy decisions and reporting. The most important capabilities of the technical system will be the successful integration of data from the three existing data systems into the MLDS Center, the ability to generate useful information from that data, and to make that information available to key groups (including as much data as possible for the general public). The key capabilities of this system include tools to:

- extract data from a wide range of source systems of varying levels of technological sophistication;
- transform data, as needed, for validity and compatibility;
- load data into a common data repository;
- create policies that ensure confidentiality of information;
- implement technology and practices that conform to security and confidentiality best practices and policies;
- generate and modify easily a large number of standard reports;
- enable the creation and saving of customizable queries of any data field in the system;
- produce graphical representations of data; and
- ensure reports are available in easy-to-understand formats via the internet.

Requirement 1 – Update on Implementation of the Maryland Longitudinal Data System (MLDS)

The Board, through the organizational mechanisms described above, has made considerable progress in establishing the Maryland Longitudinal Data System and the MLDS Center, which will administer and use that system. The following sections outline the implementation timeline for the MLDS and MLDS Center, the status of supporting technical projects, the planning and organization for the MLDS Center, the status of Maryland's most recent SLDS grant and an overview of the current funding status.

Timeline for Implementation

The system development plan prepared for the Race to the Top grant project, which funds the development of the MLDS, estimates that the MLDS data warehouse with the Center would go fully into production by July 2013. However, this "full-go-live" System will not be fully completed until MSDE turns over of the data warehouse application, associated hardware, and operations methods to the MLDS Governing Board and its Center staff for operation. It is estimated that the MLDS data warehouse development will be completed by July 2013 and turned over to the MLDS Governing Board in February 2014.

In order to bring the MLDS into operation and begin serving the needs of Marylanders as soon as possible, a phased roll-out strategy has been developed that will allow certain MLDS dashboards to become publicly available as quickly as possible. The remainder of this section lays out the phased "go-live" strategy to meet the timeline, and identifies key tasks to make the Center and MLDS fully operational. This project divides the rollout into three phases: an Alpha Rollout, Beta Rollout, and Operational Rollout. Table 1 shows these three phases, and associated key tasks.

"Alpha Rollout"

The initial work on the Alpha Rollout phase was completed in September 2012 with plans to make the results public in January 2013. The Alpha phase focused on meeting specific statutory requirements and on making key aspects of the system ready for user acceptance testing. The key tasks in this phase include:

Acceptance testing:

- The setup of the development and test software and hardware environments.
- Development of the database to support four dashboards.
- Development of dashboards for the first four policy questions.
- Development of the P20 policy interface for the four policy questions.

- Development of a publicly available set of data tables and dashboards.

Statutory requirements:

- Agreement by MSDE, MHEC and DLLR to provide specific data flows to the MLDS.
- Approval by the MLDS Governing Board of the data security and safeguarding plan (see Appendix B).
- Approval by the MLDS Governing Board of the data inventory (see Appendix C).
- Approval by the MLDS Governing Board to load data into the system.

"Beta Rollout"

The Beta Rollout phase is scheduled to be completed by July 2013. This phase focuses on:

- Identification and hiring of an Executive Director for MLDS Center.
- Establishing the MLDS Center and initial staff hiring.
- Completion of development of the MLDS data warehouse including dashboards, policy briefs, and data import programs.
- Implementation of operations procedures and inter-agency memorandums of understanding needed for the Center and data warehouse system to go into full service operation.
- Loading of production data with quality verification.
- Implementation of full security procedures and technologies.
- Testing and signoff of the data warehouse functionality by the testers provided by the participating MLDS agencies.

"Operational Rollout"

The final phase is the Operational Rollout phase and will extend from July 2013 into 2014. This phase is scheduled to be completed by February 2014 and is sometimes commonly refer to as "Go-Live." This phase focuses on completing the set up of the MLDS Center physical facility and hiring of staff, and the legal change of ownership of the MLDS data warehouse software and computers to the MLDS Governing Board from MSDE. At this point the Center should be fully operational and fully staffed and technical infrastructure will be administered by the MLDS Center's technical team.

A phased rollout strategy will bring the MLDS Center and the MLDS to full operational status by February 2014 while allowing complex, interdependent tasks and approval processes to be accomplished in a timely manner. The phased rollout approach also allows access to the MLDS data warehouse for testing and limited use purposes as early as possible without compromising security or data usage requirements.

Table 1 – Implementation Time Line

GOING-LIVE STAGES & TASKS		PROGRESS MILESTONES
OPERATIONAL ROLLOUT Center and System Service Ready	>>>	February 1, 2014
MSDE transfers system to MLDS Governing Board		February 1, 2014
MLDS Center reviews System for transfer acceptance		November 1, 2013
MLDS Center Technical Team Fully Staffed		September 1, 2013
MLDS Center FY14 Budget		July 1, 2013
BETA MLDS ROLLOUT System Used by Agency Analysts and Expanded Public data	>>>	July 1, 2013
User dashboard & security testing/signoff completed		Pending
Production & ID crosswalk data load completed		Pending
Data quality & ETL controls fully implemented		Pending
System operations procedures implemented		Pending
Executive Director of MLDS Center Hired		Pending
SASID-SSN ET and Batch data collection implemented		In progress
MLDS Center facility selection		In progress
Policy briefs for P20 questions completed		In progress
Development of all dashboards completed		In progress
Full login & data security systems implemented		In progress
Production system installed		In progress
ALPHA MLDS ROLLOUT Access Granted to User Testers and limited Public data available	>>>	Sept. 2012
Inter-agency data governance & DPSCS MOUs		Completed
MLDS Board approves glossary and security plan that allows data loading to MLDS databases in MLDS environments		Completed
Testing of interface & Sept. dashboards completed		Completed
Limited login & data access security implemented		Completed
Temporary data MOUs for inter-agency test data, and development database loaded		Completed
Data Security Governance document completed		Completed
Data Glossary for initial data sets operational		Completed
Test system installed		Completed
P20 policies & user interface for Sept. developed		Completed
Dashboards/databases for Sept. developed		Completed
Development system installed		Completed

Supporting Technical Projects

In addition to the main technical effort associated with the creation of the MLDS data warehouse, there exist several critical supporting technical projects which are required to create a data and technology infrastructure which will allow the MLDS to be both effective and efficient in meeting the State's data needs. They include:

- Electronic transcripts – The implementation of electronic transcripts is considered critical to this project because it will allow the routine transmission of critical data at a very high level of quality between the Local Education Agencies (LEA's) and the institutions of higher education (IHE's). Currently, all Maryland public IHE's and a majority of LEA's are moving towards adoption of electronic transcripts within the standard established by the MLDS Governing Board. Maryland's independent IHE's are not adopting the specified electronic transcripts, but plan to provide data by other means.

- PK-12 LDS system – Resident within MSDE, the PK-12 LDS is rapidly moving toward expansion. Unlike the cross agency system, this system is entirely governed within MSDE and provides federal assurance reporting, and direct support to individual schools and districts. It provides the technical model which is being used for the construction of the MLDS System to be used by the MLDS Center. It is substantially complete and in use.

- Higher Education Data System – MHEC is currently upgrading its technical systems in order to more effectively be able to process data and support the MLDS. In addition, MHEC is engaged in the most extensive revision of its data collections in more thirty years to ensure that critical and timely data are available for both agency use and the MLDS.

- Workforce Data System – DLLR working with the Jacob France Institute has a long standing system for tracking individuals in the workforce. They are currently engaged in an expansion of this system supported by a grant from the U.S. Department of Labor. DLLR is also in the process of upgrading existing Adult Ed and Correctional Ed data systems with SLDS grant monies.

Implementation of the MLDS Center

The Board is currently proceeding with a plan to establish the MLDS Center through a partnership between the School of Social Work (SSW) and College of Education (COE) at the University of Maryland (UM) and the Maryland State Department of Education (MSDE), Maryland Higher Education Commission (MHEC), and the Department of Labor, Licensing and Regulation (DLLR). This collaboration provides the opportunity to capitalize on the strengths and capacities of each partner to best provide the kind of data services, management, research and program evaluation that will advance effective educational and training outcomes across the state. The Center will be overseen by the Executive Director who will report directly to the Governing Board.

Central to this collaboration and long-term achievement of management efficiencies is a proposed shared staffing model. Many of the positions including three associate directors will be half-time employees of the Center and hold half-time appointments within either agencies or the university. Other staff may be similarly shared. This will allow the MLDS Center to effectively remain integrated into the critical business of the State's agencies and draw on the considerable intellectual and research resources of the University.

The three Associate Directors will be hired to oversee the complementary processes for successful Center operation: Information Technology and Data Management; Reporting and Portal Services; and Research and Policy Services. The areas of responsibility associated with each area are:

- Information Technology and Data Management – This division will oversee the security of MLDS data and maintenance and development of the MLDS Center technology. Leveraging the enormous amount of effort that has already gone into the development of data transfer and access mechanisms, MSDE, MHEC, and DLLR will continue their ongoing joint efforts to gather, merge, and manage the data from the various sources including managing the partnership with DPSCS.

- Reporting and Portal Services– This division will oversee the development of the data dashboard content to ensure that it is appropriately accessible to end users. This group will provide 'fast response' activities in order to respond to time sensitive data information requests from policy makers or education leaders. Staff in the Reporting and Portal Services team will maintain reports that have been created and are part of the data dashboard and will work with the Research and Program Evaluation team to create new information for the web portal as research and policy questions are answered.

- Research and Policy Services– This division's activities consist of the development of research questions, and creating an evidence-based context to interpret results. The University of Maryland School of Social Work (at UMB) and College of Education (at UMCP) are national leaders in research and evaluation services and will be at the forefront of the research and evaluation efforts. This division of the center will focus on expanding knowledge of key education issues, formulation of answerable research questions that will inform and advance education policy and programming across Maryland, and the advanced statistical analysis needed to analyze large complex datasets.

Figure 1 and 2 provide a graphical representation of the major units and relationships in this organizational framework. Staff members assigned to this collaborative effort are currently developing a budget which will focus on maximizing the current grant resources and phase in operations at the center as it becomes operational in Fiscal Year 2014.

Figure 1: Overview of Proposed Organizational Structure of MLDS Center

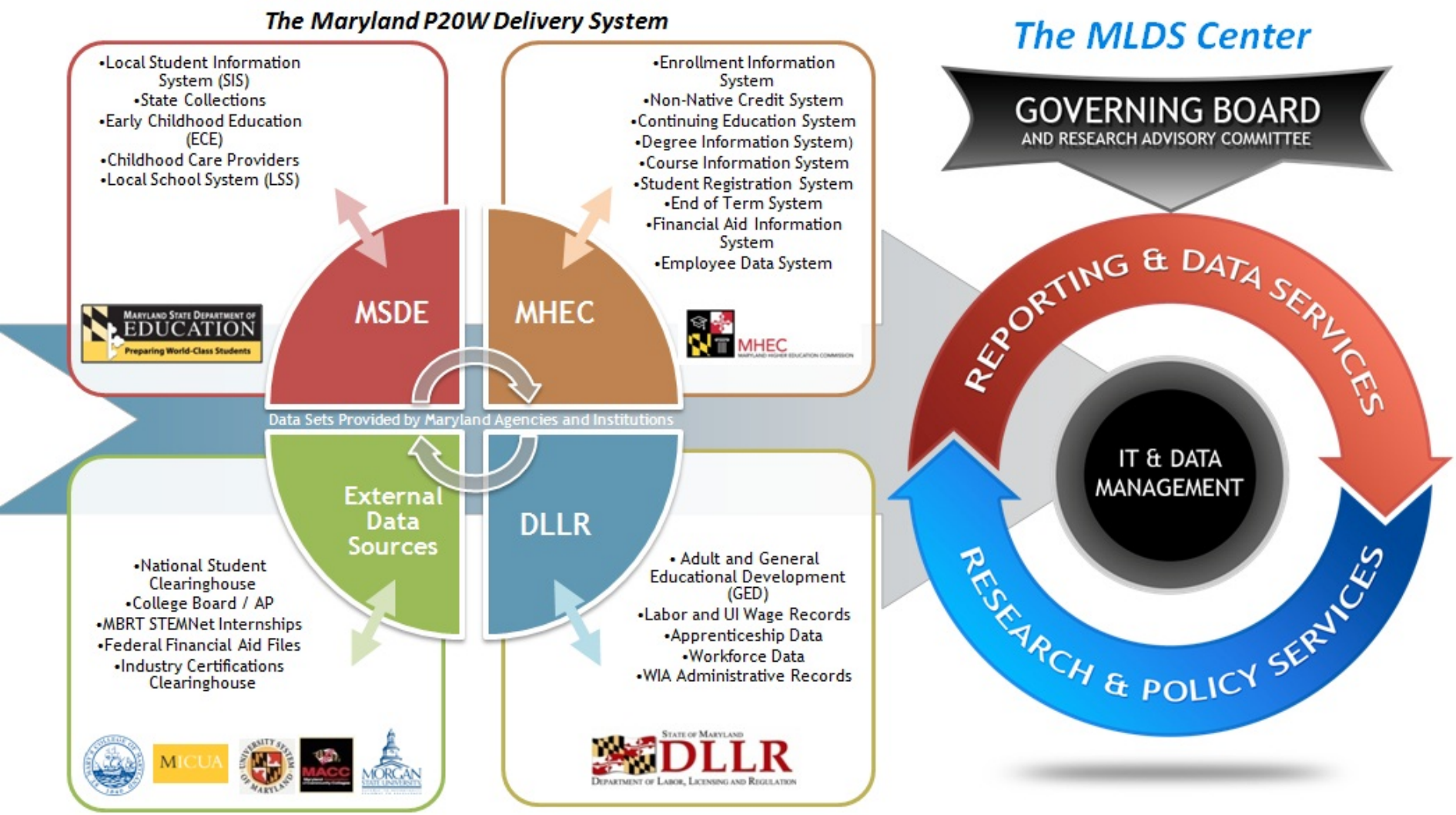
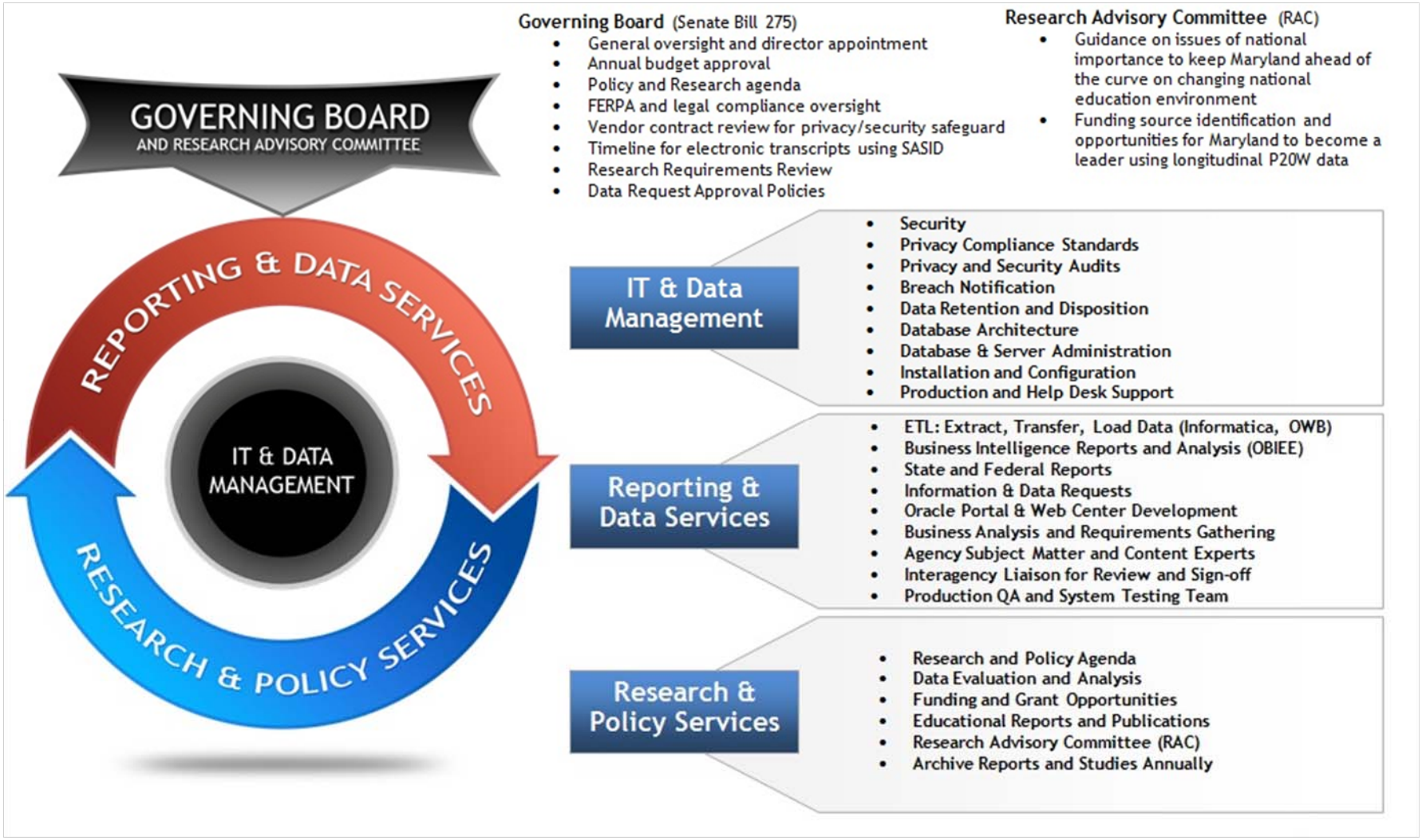


Figure 2: Organization of Critical Tasks in Proposed MLDS Center Organization



New SLDS Grant

During 2012, the state of Maryland was awarded a third U.S. Department of Education State Longitudinal Data System grant. The purpose of the award was to allow the State "to develop and link postsecondary and/or workforce data with the State's PK-12 data system." The PK-12 LDS and MLDS face challenges to delivering the kind of data that is anticipated by both policy makers and the education community. These challenges include: (a) gaps in data collections; (b) complexity in blending disparate data from multiple agencies; (c) the ability to carry out research on critical areas; and (d) training of key policy makers, such as state legislators, on how to use MLDS data. To meet these challenges, this grant will attempt to accomplish five objectives:

- Expand data collections for the MLDS – These expanded collections will include private career school data, adult GED® data, adult correctional education data;
- Improve the quality of the data – This will be accomplished through the implementation of a master data management system and the addition of a probabilistic directory data matching subsystem and web service;
- Create advanced Dashboards for Policy Decision Makers – These include development of a PK12-P20W CTE curriculum alignment dashboard, early college access outcome dashboard, Develop College-to-Work CTE program outcome dashboard, and a Education to Work Life-Span Summary dashboard;
- Expand Training and Professional Development for Policy Decision Makers – This includes the addition of an MLDS Research Training Academy and a MLDS Legislators Training Academy;
- Provide funding for an initial round of MLDS Research – Projects include assessment of STEM post-graduate student regional work retention, the assessment of the need for inclusion of online education data in the MLDS, and the assessment of the training and retention of early childhood workforce in Maryland.

Taken together these projects will substantially advance the MLDS toward a complete and operational data system.

Current Funding Overview

Per Chapter 190, the Governing Board is responsible for seeking State funding and extramural sources of funding. This section details the sources of funding currently being used in the work to establish the MLDS and MLDS Center. It is broadly divided between State of Maryland sources and Federal sources.

State funding

At present no State General Funds have been allocated specifically for the MLDS Center or any of its supporting systems. A budget is currently being prepared that requests a state general fund allocation which will allow the MLDS Center to become operational during FY 2014.

Additionally, although no direct funding has been allocated, MSDE, MHEC, DLLR, USM and the Jacob France Institute have provided substantial unreimbursed in-kind contributions of staff time and expertise. Morgan State, St. Mary's, the Maryland Association of Community Colleges (MACC), and the Maryland Independent Colleges Association (MICUA) have also allocated staff to MLDS work.

Federal Funding

The State of Maryland received two federal grants in 2010 and one in 2012 that are being used directly in the creation of the Center or in support of the three participating agencies. These federal grants are listed below:

US Department of Education "Race to the Top" Grant
Maryland's receipt of a $250 million Race to the Top grant has significantly propelled the development of the LDS and Center. "Using data to improve instruction" was one of the four assurances of Race to the Top, and the State's application designated more funding for this section than any other single section, with approximately $47 million allocated for improvements in data capabilities. Included in this $47 million is $5 million designated specifically for the creation of the P-20 portion of the MLDS and supporting higher education systems at MHEC.

US Department of Education State Longitudinal Data System Grants
MLDS development has been supported by three federal SLDS grants. The previous two grants were focused on the development of the PK-12 systems at MSDE, while the most recent grant and its goals are described on the previous page. These grants totaled $15.5 million dollars and have supported the development of the technological infrastructure for the systems now in place. None of these grants provide operating funds.

Requirement 4 – Update on Implementation of the Maryland Longitudinal Data System (MLDS)

The initial data inventory and loading of data into the MLDS test environment took place during the fall of 2012. Data were loaded from systems at MSDE, MHEC, DLLR and external data sources (e.g. National Student Clearinghouse). Portions of these data will be transferred into the production system in early 2013 for the initial release for public and agency review. A complete list of the current data elements and planned data elements appear in the data inventory included in Appendix C of this document.

Conclusion

This report has detailed the development of the Maryland P-20-W Longitudinal Data System and Center during 2012. It was prepared in accordance with the terms of Chapter 190 of the Acts of the General Assembly of 2010. With the continuing support of the U.S. Department of Education Race to the Top Grant, the State of Maryland reached several key milestones in implementing the requirements of this statute. Progress was made on the completion of several key documents and policies required for implementation, an operational test system was completed, the Board endorsed an organizational framework for the MLDS Center, and a additional SLDS grant was received. At this time, the System and the Center are on track for completion during the course of 2013.

Appendices

Appendix A. Maryland Longitudinal Data System Governing Board 2012 Membership Roster

Ex Officio Members:

Dr. William "Brit" Kirwan
Chancellor
University System of Maryland
Board Chairman

Dr. Lillian Lowery
State Superintendent
Maryland State Department of Education

Dr. Danette Howard
Secretary
Maryland Higher Education Commission

Mr. Leonard J. Howie III
Secretary
Maryland Department of Labor, Licensing, and Regulation

Dr. Bernard Sadusky
Executive Director
Maryland Association of Community Colleges

Dr. David Wilson
President
Morgan State University

Dr. Michael Martirano
Superintendent
St. Mary's Public Schools
**Representing Superintendents*

Public Members:

Ms. Nicole Marano
Stevenson University
**Representing Higher Education with Expertise in Large Data Systems*

Ms. Ayana English-Brown
Prince George's County Public Schools
**Representing Teachers*

Mr. Jason Perkins-Cohen
Job Opportunities Task Force
**Representing Workforce*

Mr. Brian Roberts
Montgomery County
**Representing Parents*

Appendix B

MARYLAND STATE LONGITUDINAL DATA SYSTEM

(MLDS)

DATA SECURITY AND SAFEGUARDING PLAN

VERSION 1.0

SEPTEMBER 6, 2012

Table of Contents

1 Introduction 1-1
1.1 Purpose 1-1
1.2 Background 1-1
1.3 Data Security and Safeguard Policy Priorities 1-1
1.4 Document Organization 1-2
1.5 Roles and Responsibilities 1-2
1.6 References 1-3
2 Data Governance Security 2-1
2.1 Goals and Objectives 2-1
2.2 Data Governance Guiding Principles 2-1
2.3 Roles and Data Protection Responsibilities 2-1
2.3.1 Executive Director, MLDS Center 2-1
2.3.2 Data Governance Board 2-2
2.3.3 Data Steward (Project Managers) 2-2
2.3.4 Information Security Officer/ Privacy Officer 2-2
2.3.5 IT Analyst(s) 2-3
2.3.6 System Administrator 2-3
2.3.7 Data Base Administrator 2-3
2.3.8 Employees 2-3
2.3.9 Data Stakeholders 2-3
2.4 Data Quality and Integrity 2-4
2.5 Access Agreements – Data Sharing 2-4
3 Authorized Access & Authentication Standard 3-1
3.1 Access Control Policy and Procedures 3-1
3.2 Account Management 3-1
3.3 Account Types and Access Privileges 3-2
3.4 Access Enforcement 3-2
3.5 Information Flow Enforcement 3-2
3.6 Separation of Duties 3-2
3.7 Least Privileged 3-2

3.8 Unsuccessful Login Attempts 3-3
3.9 System Use Notification 3-3
3.10 Concurrent Session Lock 3-3
3.11 Session Lock 3-3
3.12 Remote Access 3-4
3.13 Wireless Access 3-4
3.14 Access control for Mobile Devices 3-5
3.15 Use of State Agency and State Institution Data Systems 3-5
3.16 User-Based Collaboration & Information Sharing 3-6
3.17 Identification & Authentication Procedures 3-6
3.18 Identification and Authentication (Authorized Users) 3-6
3.19 Device-to-Device Identification and Authentication 3-6
3.20 Identifier Management 3-6
3.21 Authenticator Management 3-7
3.22 Authenticator Feedback 3-8
3.23 Cryptographic Module Authentication 3-8
3.24 Personnel Categorization 3-8
3.25 Personnel Screening 3-9
3.26 Personnel Termination 3-9
3.27 Personnel Transfer 3-9
3.28 Contract and Service Providers 3-10
3.29 Personnel Sanctions 3-10
4 Privacy Compliance Standard 4-1
4.1 Privacy Program 4-1
4.2 Privacy Impact and Risk Assessment 4-1
4.3 Privacy Requirements for Contractors and Service Providers 4-1
4.4 Privacy Awareness 4-1
4.5 Privacy Notice 4-2
4.6 Dissemination of Privacy Program Information 4-2
4.7 Use Limitation of Student or Workforce Data 4-2
4.8 Inventory of Student or Workforce Data 4-3

4.9 Complaint Management 4-3
4.10 Privacy Monitoring 4-3
5 Auditing Standard for Privacy & Data Security 5-1
5.1 Auditing and Accountability Procedure 5-1
5.2 Auditable Events 5-1
5.3 Content of Audit Records 5-1
5.4 Audit Storage Capacity 5-2
5.5 Response to Audit Processing Failure 5-2
5.6 Audit Review Analysis, and Reporting 5-2
5.7 Audit Reduction and Report Generation 5-2
5.8 Time Stamps 5-2
5.9 Protection of Audit Information 5-3
5.10 Non-Repudiation 5-3
5.11 Audit Record Generation 5-3
5.12 Audit Record Retention 5-3
6 Breach Notification Procedures 6-1
6.1 Breach Notification Procedures 6-1
6.2 Privacy Reporting 6-1
6.3 Privacy Incident Response 6-1
7 Data Retention and Disposition Standard 7-1
7.1 Data Retention and Disposition Procedures 7-1
7.2 Data Retention and Disposal 7-1
8 General Controls 8-1
8.1 Information Integrity 8-1
8.1.1 Malicious Code 8-1
8.1.2 MLDS Monitoring 8-1
8.1.3 Security Alerts, Advisories, and Directives 8-1
8.2 Security Awareness and Training Procedures 8-2
8.2.1 Security Awareness 8-2
8.2.2 Security Training 8-2
8.2.3 Security Training Records 8-2

8.3 System Security Assessment and Authorization 8-2
8.3.1 Security Assessments 8-2
8.3.2 MLDS Connections 8-3
8.3.3 Plan of Action and Milestones – System Level 8-3
8.4 Configuration Management 8-3
8.4.1 Configuration Management Plan and Procedures 8-3
8.4.2 Baseline Configuration 8-4
8.4.3 Configuration Change Control 8-4
8.4.4 Configuration Settings 8-4
8.4.5 Least Functionality 8-5
8.4.6 MLDS Component Inventory 8-5
8.5 Contingency Planning 8-6
8.5.1 Contingency Planning Procedures 8-6
8.5.2 MLDS Recovery and Reconstitution 8-6
8.5.3 Contingency Plan 8-6
8.5.4 Contingency Training, Plan Testing, and Exercises 8-7
8.5.5 Alternate Storage Site 8-7
8.5.6 MLDS Backup 8-7
8.6 Incident Response 8-8
8.6.1 Incident Response Procedures 8-8
8.6.2 Incident Response Training, Testing, and Exercises 8-8
8.6.3 Incident Handling 8-8
8.6.4 Incident Monitoring 8-8
8.6.5 Incident Reporting 8-8
8.6.6 Incident Response Assistance 8-9
8.6.7 Incident Response Plan 8-9
8.7 Maintenance 8-9
8.7.1 Maintenance Procedures 8-9
8.7.2 Controlled Maintenance 8-10
8.7.3 Maintenance Tools 8-10
8.7.4 Non-Local Maintenance 8-10

8.7.5 Maintenance Personnel 8-11
8.7.6 Timely Maintenance 8-11
8.8 Media Protection 8-11
8.8.1 Media Protection Procedures 8-11
8.9 Physical and Environmental Protection 8-12
8.9.1 Physical and Environmental Protection Procedures 8-12
8.9.2 Physical Access Authorizations 8-12
8.9.3 Physical Access Control 8-12
8.9.4 Access Control for Transmission Medium 8-13
8.9.5 Access Control for Output Devices 8-13
8.9.6 Monitoring Physical Access 8-13
8.9.7 Visitor Control 8-13
8.9.8 Access Records 8-13
8.9.9 Power Equipment and Power Cabling 8-14
8.9.10 Emergency Shutoff 8-14
8.9.11 Emergency Power 8-14
8.9.12 Emergency Lighting 8-14
8.9.13 Fire Protection 8-14
8.9.14 Temperature and Humidity Controls 8-14
8.9.15 Water Damage Protection 8-15
8.9.16 Delivery and Removal 8-15
8.9.17 Alternate Work Site 8-15
8.9.18 Location of MLDS Components 8-15
8.10 Risk Assessment 8-15
8.10.1 Risk Assessment Procedures 8-15
8.10.2 Risk Assessment 8-15
8.10.3 Vulnerability Scanning 8-16
8.10.4 Rules of Behavior 8-16
8.11 Security Program Management 8-17
8.11.1 Senior Information Security Officer 8-17
8.11.2 Information Security Resources 8-17

8.11.3 Plan of Action and Milestones – Program Level 8-17
8.11.4 MLDS Inventory 8-17
8.11.5 Information Security Measures of Performance 8-17
9 Terms and Terminology (Note: Not all terms below are used in this document) 9-1
10 Record of Revisions 10-4
11 Background Information 11-5
11.1 Data Governance Workflow 11-5

1 Introduction

1.1 Purpose

The Maryland Longitudinal Data System (MLDS) Data Security and Safeguard Plan identifies required policies and procedures to address safeguard requirements for the:

- Maryland Longitudinal Data System (MLDS);
- MLDS Center and the Data Center at which the MLDS is housed; and the,
- MLDS data governance process.

1.2 Background

The Maryland Education Article §24-702 establishes the MLDS, which is "… a statewide data system that contains individual-level student data and workforce data from all levels of education and the State's workforce." Section 24-704 outlines the minimally acceptable data security and safeguard requirements that are to be met prior to the system going operational and populated with live (versus non-sensitive test) data. Section 24-703 states that there will be a MLDS Center, which is an independent unit within the State government. The Center is responsible for conducting the business processes that are required "… to examine student progress and outcomes over time, including preparation for postsecondary education and the workforce." (§24-702 (b)(2)).

Researchers may use student or workforce data which has undergone anonymization or de-identification to conduct research. Section 9 contains definitions of these terms. Only employees of the MLDS Data Center are authorized to access the MLDS and to conduct this research.

The Data Security and Safeguarding Plan will be reviewed periodically and the resulting revisions will be documented in Section 10, Record of Revisions.

1.3 Data Security and Safeguard Policy Priorities

To ensure compliance with the intent of the legislation, data security and safeguard requirements are provided and are in accordance with the priorities stated in:

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 polices.

Additional policies and procedures will be developed as needed. Security and safeguard requirements address and are consistent with the requirements and guidance found in paragraph 1.6, References. The Governing Board and Center Executive Director are responsible for

managing risks to the MLDS project. This plan shall be reviewed on an annual basis to evaluate the effectiveness of the controls in managing MLDS risks.

1.4 Document Organization

The MLDS Data Security and Safeguards Program shall adopt a hierarchical approach to the development and implementation of policy and procedures, developing policy first and then procedures. The policy statements will reflect content from sources within paragraph 1.6. When possible, federal and publicly available sources will be used as the basis for the procedures and tailored to the specific needs of the MLDS Center and the MLDS.

The MLDS Data Security and Safeguard Plan is a living document and will contain the top level policy statements from which procedures will be developed. Appendices may be added as new policy requirements become known.

Section 2 describes the data governance process and associated security controls. This section is in draft pending the actual start of MLDS Center operations.

Sections 3 through 8 describe the planned data security and safeguard controls for the MLDS Center and the MLDS.

Section 9 contains terms and terminology relevant to the MLDS.

Section 10 contains Revision History.

Section 11 contains supporting documentation.

1.5 Roles and Responsibilities

The Maryland Longitudinal Data System Center shall:

- Oversee and maintain the warehouse of the MLDS data sets,
- Ensure routine and ongoing compliance with the federal Family Educational Rights and Privacy Act (FERPA), the federal Privacy Act, the federal Workforce Investment Act (WIA), the U.S. Department of Labor's rules governing confidentiality of State Unemployment Compensation information, and other relevant privacy laws, regulations, and policies,
- Provide data security, including the capacity for audit trails, and
- Perform regular audits for compliance with data privacy and security standards.

The Executive Director of the MLDS Center shall ensure the implementation of the requirements found within this Data Security and Safeguarding Plan.

1.6 References

Family Educational Rights and Privacy Act (FERPA) Legislation Act of 1974 (20 U.S.C. § 1232g; 34 CFR Part 99), FERPA Regulations. Retrieved from http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf

Federal Register, Family Educational Rights and Privacy (2011). Notice of Proposed Rule. Retrieved from https://www.federalregister.gov/articles/2011/04/08/2011-8205/family-educational-rights-and-privacy#p-3

Federal Register, 20 CFR 603 - FEDERAL-STATE UNEMPLOYMENT COMPENSATION (UC) PROGRAM; CONFIDENTIALITY AND DISCLOSURE OF STATE UC INFORMATION https://www.federalregister.gov/select-citation/2006/09/27/20-CFR-603

Maryland State Information Technology Security Policy and Standards. Retrieved from http://doit.maryland.gov/support/pages/securitypolicies.aspx

U.S. Department of Commerce, National Institute of Standards and Technology (2009). *Special Publication (SP) 800-53, Revision 3: Recommended Security Controls for Federal Information Systems and Organizations*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

U.S. Department of Commerce, National Institute of Standards and Technology (2012). *Special Publication (SP) 800-53, Initial Public Draft: Recommended Security Controls for Federal Information Systems and Organizations*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

U.S. Department of Commerce, National Institute of Standards and Technology (2010). *Special Publication (SP) 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

U.S. Department of Commerce, National Institute of Standards and Technology (2010). *Special Publication (SP) 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

U.S. Department of Education, Privacy Technical Assistance Center (2011). *Data Governance and Stewardship Checklist.* Retrieved from http://www2.ed.gov/policy/gen/guid/ptac/pdf/issue-brief-data-governance-and-stewardship.pdf

U.S. Department of Education, Privacy Technical Assistance Center (2011). *Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records*. Retrieved from http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011601

U.S. Department of Education, Privacy Technical Assistance Center (2011*). Data Stewardship: Managing Personally Identifiable Information in Electronic Student Educations Records.* Retrieved from http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011602

U.S. Department of Education, Privacy Technical Assistance Center (2011). *Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting.* Retrieved from http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011603

2 Data Governance Security

2.1 Goals and Objectives

This section is in draft. Its purpose is to outline any additional information technology security controls that are necessary to support the data governance process. A short definition of data governance is how the MLDS Center will perform decision making regarding data retrieval, sharing, and use.

2.2 Data Governance Guiding Principles

Below bullets represent an initial set of guiding principles and are *draft only*.

- *Regular review of MLDS holdings of collected student or workforce data to determine whether the student or workforce data is still relevant and necessary for meeting the MLDS Center's purpose and mission.*
- *Outlines how data will be retrieved, shared, and used*
- *Ensure value from efforts*
- *Maintain scope and focus of data retrieval and use*
- *Establish accountabilities*
- *Define measurable success*
- *Anyone handling student or workforce data or with ability to access the information should be trained annually in the handling of sensitive information and in their responsibilities to monitor, detect, and report any security violations*

2.3 Roles and Data Protection Responsibilities

Note: The below comments are ***draft*** *only and will be formalized once the MLDS Center has adopted a defined data governance process. A draft data governance work flow is found at Section 11.*

2.3.1 Executive Director, MLDS Center

The Executive Director shall oversee the functions and duties of the MLDS Center. As identified in the Maryland Education Article § 24-703, those functions and duties, which address data governance, compliance, or security, include the following:

a. Serve as a central repository of student data and workforce data in the Maryland Longitudinal Data System, including data sets provided by:
   (i) The State Department of Education;
   (ii) Local education agencies;
   (iii) The Maryland Higher Education Commission;
   (iv) Institutions of higher education; and,
   (v) The Department of Labor, Licensing, and Regulation;

b. Oversee and maintain the warehouse of the Maryland Longitudinal Data System data sets;
c. Ensure routine and ongoing compliance with the federal Family Educational Rights and Privacy Act and other relevant privacy laws and policies, including:
    (i) The required use of de-identified data in data research and reporting;
    (ii) The required disposition of information that is no longer needed;
    (iii) Providing data security, including the capacity for audit trails;
    (iv) Providing for performance of regular audits for compliance with data privacy and security standards; and
    (v) Implementing guidelines and policies that prevent the reporting of other potentially identifying data;
d. Conduct research using timely and accurate student data and workforce data to improve the State's education system and guide decision making by State and local governments, educational agencies, institutions, teachers, and other education professionals;

2.3.2 Data Governance Board

[Decision making regarding how data will be retrieved, shared, and used.]

- *Consists of MLDS Center Data Stewards*
- *Set direction for data quality*
- *Monitor data quality*
- *Report status for quality-focused initiatives*
- *Identify stakeholders, establish decision rights, clarify accountability*
- *Ensure protection of sensitive data*
- *Align initiatives*
- *Enforce regulatory, contractual, architectural, and compliance requirements*
- *Identify measures of success*

2.3.3 Data Steward (Project Managers)

- *Monitor data quality;*
- *Protect sensitive data, and student or workforce data;*
- *Identify risk;*
- *Coordinate with stakeholders;*
- *Ensure consistent data usage and data definitions;*
- *Report on data-related tasks or projects;*
- *Monitor data to determine when no longer used or needed;*
- *Maintain inventory of data assets*

2.3.4 Information Security Officer/ Privacy Officer

[May be sole responsibility or an additional duty; Responsible for monitoring implementation of this plan]

- *Assess risk or other impact of adding or acquiring additional data from existing or new external source*
- *Document assessment results*
- *Add or modify existing controls, if required*
- *Update system security plan;*
- *Monitors the controls within this plan that are specific to privacy;*
- *Investigates and reports data breaches; and,*
- *Proves compliance with privacy and data governance policies.]*

2.3.5 IT Analyst(s)

- *Assess impact of adding data to the MLDS*
- *Document assessment results*
- *Plan and implement any new or modified extract, transform, or load actions*
- *Conduct operational test/verify results*
- *Update data dictionaries*

2.3.6 System Administrator

The System Administrator for the MLDS shall:

- *Setup and Maintain user accounts*
- *Maintain the system, ensuring patches and settings are in alignment with this plan and relevant procedures*
- *Trouble shoot problems and arrange for repairs*
- *Monitor system performance*
- *Install software*
- *Create backup and be able to recover the system*
- *… Note – these duties need to be coordinated with the MLDS Data Center system admins]*

2.3.7 Data Base Administrator

[Responsibilities to be determined]

2.3.8 Employees

[Adhere to rules, report incidents, complete annual training awareness]

2.3.9 Data Stakeholders

[Refers to, i.e., Maryland Department of Labor, Licensing, and Regulation (DLLR), State Department of Education (MSDE) and the Maryland Higher Education Commission (MHEC)] and agreements with MLDS Center on data use and handling]

2.4 Data Quality and Integrity

The MLDS Center shall:

a. Confirm to the greatest extent practicable upon retrieval of student or workforce data , the accuracy, relevance, timeliness, and completeness of that information;
b. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information; and,
c. Document processes to ensure the integrity of student or workforce data through existing security controls.

2.5 Access Agreements – Data Sharing

The MLDS Center shall:

a. Ensure that individuals requiring access to MLDS (such are repair persons or employees) sign appropriate access agreements prior to being granted access; and
b. Review/update the access agreements annually or when major changes have occurred.

3 Authorized Access & Authentication Standard

3.1 Access Control Policy and Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented authorized access and authentication procedure that will limit access to the MLDS to authorized users. The procedure:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Facilitates the implementation of the authorized access and authentication policies and associated authorized access and authentication controls.

3.2 Account Management

a. The MLDS Center shall manage information system accounts, including:
    1) Identifying account types;
    2) Group or shared IDs are prohibited unless they are documented as "Functional IDs". Functional IDs are user accounts associated with a group or role that may be used by multiple individuals (e.g., Emergency Problem/Fix IDs) or that are associated with a particular production job process;
    3) Identifying authorized users of the information system and specifying access privileges (see paragraph 3.3 below). Direct access to data in the Maryland Longitudinal Data System shall be restricted to authorized staff of the Center;
    4) Ensuring each user has a unique user ID;
    5) Requiring approval from appropriate officials for requests to establish accounts;
    6) Establishing, activating, modifying, disabling, and removing accounts in a timely manner;
    7) Archiving inactive or terminated use accounts;
    8) Specifically authorizing and monitoring the use of temporary accounts;
    9) Notifying account managers when temporary accounts are no longer required and when MLDS users are terminated, transferred, or MLDS usage or need-to know/need-to-share changes;
    10) Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
    11) Validating system users who request reinstatement of user account privileges suspended or revoked by the MLDS;
    12) Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and

13) Reviewing accounts: (i) User accounts shall be reviewed quarterly, at a minimum; and (ii) Privileged accounts (e.g., system administrators, accounts with elevated access privileges) shall be reviewed semi-annually, at a minimum.

b. The MLDS Center shall employ automated mechanisms to support the management of MLDS accounts.
c. The MLDS shall, through automation:
    1) Terminate temporary and emergency accounts within 72 hours;
    2) Disable accounts which have been inactive after 90 days; and,
    3) Audit account creation, modification, disabling, and termination actions and notify, as required, appropriate individuals.

3.3 Account Types and Access Privileges

The MLDS Center shall define and manage account types and access privileges for the MLDS to include access to virtual machines or servers, the local area network and components, and the database.

3.4 Access Enforcement

The MLDS Center and the MLDS shall enforce approved authorizations for logical access to the system in accordance with applicable procedures.

3.5 Information Flow Enforcement

The MLDS shall enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable MLDS policy or procedures.

3.6 Separation of Duties

The MLDS Center shall:

a. Separate duties of individuals, to prevent harmful activity without collusion;
b. Document separation of duties; and,
c. Implement separation of duties through assigned MLDS access authorizations.

3.7 Least Privileged

The MLDS Center shall:

a. Employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with the MLDS mission and functions;
b. Explicitly authorize access to security functions (deployed in hardware, software, and firmware) and security-relevant information; and,
c. Require that users of MLDS accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other

system functions, and if feasible, audit any use of privileged accounts, or roles, for such functions.

3.8 Unsuccessful Login Attempts

The MLDS shall lock an account after four (4) consecutive unsuccessful access attempts within a fifteen (15) minute period by automatically locking that account for a minimum of 60 minutes. While the 60 minutes password count will be reset after 60 minutes, the account will remain locked until unlocked by an administrator.

3.9 System Use Notification

The MLDS shall:

a. Display an approved system use notification message or banner that identifies the system as the property of the Maryland State Government, before granting access to the system that provides privacy and security notices consistent with state and federal and state laws, directives, polices, or guidance. The text shall read:

> "Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of State of Maryland."

b. Maintain the system-use notification message/warning banner on the screen until the user takes explicit actions to log on to or further access the MLDS.

3.10 Concurrent Session Lock

The MLDS shall limit the number of interactive sessions as follows:

a. One (1) session for non-privileged authorized accounts (e.g., users);
b. Three (3) sessions are allowed for privileged accounts (e.g., system administrators, accounts with elevated access privileges); and,
c. Accounts used for automated processing by applications (e.g., database, service accounts) are not subject to the concurrent session limits above.

3.11 Session Lock

The MLDS shall implement a session lock at the operating system level that:

a. Initiates a session lock (e.g., screensaver) after 15 minutes of inactivity or upon receiving a request from the user (e.g., lock computer); and,
b. Prevents further access (e.g., password protected) to the system until the user reestablishes access using established identification and authentication procedures.

3.12 Remote Access

The MLDS Center shall:

a. Document allowed methods of remote access to the MLDS;
b. Establish usage restrictions and implementation guidance for each allowed remote access method;
c. Monitor for unauthorized remote access to the MLDS;
d. Authorize remote access to the MLDS prior to connection;
e. Enforce requirements for remote connections to the MLDS;
f. Employ automate mechanisms to facilitate the monitoring and control of remote access methods;
g. Use cryptography to protect the confidentiality and integrity of remote access sessions. Encrypted remote access circuits shall comply with the encryption standards as outlined in FIPS 140-2;
h. Route remote accesses to the MLDS through a limited number of managed access control points;
i. Restrict the execution of privileged commands and access to security-relevant information via remote access for compelling operational needs only, and only when an operational emergency exists, such as a breach or potential breach of the MLDS's security;
j. Continuously monitor for unauthorized remote connections to the MLDS and take appropriate action if an unauthorized connection is discovered;
k. Ensure that remote sessions for accessing security functions and security-relevant information employ additional security measures and are audited; and,
l. Disable networking protocols within the MLDS deemed to be non-secure, except for explicitly identified components in support of specific operational requirements.

3.13 Wireless Access

a. The MLDS Center shall:
    1) Establish usage restrictions and implementation guidance for wireless access in accordance with the Maryland Department of Information Technology Information Security Policy, version 3.0, Appendix D;
    2) Monitor for unauthorized wireless access to the MLDS;
    3) Authorize wireless access to the MLDS prior to connection;
    4) Enforce requirements for wireless connections to the MLDS; and,
    5) Monitor for unauthorized wireless connections to the MLDS, including scanning for unauthorized wireless access points, at least semi-annually, and take appropriate action if an unauthorized connection is discovered.
b. The MLDS shall protect wireless access to the system using authentication and encryption.

3.14 Access control for Mobile Devices

a. The MLDS Center shall:
   1) Establish usage restrictions and implementation guidance for MLDS Center laptop computers and other Portable Electronic Devices (PEDs) (e.g., PDAs, cellular phones);
   2) Document, monitor, and control access of laptop computers and other Portable Electronic Devices (e.g., PDAs, cellular phones) to the MLDS;
   3) Monitor for unauthorized connections of mobile devices to the MLDS;
   4) Enforce requirements for the connection of mobile devices to the MLDS;
   5) Disable MLDS functionality that provides the capability for automatic execution of code on removable media without user direction;
   6) Issue specially configured mobile devices to individuals traveling to locations that the MLDS Center deems to be of significant risk in accordance with internal policies and procedures;
   7) Apply approved inspection and preventative measures to mobile devices returning from locations that are deemed to be of significant risk in accordance with the State of Maryland policies and procedures;
   8) Restrict the use of writable, removable media within the MLDS. The use of removable media in the MLDS shall be prohibited when the owner of the media cannot be identified; and,
   9) Prohibit the use of privately owned portable electronic devices or removable media to process, store, or transmit MLDS information.

   Note: Examples of removable media include: USB memory sticks, external hard disk drives and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Personally owned equipment shall include all systems, devices, software, and media owned by an individual, but shall not include systems, devices, software, media that the MLDS Center has on a payment schedule or is leasing, or contractor-furnished IT equipment. Personally owned equipment, software and media (e.g., thumb drives, etc.) shall not be used to process, access, or store sensitive information, nor shall such equipment be connected to the MLDS directly or via a Virtual Private Network (VPN).

3.15 Use of State Agency and State Institution Data Systems

a. The MLDS Center shall establish terms and conditions, consistent with any trust relationships established with the state agencies and institutions providing data to the MLDS, allowing authorized individuals to access the MLDS for the purpose of transmitting student and workforce data.
b. The MLDS Center shall permit authorized individuals to access the MLDS to process, store, or transmit data only when the MLDS Center:

1) Can verify the implementation of required security controls on the state agency and state institution as specified in the MLDS Center's information security plan; or
2) Has an approved MLDS connection or processing agreement with the state agency or state institution system providing data to the MLDS.

3.16 User-Based Collaboration & Information Sharing

The MLDS Center shall define circumstances for using collaborative methods or tools by authorized MLDS users when these users are sharing information or data with other authorized MLDS users.

3.17 Identification & Authentication Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented identification and authentication procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among MLDS Center, and compliance; and
b. Facilitates the implementation of identification and authentication controls.

3.18 Identification and Authentication (Authorized Users)

The MLDS shall:

a. Uniquely identify and authenticate authorized users (or processes acting on behalf of authorized users);
b. Use multifactor authentication for network access to privileged accounts; and,
c. Use multifactor authentication for local access to privileged accounts.

3.19 Device-to-Device Identification and Authentication

a. The MLDS shall:
   1) Uniquely identify and authenticate devices before establishing a connection.
   2) Authenticate devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based. NOTE: Remote network connection is any connection with a device communicating through an external network (e.g., the Internet); and,
   3) Authenticate devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

b. The MLDS Center shall standardize, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device.

3.20 Identifier Management

a. The MLDS Center shall manage MLDS identifiers for authorized users and devices by:

1) Receiving authorization from a designated MLDS Center official to assign a user or device identifier;
2) Selecting an identifier that uniquely identifies an individual or device;
3) Assigning the user identifier to the intended party or the device identifier to the intended device;
4) Preventing reuse of user or device identifiers;
5) Prohibiting the use of MLDS account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address);
6) Requiring that registration to receive a user ID and password include authorization by a supervisor, and be done in person before a designated registration authority; and,
7) Managing user identifiers by uniquely identifying the user.

b. The MLDS shall dynamically manage identifiers, attributes, and associated access authorizations.

3.21 Authenticator Management

a. The MLDS Center shall manage MLDS authenticators for authorized users and devices by:
   1) Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
   2) Establishing initial authenticator content for authenticators defined by the MLDS Center;
   3) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
   4) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
   5) Changing default content of authenticators upon MLDS installation;
   6) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
   7) Changing/refreshing authenticators ; and,
   8) Protecting authenticator content from unauthorized disclosure and modification; and
   9) Requiring users to take, and having devices implement, specific measures to safeguard authenticators.
      NOTE: User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration.

b. The MLDS, for password-based authentication, shall:
   1) Enforce minimum password construction, usage and change requirements as follows:

a) The password must not be the same as the user id;
b) Passwords must never be displayed on the screen;
c) Change temporary passwords at the first logon;
d) Passwords must be a minimum of eight (8) characters and consist of mixed alphabetic, numeric, and special characters. Passwords must not consist of all numbers, all special characters, or all alphabetic characters;
e) Passwords must not contain leading or trailing blanks;
f) Force change of user passwords every 90 days;
g) Password reuse must be prohibited by not allowing the last 20 passwords to be reused with a minimum password age of at least 48 hours;
h) Where possible, users should be prohibited from only changing/or adding one (1) character to their previous password (i.e., users should be prohibited from using passwords that are similar to their previous password);
i) State issued login credentials (username & password) shall not to be used for ancillary 3rd party services (online Web accounts, e-mail, e-commerce, etc.)
j) Passwords older than the expiry date must be changed before any other system activity is performed;
k) User ids associated with a password must be disabled or locked after 60 days of inactivity; and,
l) When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established.

2) Encrypt passwords in storage and in transmission.

c. The MLDS, for PKI-based authentication (if PKI is in use), shall:
   1) Validate certificates by constructing a certification path with status information to an accepted trust anchor;
   2) Enforce authorized access to the corresponding private key; and
   3) Map the authenticated identity to the user account.
d. The MLDS Center shall require that the registration process to receive authenticators be carried out in person before a designated registration authority with authorization by a designated MLDS Center official (e.g., a supervisor).

3.22 Authenticator Feedback

The MLDS shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

3.23 Cryptographic Module Authentication

The MLDS shall use mechanisms for authentication to a cryptographic module that meets the requirements of Federal Information Processing Standard (FIPS) Pub 140-2.

3.24 Personnel Categorization

The MLDS Center shall:

a. Assign a sensitivity/risk level designation for all positions (employee and contractor);
b. Establish screening criteria for individuals filling these positions; and
c. Review and revise position sensitivity/risk level designations at a minimum annually or when position descriptions are rewritten.

3.25 Personnel Screening

The MLDS Center shall screen all employees and contractors before authorizing access to the MLDS, at a minimum a criminal background check will be performed. All MLDS Center employees shall sign a confidentiality agreement upon accepting employment with the MLDS Center.

3.26 Personnel Termination

a. The MLDS Center shall require departing employees to return all forms of media used to gain system access to MLDS Center media, personal electronic devices, keys, identification (ID) cards, proxy cards, and any other MLDS Center property on their last workday.
b. Unfriendly termination (fired or resignation) involves the removal of an employee under involuntary or adverse conditions (e.g., engaging in unauthorized activities). Given the potential for adverse consequences during unfriendly termination, the MLDS Center shall at a minimum, include the following in unfriendly termination procedures (Note: Unfriendly termination (fired or resignation) involves the removal of an employee under involuntary or adverse conditions (e.g., engaging in unauthorized activities) and may result in adverse consequences):
    1) Immediate termination of MLDS access;
    2) Retrieval of MLDS Center property (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes);
    3) Briefing on the continuing responsibilities for confidentiality and privacy; and
    4) Retaining access to MLDS Center information and the MLDS formerly controlled by the terminated individual.
c. The MLDS Center shall conduct an exit interview with a departing employee, after an employee is notified of termination, but before their departure, to ensure all out processing/exit actions are completed and all MLDS Center property and equipment is returned.

3.27 Personnel Transfer

The MLDS Center shall implement and maintain procedures to ensure appropriate system accesses are revoked for employees/contractors who leave the MLDS Center, are reassigned to other duties, on extended leave, or are under disciplinary actions.

a. Logical and physical access authorizations to the MLDS and MLDS Center facilities shall be reviewed when personnel are reassigned or transferred to other positions within the MLDS Center.

b. Transfer or reassignment actions shall be initiated within five (5) business days of the formal transfer action.

3.28 Contract and Service Providers

a. The MLDS Center shall:
   1) Establish personnel security requirements including security roles and responsibilities for contractor or service providers (for example, Data Center contractor or service employees, hosting center contractor or service employees) ;
   2) Require contractors and service providers to comply with personnel security policies and procedures of the organization (for example, Data Center contractor or service employees, hosting center contractor or service employees);
   3) Document personnel security requirements; and
   4) Monitor provider compliance.
b. The MLDS Center shall require contractor and service providers to notify the Information Security Officer of the MLDS Center of any personnel transfers or terminations of any contractor or service employees working at any MLDS Center facilities with credentials, badges, or MLDS privileges within 24 hours.

3.29 Personnel Sanctions

The MLDS Center shall employ a formal sanctions process, as set forth in relevant state laws, for personnel failing to comply with established information security policies and procedures.

4 Privacy Compliance Standard

4.1 Privacy Program

The MLDS Center shall:

a. Assign an employee as the Privacy Officer accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the retrieval, use, maintenance, sharing, and disposal of student or workforce data.
b. Develop, disseminate, review, and update annually a formal, documented privacy compliance procedure that:
    1) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2) Facilitates the implementation of the privacy compliance policy and associated privacy controls
c. Monitor federal and state privacy laws and policy for changes that affect the privacy program; and,
d. Allocate budget and staffing resources to implement and operate the MLDS privacy program.

4.2 Privacy Impact and Risk Assessment

The MLDS Center shall:

a. Establish a privacy risk assessment process that assesses privacy risk to individuals resulting from the retrieval, sharing, storing, transmitting, and use of student or workforce data; and,
b. Conduct a Privacy Impact Assessment (PIA) for the MLDS in accordance with applicable state law and federal privacy laws.

4.3 Privacy Requirements for Contractors and Service Providers

The MLDS Center shall:

a. Establish privacy roles and responsibilities for contractors and service providers;
b. Require any contractors or service providers who may require temporary access, for purpose of repairs or emergencies, to the MLDS to sign a confidentiality agreement; and
c. Include privacy requirements in MLDS Center contracts and other acquisition-related documents.

4.4 Privacy Awareness

The MLDS Center shall:

a. Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
b. Administer basic privacy training at least annually and targeted, role-based privacy training for personnel having responsibility for student or workforce data or for activities that use this data, at least annually; and
c. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually.

4.5 Privacy Notice

The MLDS Center shall provide a privacy notice that reflects the MLDS legislative requirements:

a. Direct access to data in the Maryland Longitudinal Data System shall be restricted to authorized staff of the Center.
b. The Center may only use de-identified data in the analysis, research, and reporting conducted by the Center.
c. The Center may only use aggregate data in the release of data in reports and in response to data requests.
d. Data that may be identifiable based on the size or uniqueness of the population under consideration may not be reported in any form by the Center.
e. The Center may not release information that may not be disclosed under the federal Family Educational Rights and Privacy Act and other relevant privacy laws and policies.

4.6 Dissemination of Privacy Program Information

The MLDS Center shall:

a. Ensure that the public has access to information about its privacy activities and is able to communicate with its Privacy Officer; and
b. Ensure that its privacy practices are publicly available through organizational websites or otherwise.

4.7 Use Limitation of Student or Workforce Data

a. Student or workforce data is a specific type of sensitive information that the MLDS shall receive from sources, such as the Maryland Department of Labor, Licensing, and Regulation, State Department of Education and the Maryland Higher Education Commission.
b. The MLDS Center shall use student or workforce data internally only for the authorized purpose(s) as identified in the legislative language (see paragraph 4.5 above);
c. All MLDS employees shall be responsible for protecting any student and workforce data that they may have in their possession, whether the student and workforce data is in paper form or in MLDS-owned computer equipment and the MLDS.

d. Student or workforce data shall only be viewed by those authorized employees within the MLDS Center as having a "need to know" or requires access to the information, in the performance of their duties.
e. Sensitive information, such as user accounts and passwords, and student or workforce data that is stored or transmitted by computer equipment (such as laptops and memory storage devices) shall be encrypted.
f. Sensitive Information, such as such as user accounts and passwords, student or workforce data shall not be posted to internal or external websites.
g. No information containing sensitive or student or workforce data shall be placed into an employee's calendar (e.g., Outlook, etc.).

4.8 Inventory of Student or Workforce Data

The MLDS Center shall:

a. Identify the student or workforce data that are relevant and necessary to accomplish the legally authorized purpose of the data retrieval;
b. Limit the retrieval and retention of the student or workforce data to the minimum elements identified for the purposes
c. Conduct an initial evaluation of student or workforce data holdings and establish and follow a schedule for regularly reviewing those holdings at least semi-annually to ensure that the student or workforce data continues to be necessary to accomplish the legally authorized purpose for which it was collected;
d. Establish, maintain, and update an inventory that contains a listing of all MLDS subsystems identified as retrieving, using, or maintaining student or workforce data; and
e. Provide each update of the student or workforce data inventory to the Center Executive Director or information security official to support the establishment of information security requirements.

4.9 Complaint Management

The MLDS Center shall:

a. Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.
b. Respond to complaints, concerns, or questions from individuals within 30 business days.

4.10 Privacy Monitoring

The MLDS Center shall inspect semi-annually, and monitor as near real time as feasible, privacy controls and internal privacy procedures, to ensure effective implementation.

5 Auditing Standard for Privacy & Data Security

5.1 Auditing and Accountability Procedure

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented audit and accountability procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the audit and accountability policy and associated audit and accountability controls.

5.2 Auditable Events

The MLDS Center shall:

a. Determine, based on a risk assessment, that the MLDS is capable of auditing events as identified in the Maryland Department of Information Technology Information Security Policy, version 3.0, paragraph 7.1;
b. Coordinate the security audit function with other organizational entities (for example, Office of Legislative Audits, security consultants, Department of Information Technology, internal auditors) requiring audit related information to enhance mutual support and to help guide the selection of auditable events;
c. Provide a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents;
d. Determine, based on current threat information and ongoing assessment of risk, what events are to be audited within the MLDS; and,
e. Review and update the list of identified auditable events at a minimum annually;
f. Include execution of privileged functions in the list of events to be audited by the MLDS. Note: In this context, privileged functions consist of commands executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

5.3 Content of Audit Records

The MLDS shall:

a. Produce audit records that contain sufficient information, at a minimum, to establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event; and,
b. Include detailed information in the audit records for audit events identified by type, location, or subject.

5.4 Audit Storage Capacity

The MLDS Center shall allocate audit record storage capacity based on the types of auditing to be performed and the audit processing requirements, and configure auditing to reduce the likelihood of such capacity being exceeded.

5.5 Response to Audit Processing Failure

The MLDS Center shall:

a. Alert the MLDS Information Security Officer in the event of an audit processing failure; and,
b. Implement additional actions in accordance with the MLDS Incident Response Procedures.

5.6 Audit Review Analysis, and Reporting

The MLDS Center shall:

a. Review and analyze MLDS audit records, on a routine basis (daily or weekly), for indications of inappropriate or unusual activity, and report findings to the MLDS Information Security Officer; and
b. Adjust the level of audit review, analysis, and reporting within the MLDS when there is a change in risk to MLDS operations, assets, individuals, based on law enforcement information, intelligence information, or other credible sources of information; and,
c. Integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

5.7 Audit Reduction and Report Generation

The MLDS shall provide:

a. An audit reduction and report generation capability, which does not alter original audit records. Note: An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements. and for after-the-fact investigations of security incidents; and,
b. The capability to automatically process audit records for events of interest based on selectable, event criteria as identified in applicable state policy.

5.8 Time Stamps

The MLDS shall:

a. Use internal system clocks to generate time stamps for audit records, and,
b. Synchronize internal information system clocks at a minimum quarterly.

5.9 Protection of Audit Information

The MLDS shall protect audit information and audit tools from unauthorized access, modification, and deletion.

5.10 Non-Repudiation

The MLDS shall achieve non-repudiation by protecting against an individual falsely denying having performed a particular action.

5.11 Audit Record Generation

The MLDS shall, in accordance with the Maryland Department of Information Technology Information Security Policy, version 3.0, and the MLDS Incident Response procedures:

a. Provide audit record generation capability for auditable events within the MLDS components;
b. Allow a designated organizational personnel to select which auditable events are to be audited by specific components of the system;
c. Generate audit records for auditable events; and,
d. Compile audit records into a system-wide (logical or physical) audit trail that is time-correlated.

5.12 Audit Record Retention

The MLDS Center shall retain audit records for the lesser of three (3) years or until the Office of Legislative Audits completes the audit of the entity to:

a. Enable the recreation of computer related accesses to both the operating system and to the application wherever confidential information is stored;
b. Provide support for after-the-fact investigations of security incidents; and
c. Meet regulatory and organizational information retention requirements.

6 Breach Notification Procedures

6.1 Breach Notification Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented breach notification procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the breach notification policy and associated breach notification controls.

6.2 Privacy Reporting

The Executive Director, MLDS Center, shall develop, disseminate, and update reports to the Governing Board at least semi-annually to demonstrate accountability with specific statutory and regulatory privacy program mandates.

6.3 Privacy Incident Response

The MLDS Center shall provide an organized and effective response to any privacy incident involving student or workforce data in accordance with the Incident Response Plan, as described in paragraph 8.6 of this document.

7 Data Retention and Disposition Standard

7.1 Data Retention and Disposition Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented data retention and disposition procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the data retention and disposition standard and associated data retention and disposition controls.

7.2 Data Retention and Disposal

The MLDS Center shall:

a. Retain student or workforce data in accordance with Maryland Education Article §24-702(c), which states, "The linkage of the student data and workforce data for the purpose of the MLDS shall be limited to no longer than 5 years from the date of latest attendance in any educational institution in the State."
b. Dispose of, destroy, erase, and/or anonymize the student or workforce data, regardless of the method of storage in accordance with a state-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
c. Use state-approved methods to ensure secure deletion or destruction of student or workforce data (including originals, copies, and archived records).
d. Configure the MLDS to record the date student or workforce data is retrieved or updated and when the student or workforce data is to be deleted. .

8 General Controls

8.1 Information Integrity

8.1.1 Malicious Code

a. The MLDS Data Center shall:
   1) Employ malicious code protection mechanisms at MLDS entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
   2) Update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with MLDS Center configuration management policy and procedures;
   3) Configure malicious code protection mechanisms to:
      i. Perform monthly scans of the MLDS and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with MLDS Center security policy; and
      ii. Block malicious code, with notification to the user, in response to malicious code detection; and
   4) Centrally manage malicious code protection mechanisms.

b. The MLDS shall:
   1) Automatically update malicious code protection mechanisms (including signature definitions); and,
   2) Prevent non-privileged users from circumventing malicious code protection capabilities.

8.1.2 MLDS Monitoring

The MLDS Data Center shall monitor the MLDS to detect attacks and indicators of potential attacks.

8.1.3 Security Alerts, Advisories, and Directives

The MLDS Center shall:

a. Receive information system security alerts, advisories, and directives from designated external organizations (for example, Department of Information Technology (DoIT), regional, or national security organizations) on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to MLDS employees; and
d. Implement security directives in accordance with established time frames.

8.2 Security Awareness and Training Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented awareness and training procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the awareness and training policy and associated awareness and training controls.

8.2.1 Security Awareness

The MLDS Center shall ensure that all authorize users (to include MLDS Center employees, contractors) receive security awareness training within five business days of being employed by the MLDS Center, if he/she has not received awareness training within the past twelve months. Security awareness training shall be provided to all MLDS authorized users:

a. As part of initial training for new users;
b. When required by MLDS changes; and
c. At least annually thereafter.

8.2.2 Security Training

The MLDS Center shall provide role-based, security-related training to those MLDS Center employees who have significant security responsibilities relevant to the MLDS. This includes the MLDS Executive Director, Security Specialist, Network Administrator, Systems Administrator, Database Administrator (DBA), Programmer/Systems Analyst, Systems Designer/Systems Developer, and help desk personnel. The training shall be oriented to the individual's role and operational security responsibilities. This training shall be administered:

a. Before authorizing access to the MLDS or performing assigned duties;
b. When there are significant changes to the MLDS environment or procedures; and,
c. At least annually thereafter.

8.2.3 Security Training Records

The MLDS Center shall:

a. Document and monitor individual MLDS security training activities; and
b. Retain training records for a period of three (3) years.

8.3 System Security Assessment and Authorization

8.3.1 Security Assessments

a. The MLDS Center shall develop and employ a security assessment plan that describes the scope of the assessment, including:
    1) Security controls and control enhancements under assessment;

2) Assessment procedures to be used to determine security control effectiveness;
3) Assessment environment, assessment team, and assessment roles and responsibilities; and,
4) The results of all security assessments shall be documented in a security assessment report.

b. The MLDS Center shall include announced assessments as part of its security control assessments on an annual basis. These assessments may consist of, but are not limited to the following assessment types:
   1) In-depth monitoring;
   2) Malicious user testing;
   3) Penetration testing; and
   4) Red team exercises.

8.3.2 MLDS Connections

The MLDS Center shall:

a. Document MLDS connections through an Interconnection Security Agreement (ISA) and associated security requirements for each connection, the interface characteristics, security requirement, and the nature of the information communicated;
b. Monitor MLDS connections, verifying enforcement of security requirements.
c. Apply adequate countermeasures before connecting any equipment to the MLDS; and, ;
d. Establish any interconnections between MLDS and state agency and state institution systems providing data to the MLDS through controlled interfaces.

8.3.3 Plan of Action and Milestones – System Level

The MLDS Center shall:

a. Develop a Plan of Action and Milestones (POA&M) to document the planned remedial actions to correct weaknesses or deficiencies noted during the initial assessment of the security controls and when necessary, to reduce or eliminate known vulnerabilities in the system;
b. Update existing POA&Ms on an annual basis, at a minimum, based on the findings from security controls assessments, security impact analyses, and monitoring activities;

8.4 Configuration Management

8.4.1 Configuration Management Plan and Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented configuration management plan and change control procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and

b. Facilitates the implementation of configuration management and change control policy and associated configuration management controls.

8.4.2 Baseline Configuration

a. The MLDS Center shall develop, document, and maintain under configuration control, a current baseline configuration of the MLDS and associated software or hardware components, including communications and connectivity-related aspects of the systems. The baseline configuration shall:
   1) Provide information about the components of the MLDS and each component's technology (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with the current version numbers and patch information), network topology, and logical placement within the MLDS architecture.
   2) Use only legal and licensed (including open source, shareware, and freeware licenses, etc.) software (including operating system, databases, applications, etc.) shall be used or installed on MLDS. and,
b. The MLDS Center shall review and update the baseline configuration of the MLDS:
   1) When required due to significant changes to more than 25% of the baseline; and
   2) As an integral part of the MLDS component installations and upgrades.
c. The MLDS Center shall retain older versions of baseline configurations to support rollback.

8.4.3 Configuration Change Control

The MLDS Center shall:

a. Determine the types of changes to the MLDS that are configuration controlled;
b. Review proposed configuration controlled changes to the MLDS and approve;
c. Disapprove such changes with explicit consideration for security impact analyses;
d. Document approved configuration controlled changes to the MLDS;
e. Retain and review records of configuration controlled changes to the MLDS;
f. Audit activities associated with configuration controlled changes to the MLDS;
g. Coordinate and provide oversight for configuration change control activities through a configuration control board; and,
h. The MLDS Center shall test, validate, and document changes to the MLDS before implementing the changes in the production environment.

8.4.4 Configuration Settings

The MLDS Center shall, throughout the MLDS's lifecycle, and in accordance with MLDS security policies:

a. Establish and document mandatory baseline configuration settings for IT products employed in the MLDS using security configuration checklists (e.g., DISA Security

Technical Implementation Guide (STIG), NSA hardening guides, Center for Internet Security (CIS) security benchmark guides) that reflect the most restrictive mode consistent with operational requirements;

b. Implement and enforce the established configuration settings;
c. Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the MLDS based on explicit operational requirements; and,
d. Monitor and control changes to the configuration settings.

8.4.5 Least Functionality

a. The MLDS Center shall configure the MLDS to provide only essential capabilities and disable or remove any unnecessary or non-secure functions, ports, protocols, and/or services. The MLDS shall:
    1) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software on the MLDS; and
    2) Review and update the list of authorized software on a semi-annual basis.
b. The MLDS Center shall:
    1) Review the MLDS semi-annually to identify unnecessary and non-secure functions, ports, protocols, and services; and
    2) Disable functions, ports, protocols, and services within the MLDS deemed to be unnecessary or non-secure.

8.4.6 MLDS Component Inventory

a. The MLDS Center shall develop, document, and maintain an inventory of MLDS components that:
    1) Accurately reflects the MLDS;
    2) Is consistent with the authorization boundary of the MLDS;
    3) Is at a level of granularity deemed necessary for tracking and reporting, as requirements defined within this section for the MLDS components;
    4) Includes all MLDS-defined information deemed necessary to achieve effective property accountability; and
    5) Is available for review and audit by designated MLDS officials.
b. The MLDS Center shall maintain a current and updated inventory of MLDS components as an integral part of component installations, removals, and MLDS updates. The inventory management system shall include, at a minimum:
    a) Manufacturer
    b) Model Number
    c) Serial Number
    d) IP Address
    e) MLDS Barcode
    f) Hostname

g) Function
h) Software License number
i) Interconnections
j) System/Component Information
k) System/Component Owner

c. The MLDS Center shall:
   1) Employ automated mechanisms annually to detect the addition of unauthorized components/devices into the MLDS; and,
   2) Disable network access by such components/devices or notify designated MLDS personnel of unauthorized components/devices.
d. The MLDS Center shall include in property accountability information for the MLDS components, a means for identifying individuals (e.g. position, name and/or role), who are responsible for administering those components.
e. The MLDS Center shall verify that all components within the physical boundary of the MLDS are either inventoried as a part of the system or recognized by another system as a component within that system.

8.5 Contingency Planning

8.5.1 Contingency Planning Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented contingency planning procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of contingency planning policy and associated contingency planning controls.

8.5.2 MLDS Recovery and Reconstitution

The MLDS Center shall:

a. Provide for the recovery and reconstitution of the MLDS to a known state after any disruption, compromise, or failure;
b. Implement transaction recovery for systems that are transaction-based; and,
c. Provide compensating security controls for circumstances that can inhibit recovery and reconstitution to a known state/configuration.

8.5.3 Contingency Plan

The MLDS Center shall:

a. Develop and maintain a contingency plan that:
   1) Identifies essential functions and associated contingency requirements;

2) Provides recovery objectives, restoration priorities, and metrics;
3) Addresses contingency roles, responsibilities, assigned individuals with contact information;
4) Addresses eventual, full MLDS restoration without deterioration of the security measures originally planned and implemented; and
5) Is reviewed and approved by the MLDS Center Executive Director.

b. Plan for the resumption of essential functions as soon as feasible after contingency plan activation, and as defined within the MLDS recovery strategy.

8.5.4 Contingency Training, Plan Testing, and Exercises

a. All MLDS and MLDS Data Center personnel shall be trained in their roles and responsibilities in executing the contingency plan with respect to the MLDS and provided refresher training at least annually.
b. The MLDS Center shall:
   1) Test the contingency plan for the MLDS to determine the effectiveness of the plan and the MLDS Center's readiness to execute the plan;
   2) Review the contingency plan test results; and
   3) Initiate corrective actions.

8.5.5 Alternate Storage Site

The MLDS Center shall:

a. Establish an alternate storage site including necessary agreements to permit the storage and recovery of MLDS backup information;
b. Identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards; and,
c. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions, as required.

8.5.6 MLDS Backup

The MLDS Data Center shall:

a. Conduct backups of user-level information contained in the MLDS at least weekly;
b. Conduct backups of system-level information contained in the MLDS at least daily;
c. Conduct backups of MLDS documentation including security-related documentation at least monthly;
d. Protect the confidentiality and integrity of backup information at the storage location - The media shall be marked with the highest level of sensitivity;
e. Restrict access to backup media to authorized personnel only; and,
f. Test backup information to verify media reliability and information integrity at least semi-annually.

8.6 Incident Response

8.6.1 Incident Response Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented incident response procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the incident response policy and associated incident response controls.

8.6.2 Incident Response Training, Testing, and Exercises

The MLDS Center shall:

a. Train personnel in their incident response roles and responsibilities with respect to the MLDS;
b. Provide incident response refresher training at least annually; and,
c. Test and/or exercise the incident response capability for the MLDS at least annually to determine the incident response effectiveness and document the results.

8.6.3 Incident Handling

The MLDS Center shall:

a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinate incident handling activities with contingency planning activities;
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures and implements the procedures accordingly; and,
d. Employ automated mechanisms, when available, to support the incident handling process.

8.6.4 Incident Monitoring

The MLDS Center shall track and document MLDS security incidents.

8.6.5 Incident Reporting

The MLDS Center shall:

a. Require MLSD Center employees and contractor personnel to report suspected security incidents to the MLDS Center Information Security Officer within twenty-four hours;
b. Report security incident information to the Governing Board, the Maryland Department of Information Technology (DoIT), MSDE, DLLR, MHEC, and to law enforcement officials, if applicable; and,
c. Incorporate an automated capability to assist in reporting of security incidents.

8.6.6 Incident Response Assistance

The MLDS Center shall provide an incident response support resource (e.g., helpdesk or assistance group) to offer advice and assistance to MLDS Center staff for handling and reporting of security incidents.

8.6.7 Incident Response Plan

The MLDS Center shall:

a. Develop an incident response plan that:
   1) Provides the MLDS Center with a roadmap for implementing its incident response capability;
   2) Describes the structure of the incident response capability;
   3) Provides a high-level approach for how the incident response capability fits into the overall MLDS Center;
   4) Meets the unique requirements of the MLDS Center, which relate to its mission, size, structure, and functions;
   5) Defines reportable incidents;
   6) Provides metrics for measuring the incident response capability within the MLDS Center;
   7) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8) Is reviewed and approved by designated officials within the MLDS Center.
b. Distribute copies of the incident response plan to authorized MLDS Center incident response personnel and MLDS Center business units;
c. Review the incident response plan at a minimum on an annual basis;
d. Revise the incident response plan to address system and MLDS Center changes or problems encountered during plan implementation, execution, or testing; and
e. Communicate incident response plan changes to authorized MLDS Center incident response personnel and MLDS Center.

8.7 Maintenance

8.7.1 Maintenance Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented maintenance procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the maintenance policy and associated maintenance controls.

8.7.2 Controlled Maintenance

a. The MLDS Center shall:
   1) Schedule, perform, document, and review records of maintenance and repairs on MLDS components in accordance with manufacturer or vendor specifications and/or MLDS Center requirements;
   2) Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
   3) Require that a designated MLDS Center official explicitly approve the removal of any MLDS system components from the MLDS Center or the Data Center facilities for off-site maintenance or repair;
   4) Sanitize equipment to remove all information from associated media prior to removal from MLDS Center or Data Center facilities for off-site maintenance or repairs; and
   5) Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
b. The MLDS Center shall maintain maintenance records for the MLDS that include:
   1) Date and time of maintenance;
   2) Name of the individual performing the maintenance;
   3) Name of escort, if necessary;
   4) A description of the maintenance performed; and
   5) A list of equipment removed or replaced (including identification numbers, if applicable).

8.7.3 Maintenance Tools

The MLDS Center shall:

a. Approve, control, monitor the use of, information system maintenance tools;
b. Check all media containing diagnostic and test programs for malicious code before the media is used in the maintenance or troubleshooting of the MLDS; and,
c. Prevent the unauthorized removal of maintenance equipment by one of the following:
   1) Verifying that there is no MLDS Center or MLDS information contained on the equipment;
   2) Sanitizing or destroying the equipment;
   3) Retaining the equipment within the facility; or
   4) Obtaining an exemption from a designated a MLDS Center official explicitly authorizing removal of the equipment from the facility.

8.7.4 Non-Local Maintenance

The MLDS Center shall:

a. Authorize, monitor, and control non-local maintenance and diagnostic activities;

b. Allow the use of non-local maintenance and diagnostic tools only as necessary and when no other alternative is available;
c. Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
d. Maintain records for non-local maintenance and diagnostic activities;
e. Terminate all sessions, maintenance ports, and network connections when nonlocal maintenance is completed;
f. Audit non-local maintenance and diagnostic sessions. Designated MLDS Center personnel shall review the maintenance records of the sessions;
g. Document, in the security plan for the MLDS, the installation and use of non-local maintenance and diagnostic connections; and,
h. Require that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or
i. Remove the component to be serviced from the MLDS and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to MLDS Center information) before removal from MLDS Center or Data Center facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the MLDS.

8.7.5 Maintenance Personnel

The MLDS Center shall:

a. Establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel;
b. Ensure that personnel performing maintenance on the MLDS have required access authorizations or designate MLDS Center personnel with required access authorizations and technical competence deemed necessary to supervise MLDS maintenance when maintenance personnel do not possess the required access authorizations; and
c. Limit access to system software and hardware to authorized personnel.

8.7.6 Timely Maintenance

The MLDS Center shall obtain maintenance support and/or spare parts for failed MLDS components and/or key information technology components within a period consistent with recovery time objectives.

8.8 Media Protection

8.8.1 Media Protection Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented media protection procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of media protection and is consistent with the Maryland Department of Information Technology Information Security Policy, version 3.0, paragraph 6.5.

8.9 Physical and Environmental Protection

8.9.1 Physical and Environmental Protection Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented physical and environmental protection procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

8.9.2 Physical Access Authorizations

The MLDS Center shall:

a. Develop and keep current a list of personnel with authorized access to MLDS facilities where the MLDS and data reside (except for those areas within the facility officially designated as publicly accessible);
b. Issue authorization credentials (e.g., badges, identification cards, and smart cards); and,
c. Review and approve the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.

8.9.3 Physical Access Control

The MLDS Center and Data Center shall:

a. Enforce physical access authorization for all physical access points (including designated entry/exit points) to the facility where the MLDS resides (excluding those areas within the facility officially designated as publicly accessible);
b. Verify individual access authorizations before granting access to a facility;
c. Control entry to facilities containing the MLDS, using physical access devices and/or guards;
d. Secure keys, combinations, and other physical access devices;
e. Inventory physical access devices at a minimum annually;
f. Change combinations and keys at least annually and when keys are lost, combinations are compromised, or individuals who have access are transferred, terminated, or no longer require access;
g. Implement access controls for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times. Access controls shall be:

1) Based on the level of risk; and
2) Sufficient to safeguard assets against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

h. Enforce physical access authorization to the MLDS independent of the physical access controls for the facility in which it is located; and,
i. Ensure all physical access points to facilities where the MLDS resides is guarded and/or alarmed and monitored 24 hours per day, 7 days per week, commensurate with identified risk.

8.9.4 Access Control for Transmission Medium

The MLDS Center and Data Center shall ensure physical access to MLDS distribution and transmission lines is controlled.

8.9.5 Access Control for Output Devices

The MLDS Center and Data Center shall control physical access to the MLDS output devices (e.g., monitors, printers) to prevent unauthorized individuals from obtaining the output.

8.9.6 Monitoring Physical Access

The MLDS Center and Data Center shall ensure:

a. Physical access to the MLDS is monitored to detect and respond to physical security incidents;
b. Physical access logs are reviewed semi-annually; and,
c. Monitoring for real-time physical intrusion alarms and surveillance equipment.

8.9.7 Visitor Control

The MLDS Center and Data Center shall:

a. Ensure control of the physical access to the MLDS by authenticating visitors before authorizing access to the facility (e.g., access roster) where the MLDS resides other than areas designated as publicly accessible. Note: Escort access to a MLDS facility requires the non-MLDS personnel (e.g., visitor) to be accompanied by an authorized MLDS or DPSCS employee and their activity to be monitored within the facility. The escort shall have the escorted person(s) in view or be situated as such the escorted person(s) cannot leave the escorted area without being seen.
b. Ensure all visitors:
   1) Sign-in upon entering the facility;
   2) Be escorted; and
   3) Sign-out when exiting the facility.

8.9.8 Access Records

The MLDS Center & Data Center shall:

a. Maintain visitor access records/logs to facilities where the MLDS resides (except for those areas within the facility officially designated as publicly accessible). Access logs shall be reviewed by designated personnel at least monthly to identify and remedy suspicious activity; and,
b. Maintain a record of all physical access, both of visitors and authorized individuals.

8.9.9 Power Equipment and Power Cabling

The MLDS Data Center shall protect power equipment and power cabling for the MLDS from damage and destruction.

8.9.10 Emergency Shutoff

The MLDS Data Center shall:

a. Provide the capability of shutting off power to the MLDS or individual system components in emergency situations;
b. Place emergency shutoff switches or devices in a location near the MLDS or system components to facilitate safe and easy access for personnel; and
c. Protect emergency power shutoff capability from unauthorized activation.

8.9.11 Emergency Power

The MLDS Data Center shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the MLDS in the event of a primary power loss.

8.9.12 Emergency Lighting

The MLDS Center and Data Center shall employ and maintain an automatic emergency lighting system that activates in the event of a power outage or a disruption of emergency exit/evacuation route areas.

8.9.13 Fire Protection

a. The MLDS Data Center shall employ and maintain fire suppression and detection devices/systems (e.g., sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors) for the MLDS that are supported by an independent energy source.
b. The MLDS Center & Data Center shall ensure detection and suppression systems are automatically activated in the event of a fire and provide notification of the activation to emergency responders.
c. The MLDS Data Center shall employ an automatic fire suppression capability for the MLDS when the facility is not staffed on a continuous basis.

8.9.14 Temperature and Humidity Controls

The MLDS Data Center shall:

a. Maintain temperature and humidity levels within facilities where the MLDS resides at acceptable levels; and

b. Monitor temperature and humidity levels daily.

8.9.15 Water Damage Protection

The MLDS Data Center shall protect the MLDS from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

8.9.16 Delivery and Removal

The MLDS components, entering and exiting a facility, shall be controlled, recorded, maintained, and authorized by MLDS Center or Data Center personnel.

8.9.17 Alternate Work Site

The MLDS Center shall:

a. Employ management, operational, and technical information system security controls as defined within this policy at alternate work sites;
b. Assess the effectiveness of security controls at alternate work sites; and
c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.
d. Ensure that individuals within the MLDS Center employ appropriate information system security controls while at alternate work sites.

8.9.18 Location of MLDS Components

The MLDS Center and Data Center shall position MLDS components within the Data Center to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

8.10 Risk Assessment

8.10.1 Risk Assessment Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented risk assessment procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the risk assessment policy and associated risk assessment controls.

8.10.2 Risk Assessment

The MLDS Center shall:

a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the MLDS and the information it processes, stores, or transmits;
b. Document risk assessment results in system security plans and risk assessment plans;
c. Review risk assessment results at least annually; and
d. Update risk assessments at least every three (3) years or whenever there are significant changes to the MLDS or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the MLDS.

Note: Examples of significant changes to the MLDS that should have a technical risk assessment updated include, but are not limited to: (i) Installation of a new or upgraded operating system, middleware component, or application; (ii) Modifications to system ports, protocols, or services; (iii) Installation of a new or upgraded hardware platform or firmware component; or (iv) Modifications to cryptographic modules or services.

8.10.3 Vulnerability Scanning

The MLDS Data Center shall:

a. Scan for vulnerabilities in the MLDS and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1) Enumerating platforms, software flaws, and improper configurations;
    2) Formatting and making transparent, checklists and test procedures; and
    3) Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from security control assessments;
d. Remediate legitimate vulnerabilities;
e. Employ vulnerability scanning tools that include the capability to readily update the MLDS vulnerabilities to be scanned; and
f. Update the MLDS, if appropriate, when new vulnerabilities are identified and reported.

8.10.4 Rules of Behavior

The MLDS Center shall:

a. Establish and make available to all MLDS authorized users, the rules that describe their responsibilities and expected behavior with regard to information and MLDS usage; and,
b. Ensure all users sign a statement indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to information and the MLDS.

8.11 Security Program Management

8.11.1 Senior Information Security Officer

The MLDS Center Director shall appoint an information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

8.11.2 Information Security Resources

The MLDS Center Director shall ensure that information security resources are available for expenditure as planned.

8.11.3 Plan of Action and Milestones – Program Level

The MLDS Center shall implement a process for ensuring that plans of action and milestones for the security program and the MLDS are maintained and shall document the remedial information security actions to mitigate risk to MLDS Center operations, assets, and individuals.

8.11.4 MLDS Inventory

The MLDS Center shall develop and maintain an inventory of the MLDS hardware and software components.

8.11.5 Information Security Measures of Performance

The MLDS Center shall develop, monitor, and report on the results of information security measures of performance to the Governing Board on a semi-annual basis.

9 **Terms and Terminology** (Note: Not all terms below are used in this document)

Adult – an individual who is age 18 or older

Adult Education – same meaning as adult education and literacy activities - services or instruction below the postsecondary level for individuals--

a. who have attained 16 years of age;
b. who are not enrolled or required to be enrolled in secondary school under State law; and
c. who--
    (i) lack sufficient mastery of basic educational skills to enable the individuals to function effectively in society;
    (ii) do not have a secondary school diploma or its recognized equivalent, and have not achieved an equivalent level of education;
    (iii) are unable to speak, read, or write the English language.

Anonymization – The act of permanently and completely removing personal identifiers from data, such as converting personally identifiable information found within the student or workforce data into aggregated data. Anonymized data is data that can no longer be associated with an individual in any manner.

Apprentice – a worker 16 years old or older, who has entered into a voluntary written agreement with a sponsor who has agreed to teach the worker a skilled trade under terms defined in MD Regulations 2.04 and2.05.

Breach – an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.

Correctional Education Service – a continuum of structured education, workforce training, and transition services to incarcerated students that will prepare the student to enter Maryland's workforce

Data Governance – a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.

Data Steward – A person delegated the responsibility for managing a specific set of data resources (Authority: ISOIEC 11179)

Dates of attendance –

(a) The term means the period of time during which a student attends or attended an educational agency or institution. Examples of dates of attendance include an academic year, a spring semester, or a first quarter.

(b) The term does not include specific daily records of a student's attendance at an educational agency or institution. (Authority: 20 U.S.C. 1232g (a)(5)(A))

De-Identification – Involves the removal of personally identifying information in order to protect student or workers privacy. De-identified data may not necessarily be anonymized data, but may be data that can be re-associated with personally identifiable student or workforce data at a later time.

Direct Identifiers – Information that relates specifically to an individual, such as the individual's residence, including for example, name, address, social security number, or other identifying number or code, telephone number, or email address.

Disclosure – To permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record. (Authority: 20 U.S.C. 1232g(b)(1) and (b)(2))

Indirect Identifiers – Information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator and other descriptors.

Record – Any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche. (Authority: 20 U.S.C. 1232g)

State Assigned Student Identifier (SASID) – identifying information assigned to each student by a local education agency based on the identifier system developed by the State Department of Education or an institution of higher education, if the student has not been assigned an identifier by a local education agency

Sensitive data – Information or data that carries the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose student data, or workforce data was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains this data.

Student Data – data relating to student performance and includes: (i) State and national assessments; (ii) Course-taking and completion; (iii) Grade point average; (iv) Remediation; (v) Retention; (vi) Degree, diploma, or credential attainment; (vii) Enrollment; and (viii) Demographic data. **Student data does not include:** (i) Juvenile delinquency records; (ii)

Criminal and CINA records; (iii) Medical and health records; and (iv) Discipline records. (MD Education Article § 24-701)

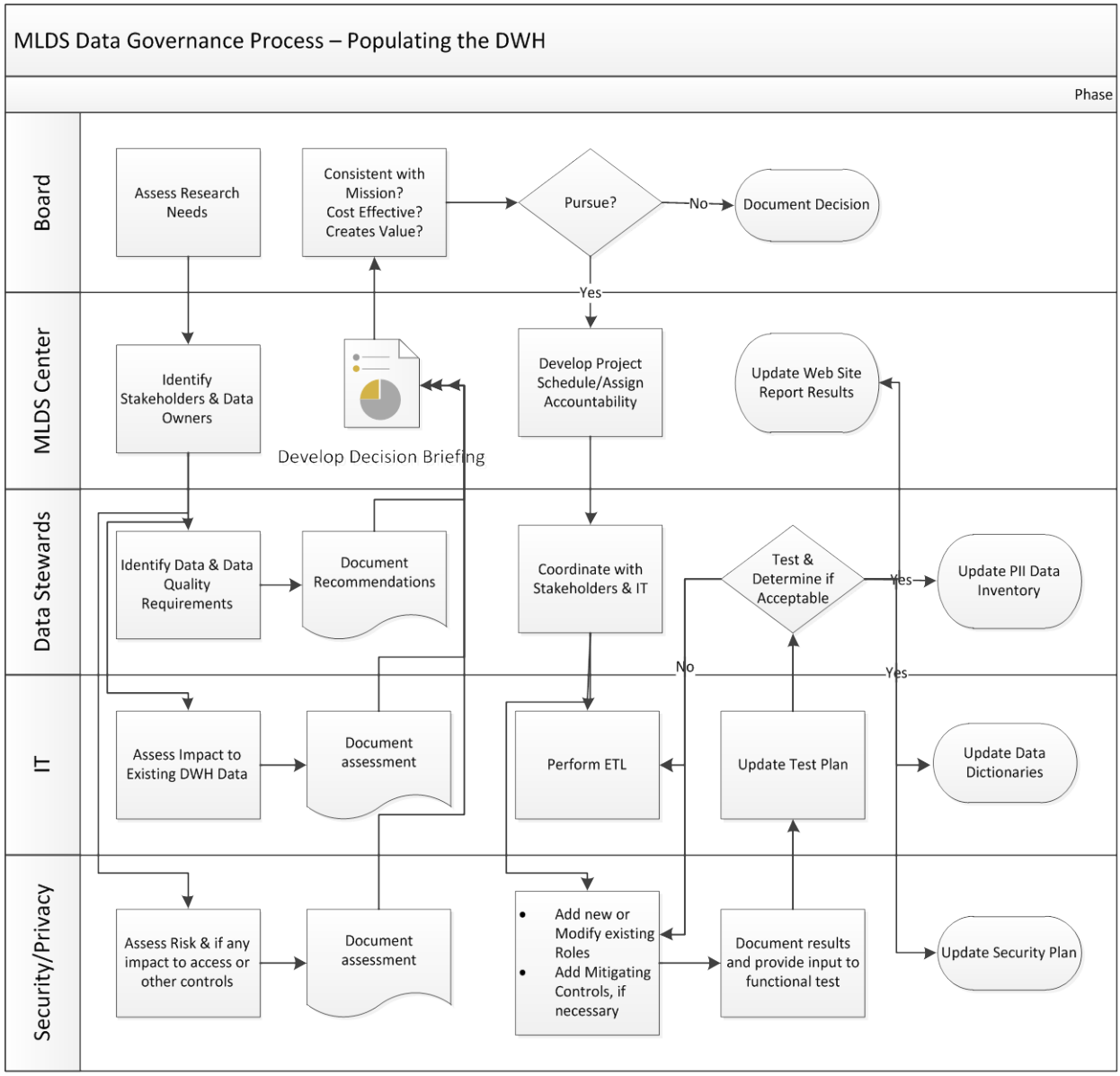
Workforce data -- data relating to: (1) Employment status; (2) Wage information; (3) Geographic location of employment; and (4) Employer information. (MD Education Article § 24-701)

10 Record of Revisions

Revision	Date	Section	Description
1.0	8/30/2012		Initial Draft

11 Background Information

11.1 Data Governance Workflow



Appendix C

MARYLAND STATE LONGITUDINAL DATA SYSTEM (MLDS)

DATA INVENTORY

VERSION 1

SEPTEMBER 1, 2012

Table of Contents

1. Overview
2. Scope, Limitations, and Updates
3. How to Use The MLDS Glossary
4. Data Contained in the Glossary
5. Data Naming Standards and Data Security
6. MLDS Online Data Glossary
7. Supporting Documents
8. For More Information
9. Change History
10. Appendices

1.0 Overview

The Maryland Longitudinal Data System (MLDS) is a data warehouse that blends select k12, higher education, and work force student data to analyze Maryland student trends in career and college readiness. This document meets state legislative requirements to make available to the Maryland State Longitudinal Data Governance Board, and the general public, information about the contents of the MLDS database.

2.0 Scope, Limitations, and Updates

The scope of the data in the MLDS data warehouse is limited by the policy questions it is designed to answer. The glossary will be updated as new data sets that answer additional policy questions are added to the data warehouse. The database contains both aggregate data sets and de-identified, encrypted student and work force data. Data associated with an individual is not available for viewing in the MLDS database and work force related data is only retained for five years after an individual leaves school. Computed fields that are displayed on reports or in business analytics are not included in the data glossary.

The MLDS data warehouse data glossary document is maintained manually. A PDF version of his document will be maintained for public distribution and will be made available on the MLDS portal. The data glossary is also available as an online lookup system. The online lookup system also provides a data element definition download capability. The online data glossary is described in Section 4.

3.0 How to Use the MLDS Glossary

This glossary can help the reader understand how the data warehouse data is organized, and lists the specific data elements it contains. This information is useful for planning research, defining informational reports, or planning various trend analyses.

In addition to looking up data elements in the data warehouse, this document shows how data elements are conceptually grouped into data domains and data entities. All data elements are grouped into CEDS various data entities that show how a group of data elements relate to a single concept such as student, school, or teacher. Data entities are then grouped into CEDS data domains such as early childhood, secondary education, or higher education.

Appendix B lists the data domains and data entities used to describe and group data elements in the MLDS data warehouse. Appendix C lists the MLDS entities and associated data elements with their definitions in the current MLDS database.

The online data glossary lists over 500 educational terms and definitions related to the state longitudinal data system, CEDS, and IPEDS data standards.

4.0 Data Contained in the Glossary

Version 1 of the database, as described in this document, contains those data sets that answer the following policy questions;

- Policy Question 2: What percentage of Maryland high school exiters go on to be enrolled in Maryland postsecondary education?
- Policy Question 3: What percentage of Maryland high school exiters entering college are assessed to need to take developmental courses and in what areas?
- Policy Question 11: Which 4-year institutions are graduating students most effectively and in the timeliest fashion?

As new data sets are added to the data warehouse to answer additional policy questions, this section will be updated.

The glossary may contain the following data for each data element;

- Domain
- Entity
- Agency/System Owner
- Data Standard
- Application
- Term Description
- Data Type
- Format
- Metric Description
- Technical Name
- Computed Field Flag
- Term Encryption Flag
- Term Masking Flag
- Usage Notes
- Disaggregation Rules
- Record Status
- Policy Question Flags

5.0 Data Naming Standards and Data Security

For security reasons, the native database data element names in the MLDS database are not listed in the glossary. Instead, the native database element names are mapped to the U.S Department of Education's Common Education Data Standard (CEDS) which is used as an alternative naming standard for the reader. Where CEDS does not provide a data element name for the native database element, other standards such as IPEDS, NCES Online Handbook, or the National Education Data Model are used. If no data naming standard is available to map to, the native data element name in the database is listed for the reader. Authorized researchers and policy analysts are able to view all database tables, schemas, and data element column names with the exception of the individual ID and personal information crosswalk tables.

6.0 MLDS Online Data Glossary

Version 1 of the MLDS Online Data Glossary is password protected on the MLDS portal. The secure data entry form allows the data administrator to enter data elements from the MLDS database with a variety of its descriptors such and its entity, domain, definition, security level, application it is associated

with and the standardized data name. The system will also support batch data loads of data elements. The online lookup system enables users to view the data elements in the database in a variety of ways, and allows users to download either a portion or the entire data glossary as a PDF file or a Microsoft Excel file.

Information on accessing and using the online data glossary dashboard is posted on the secure MLDS portal. Screen images of the glossary data entry and online lookup interfaces are shown in Appendix A.

7.0 Supporting Documents

Please refer to any of the following documents for additional support on the MLDS Data Glossary:

- **CEDS 2.0 Data Standard**
  - https://ceds.ed.gov/
- **IPEDS Data Standard**
  - http://nces.ed.gov/ipeds/
- **Common Core Data Standards**
  - http://nces.ed.gov/ccd/index.asp
- **National Education Data Model**
  - http://nces.ed.gov/forum/datamodel/

8.0 For More Information

For more information about this document, the online data glossary, and the MLDS data warehouse please fill-out the online Contact Us form on the MLDS portal that can be access at http://p12lds.msde.state.md.us/portal/page/portal/P20_MLDS/MLDS_CENTER

9.0 Change History

Date	Description/Reason for change	Authors/Contributors	Version
07/25/12	Initial Draft	John Bruns	1
09/1/12	Revision of content, addition of tables	John Bruns, Rob London	1

10.0 Appendices

- Appendix A - Screen Images of MLDS Online Data Glossary
- Appendix B - Domains and Entities
- Appendix C – Data Elements, Entities, and Definitions
- Appendix D – Data Elements for Policy Questions 2, 3, and 11
- Appendix E – List of Terms

Appendix A - Screen Images of MLDS Online Data Glossary

Figure 1: MLDS Data Element Entry Form for the Data Glossary

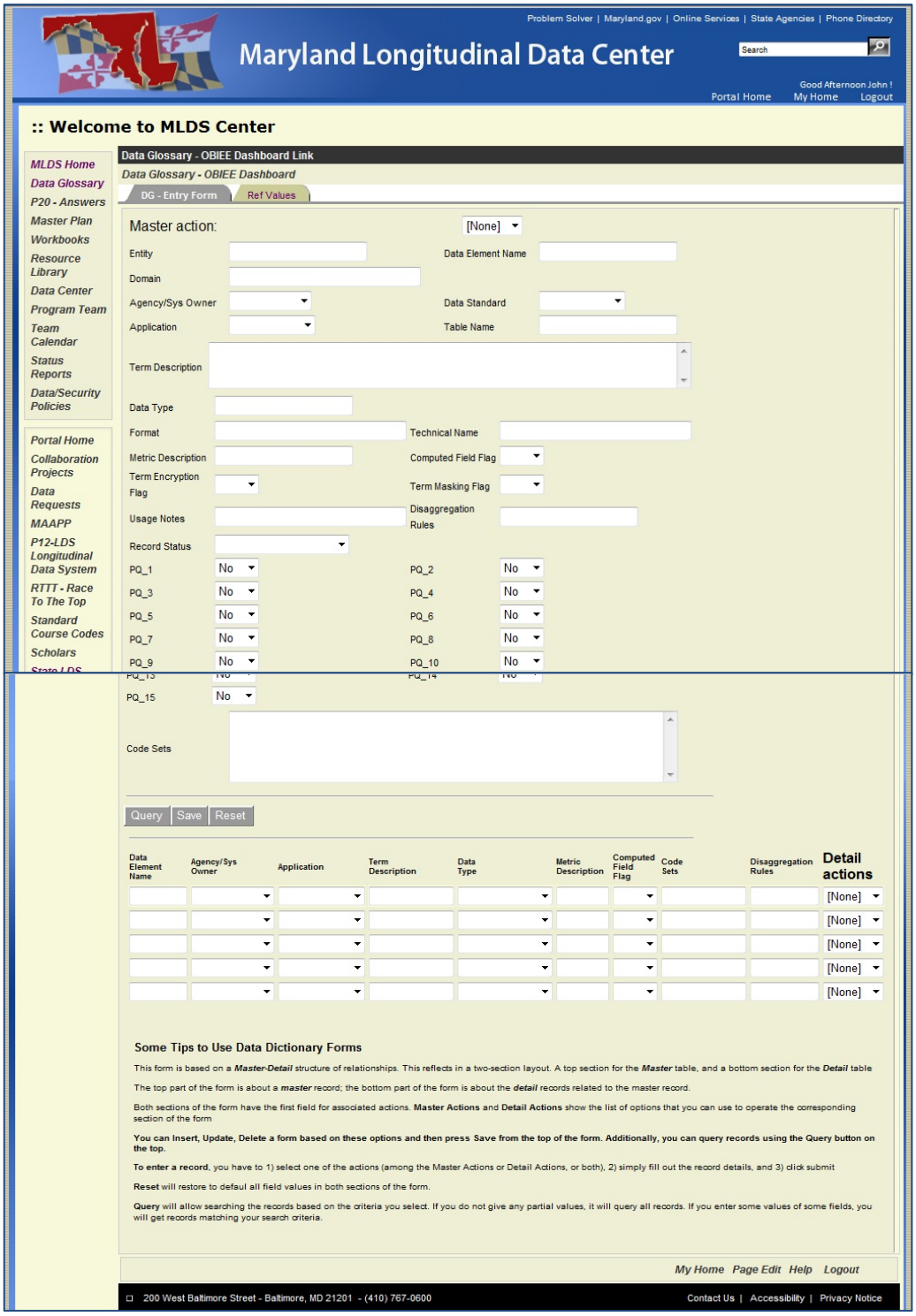


Figure 2: Data Glossary Dashboard Overview

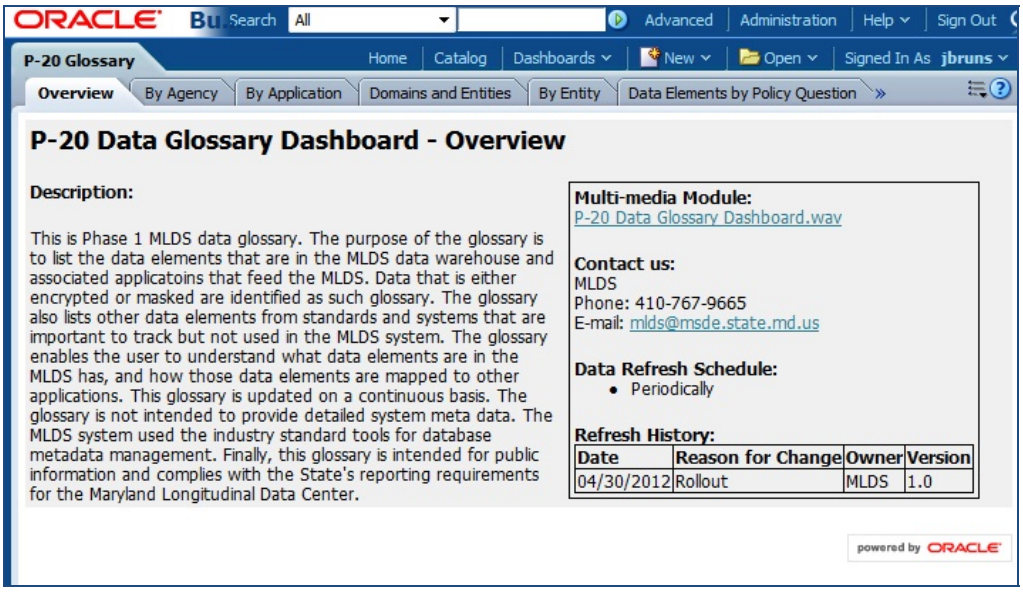
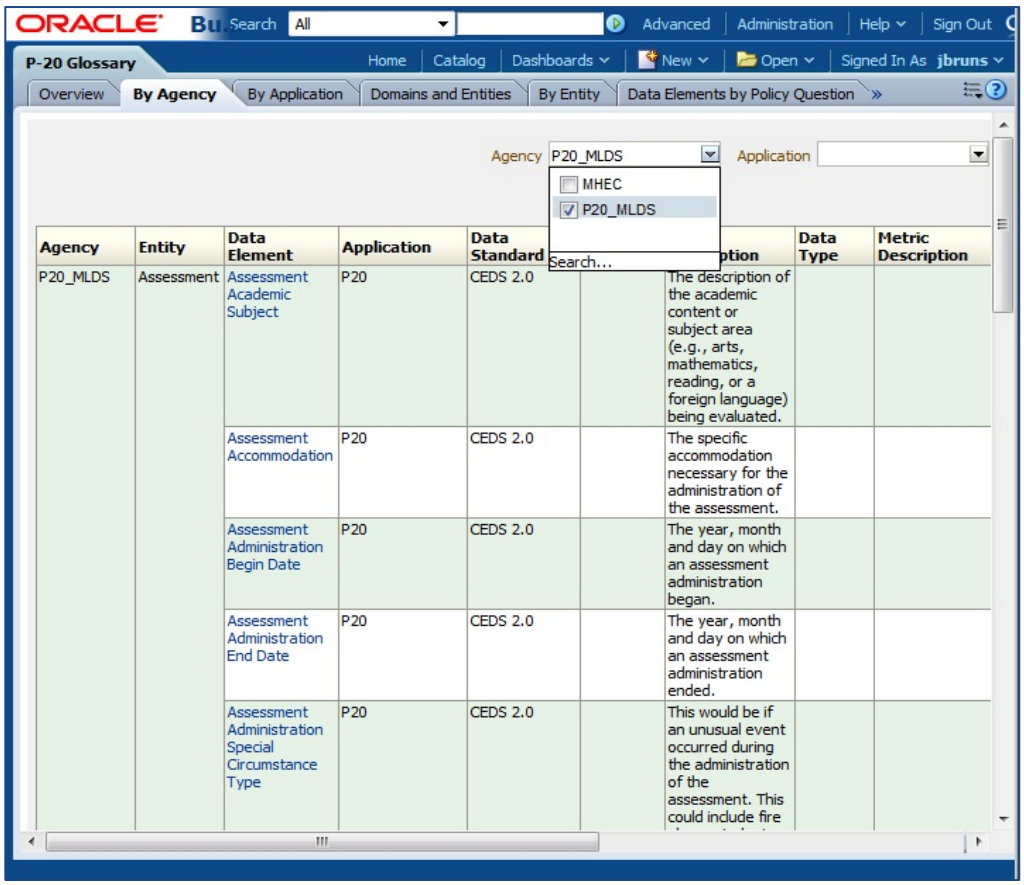


Figure 3: Data Glossary Dashboard "By Agency" Tab



Appendix B – Domains and Entities

Domain	Entity
Assessments	Assessment
	Assessment Administration
	Assessment Form
	Assessment Item
	Assessment Item Response
	Assessment Section
	Assessment Subtest
	Learning Standards Item
	Performance Level
	Student Assessment Registration
	Student Score
Early Learning	EL Child
	EL Family
	EL Organization
	EL Staff
	Parent/Guardian
K12	Assessment
	Calendar
	Incident
	K12 Course
	K12 School
	K12 Section
	K12 Staff
	K12 Student
	LEA
	Parent/Guardian
	Program
	SEA
	K12 Student
Learning Standards	Learning Standard Document
	Learning Standard Item
Postsecondary	PS Institution
	PS Section
	PS Student

Appendix C – Data Elements, Entities, and Record Status

Element Name	Entity	Record Status
Ability Grouping Status	K12 School	Reserved
Absent Attendance Category	K12 Student	Reserved
Academic Award Date	PS Student	Reserved
Academic Award Level Conferred	PS Student	Reserved
Academic Award Title	PS Student	Reserved
Academic Honors Type	K12 Student	Reserved
Accountability Report Title	LEA	Reserved
ACT Composite Score	PS Student	Active
ACT English Score	PS Student	Active
ACT Math Score	PS Student	Active
ACT Reading Score	PS Student	Active
ACT Science Score	PS Student	Active
Activity Identifier	K12 Student	Reserved
Activity Involvement Begin Date	K12 Student	Reserved
Activity Involvement End Date	K12 Student	Reserved
Activity Title	K12 Student	Reserved
Additional Credit Type Awarded	K12 Course	Reserved
Address Apartment Room or Suite Number	EL Child	Reserved
Address Apartment Room or Suite Number	EL Organization	Reserved
Address Apartment Room or Suite Number	EL Staff	Reserved
Address Apartment Room or Suite Number	K12 Staff	Reserved
Address Apartment Room or Suite Number	K12 Student	Reserved
Address Apartment Room or Suite Number	PS Student	Reserved
Address City	EL Child	Reserved
Address City	EL Organization	Reserved
Address City	EL Staff	Reserved
Address City	K12 Staff	Reserved
Address City	K12 Student	Reserved
Address City	LEA	Reserved
Address City	PS Student	Reserved
Address City	SEA	Reserved
Address City	K12 School	Active
Address County Name	EL Child	Reserved
Address County Name	EL Organization	Reserved
Address County Name	EL Staff	Reserved
Address County Name	K12 School	Active
Address County Name	K12 Student	Active

Element Name	Entity	Record Status
Address County Name	LEA	Reserved
Address County Name	PS Student	Reserved
Address Postal Code	EL Child	Reserved
Address Postal Code	EL Organization	Reserved
Address Postal Code	EL Staff	Reserved
Address Postal Code	K12 Staff	Reserved
Address Postal Code	K12 Student	Reserved
Address Postal Code	LEA	Reserved
Address Postal Code	PS Student	Active
Address Postal Code	SEA	Reserved
Address Postal Code	K12 School	Active
Address Street Number and Name	EL Child	Reserved
Address Street Number and Name	EL Organization	Reserved
Address Street Number and Name	EL Staff	Reserved
Address Street Number and Name	K12 Staff	Reserved
Address Street Number and Name	K12 Student	Reserved
Address Street Number and Name	LEA	Reserved
Address Street Number and Name	PS Student	Reserved
Address Street Number and Name	SEA	Reserved
Address Street Number and Name	K12 School	Active
Address Type for Learner	EL Child	Reserved
Address Type for Learner	K12 Student	Reserved
Address Type for Learner	PS Student	Reserved
Address Type for Organization	EL Organization	Reserved
Address Type for Organization	K12 School	Reserved
Address Type for Organization	LEA	Reserved
Address Type for Organization	SEA	Reserved
Address Type for Staff	K12 Staff	Reserved
Adequate Yearly Progress Appeal Changed Designation	K12 School	Reserved
Adequate Yearly Progress Appeal Changed Designation	LEA	Reserved
Adequate Yearly Progress Appeal Process Date	K12 School	Reserved
Adequate Yearly Progress Appeal Process Date	LEA	Reserved
Adequate Yearly Progress Status	LEA	Reserved
Adequate Yearly Progress Status	SEA	Reserved
Adequate Yearly Progress Status	K12 School	Active
Administrative Funding Control	K12 School	Reserved
Admission Exemption	PS Student	Active
Advanced Placement Course Self Selection	K12 School	Reserved
Advanced Placement Credits Awarded	PS Student	Reserved

Element Name	Entity	Record Status
Agency Type	LEA	Reserved
Ages Served	EL Organization	Reserved
Aligned with State Standards	K12 Course	Reserved
Aligned with State Standards	K12 Section	Reserved
Alternate Adequate Yearly Progress Approach Indicator	K12 School	Reserved
Alternate Adequate Yearly Progress Approach Indicator	LEA	Reserved
Alternate Day Name	Calendar	Reserved
Alternative School Focus Type	K12 School	Reserved
American Indian or Alaska Native	EL Child	Reserved
American Indian or Alaska Native	K12 Staff	Reserved
American Indian or Alaska Native	K12 Student	Active
American Indian or Alaska Native	PS Student	Active
American Indian or Alaska Native	K12 Student	Active
Annual Measurable Achievement Objective AYP Progress Attainment Status for LEP Students	LEA	Reserved
Annual Measurable Achievement Objective AYP Progress Attainment Status for LEP Students	SEA	Reserved
Annual Measurable Achievement Objective Proficiency Attainment Status for LEP Students	K12 School	Reserved
Annual Measurable Achievement Objective Proficiency Attainment Status for LEP Students	LEA	Reserved
Annual Measurable Achievement Objective Proficiency Attainment Status for LEP Students	SEA	Reserved
Annual Measurable Achievement Objective Progress Attainment Status for LEP Students	K12 School	Reserved
Annual Measurable Achievement Objective Progress Attainment Status for LEP Students	LEA	Reserved
Annual Measurable Achievement Objective Progress Attainment Status for LEP Students	SEA	Reserved
Appealed Adequate Yearly Progress Designation	K12 School	Reserved
Appealed Adequate Yearly Progress Designation	LEA	Reserved
Application Date	EL Child	Reserved
Asian	EL Child	Reserved
Asian	K12 Student	Active
Asian	K12 Student	Active
Asian	PS Student	Active
Assessment Academic Subject	Assessment	Reserved
Assessment Academic Subject	Assessment Subtest	Reserved
Assessment Academic Subject	K12 Student	Reserved
Assessment Accommodation	Assessment	Reserved
Assessment Accommodation	Assessment Administration	Reserved

Element Name	Entity	Record Status
Assessment Accommodation	K12 Student	Reserved
Assessment Accommodation	Student Assessment Registration	Reserved
Assessment Accommodation Type	K12 Student	Reserved
Assessment Accommodation Type	Student Assessment Registration	Reserved
Assessment Administration Begin Date	Assessment	Reserved
Assessment Administration Begin Date	Assessment Administration	Reserved
Assessment Administration Begin Date	K12 Student	Reserved
Assessment Administration End Date	Assessment	Reserved
Assessment Administration End Date	Assessment Administration	Reserved
Assessment Administration End Date	K12 Student	Reserved
Assessment Administration Special Circumstance Type	Assessment	Reserved
Assessment Administration Special Circumstance Type	Assessment Administration	Reserved
Assessment Administrator Identifier	Assessment	Reserved
Assessment Administrator Identifier	Assessment Administration	Reserved
Assessment Allotted Time	Assessment	Reserved
Assessment Allotted Time	Assessment Administration	Reserved
Assessment Content Standard Type	Assessment	Reserved
Assessment Content Standard Type	Assessment Subtest	Reserved
Assessment Feedback	K12 Student	Reserved
Assessment Feedback	Student Score	Reserved
Assessment Form Name	Assessment	Reserved
Assessment Form Name	Assessment Form	Reserved
Assessment Form Name	K12 Student	Reserved
Assessment Form Number	Assessment	Reserved
Assessment Form Number	Assessment Form	Reserved
Assessment Form Number	K12 Student	Reserved
Assessment Identifier	Assessment	Reserved
Assessment Identifier	Assessment	Reserved
Assessment Identifier	K12 Student	Reserved
Assessment Item Aid Set Used	Assessment	Reserved
Assessment Item Aid Set Used	Assessment Item Response	Reserved
Assessment Item Allotted Time	Assessment	Reserved

Element Name	Entity	Record Status
Assessment Item Allotted Time	Assessment Item	Reserved
Assessment Item Characteristic Type	Assessment	Reserved
Assessment Item Characteristic Type	Assessment Item	Reserved
Assessment Item Characteristic Value	Assessment	Reserved
Assessment Item Characteristic Value	Assessment Item	Reserved
Assessment Item Correct Response	Assessment	Reserved
Assessment Item Correct Response	Assessment Item	Reserved
Assessment Item Difficulty	Assessment	Reserved
Assessment Item Difficulty	Assessment Item	Reserved
Assessment Item Distractor Analysis	Assessment	Reserved
Assessment Item Distractor Analysis	Assessment Item	Reserved
Assessment Item Identifier	Assessment	Reserved
Assessment Item Identifier	Assessment Item	Reserved
Assessment Item Maximum Score	Assessment	Reserved
Assessment Item Maximum Score	Assessment Item	Reserved
Assessment Item Minimum Score	Assessment	Reserved
Assessment Item Minimum Score	Assessment Item	Reserved
Assessment Item Response Choice Pattern	Assessment	Reserved
Assessment Item Response Choice Pattern	Assessment Item	Reserved
Assessment Item Response Time	Assessment	Reserved
Assessment Item Response Time	Assessment Item Response	Reserved
Assessment Item Score Value	Assessment Item Response	Reserved
Assessment Item Stem	Assessment	Reserved
Assessment Item Stem	Assessment Item	Reserved
Assessment Item Type	Assessment	Reserved
Assessment Item Type	Assessment Item	Reserved
Assessment Language	Assessment	Reserved
Assessment Language	Assessment Administration	Reserved
Assessment Level for which Designed	Assessment	Reserved
Assessment Level for which Designed	Assessment	Reserved
Assessment Level for which Designed	K12 Student	Reserved
Assessment Location	Assessment	Reserved
Assessment Location	Assessment Administration	Reserved
Assessment Number of Items	Assessment	Reserved
Assessment Number of Items	Assessment Section	Reserved
Assessment Objective	Assessment	Reserved

Element Name	Entity	Record Status
Assessment Objective	Assessment	Reserved
Assessment Participation Indicator	Assessment Administration	Reserved
Assessment Participation Indicator	K12 Student	Reserved
Assessment Performance Level Identifier	Assessment	Reserved
Assessment Performance Level Identifier	Performance Level	Reserved
Assessment Performance Level Maximum Cut Score	Assessment	Reserved
Assessment Performance Level Maximum Cut Score	Assessment	Reserved
Assessment Performance Level Maximum Cut Score	Performance Level	Reserved
Assessment Performance Level Minimum Cut Score	Assessment	Reserved
Assessment Performance Level Minimum Cut Score	Assessment	Reserved
Assessment Performance Level Minimum Cut Score	Performance Level	Reserved
Assessment Performance Level Name	Assessment	Reserved
Assessment Performance Level Name	K12 Student	Reserved
Assessment Performance Level Name	Performance Level	Reserved
Assessment Performance Level Name	Student Score	Reserved
Assessment Performance Level Score Metric	Assessment	Reserved
Assessment Performance Level Score Metric	Assessment	Reserved
Assessment Performance Level Score Metric	Performance Level	Reserved
Assessment Performance Level Short Name	Assessment	Reserved
Assessment Performance Level Short Name	Performance Level	Reserved
Assessment Platform	Assessment	Reserved
Assessment Platform	Assessment Administration	Reserved
Assessment Proctor Identifier	Assessment	Reserved
Assessment Proctor Identifier	Assessment Administration	Reserved
Assessment Purpose	Assessment	Reserved
Assessment Purpose	Assessment Subtest	Reserved
Assessment Purpose	K12 Student	Reserved
Assessment Reason for Not Completing	K12 Student	Reserved
Assessment Reason for Not Completing	Student Assessment Registration	Reserved
Assessment Reporting Method	Assessment Administration	Reserved
Assessment Reporting Method	K12 Student	Reserved
Assessment Rubric Identifier	Assessment	Reserved
Assessment Rubric Identifier	Assessment Item	Reserved
Assessment Rubric Name	Assessment	Reserved
Assessment Rubric Name	Assessment Item	Reserved

Element Name	Entity	Record Status
Assessment Rubric Reference	Assessment	Reserved
Assessment Rubric Reference	Assessment Item	Reserved
Assessment Score Metric Type	Assessment	Reserved
Assessment Score Metric Type	Assessment Subtest	Reserved
Assessment Score Results	K12 Student	Reserved
Assessment Score Results	Student Score	Reserved
Assessment Score Scale Maximum Value	Assessment	Reserved
Assessment Score Scale Maximum Value	Assessment Subtest	Reserved
Assessment Score Scale Minimum Value	Assessment	Reserved
Assessment Score Scale Minimum Value	Assessment Subtest	Reserved
Assessment Score Scale Optimal Value	Assessment	Reserved
Assessment Score Scale Optimal Value	Assessment Subtest	Reserved
Assessment Score Scale Value	Assessment Subtest	Reserved
Assessment Score Scale Value	K12 Student	Reserved
Assessment Secure Indicator	Assessment	Reserved
Assessment Secure Indicator	Assessment Administration	Reserved
Assessment Subtest Abbreviation	Assessment	Reserved
Assessment Subtest Abbreviation	Assessment Subtest	Reserved
Assessment Subtest Description	Assessment	Reserved
Assessment Subtest Description	Assessment Subtest	Reserved
Assessment Subtest Description	K12 Student	Reserved
Assessment Subtest Identifier	Assessment	Reserved
Assessment Subtest Identifier	Assessment Subtest	Reserved
Assessment Subtest Name	Assessment	Reserved
Assessment Subtest Name	Assessment Subtest	Reserved
Assessment Subtest Name	K12 Student	Reserved
Assessment Subtest Rules	Assessment	Reserved
Assessment Subtest Rules	Assessment Subtest	Reserved
Assessment Subtest Score Value	Student Score	Reserved
Assessment Subtest Title	Assessment	Reserved
Assessment Subtest Title	Assessment Subtest	Reserved
Assessment Subtest Version	Assessment	Reserved
Assessment Subtest Version	Assessment Subtest	Reserved
Assessment Time	Assessment Administration	Reserved
Assessment Time	K12 Student	Reserved
Assessment Title	Assessment	Reserved
Assessment Title	Assessment	Reserved
Assessment Title	K12 Student	Reserved

Element Name	Entity	Record Status
Assessment Type	Assessment	Reserved
Assessment Type	Assessment	Reserved
Assessment Type Administered to Children With Disabilities	Assessment	Reserved
Assignment End Date	K12 Section	Reserved
Assignment End Date	K12 Staff	Reserved
Assignment Start Date	K12 Section	Reserved
Assignment Start Date	K12 Staff	Reserved
Attendance Event Type	K12 Student	Reserved
Available Carnegie Unit Credit	K12 Course	Reserved
Available Carnegie Unit Credit	K12 Section	Reserved
Awaiting Initial IDEA Evaluation Status	K12 Student	Reserved
Barrier to Educating Homeless	LEA	Reserved
Base Salary	K12 Staff	Reserved
Birthdate	EL Child	Reserved
Birthdate	EL Staff	Reserved
Birthdate	K12 Staff	Reserved
Birthdate	PS Student	Active
Birthdate	K12 Student	Active
Birthdate Verification	K12 Student	Reserved
Black or African American	EL Child	Reserved
Black or African American	K12 Staff	Reserved
Black or African American	K12 Student	Active
Black or African American	PS Student	Active
Building Site Number	K12 School	Reserved
Calendar Code	Calendar	Reserved
Calendar Description	Calendar	Reserved
Calendar End Date	PS Calendar	Active
Calendar Event Type	Calendar	Reserved
Calendar Start Date	PS Calendar	Active
Campus Residency Type	PS Student	Reserved
Career and Technical Education Completer	K12 Student	Active
Career and Technical Education Concentrator	K12 Student	Active
Career and Technical Education Displaced Homemaker Indicator	K12 Student	Reserved
Career and Technical Education Graduation Rate Inclusion	SEA	Reserved
Career and Technical Education Participant	K12 Student	Reserved
Career and Technical Education Student Preparing for Nontraditional Fields	K12 Student	Reserved
Career Technical Education Representation Status	K12 School	Reserved

Element Name	Entity	Record Status
Carnegie Basic Classification	PS Institution	Reserved
Charter School Indicator	K12 School	Reserved
Charter School Indicator	LEA	Reserved
Charter School Type	K12 School	Reserved
Child-to-Instructional Staff Ratio	EL Organization	Reserved
City of Birth	K12 Student	Reserved
Class Beginning Time	K12 Section	Reserved
Class Ending Time	K12 Section	Reserved
Class Meeting Days	K12 Section	Reserved
Class Period	K12 Section	Reserved
Class Ranking Date	K12 Student	Reserved
Class Section Entry Type	K12 Section	Reserved
Class Section Exit Type	K12 Section	Reserved
Class Section Exit Withdrawal Date	K12 Section	Reserved
Classification of Instructional Program Code	PS Student	Reserved
Classification of Instructional Program Use	PS Student	Reserved
Classification of Instructional Program Version	PS Student	Reserved
Classroom Identifier	K12 Section	Reserved
Classroom Position Type	K12 Staff	Reserved
Cohort Description	K12 Student	Reserved
Cohort Exclusion	PS Student	Reserved
Cohort Graduation Year	K12 Student	Active
Cohort Year	K12 Student	Active
Cohort Year	PS Student	Active
Collection Year	PS Student	Active
Consolidated Migrant Education Program Funds Status	K12 School	Reserved
Continuation of Services Reason	K12 Student	Reserved
Continuation of Services Status	K12 Student	Reserved
Continuing License Date	EL Organization	Reserved
Contract Days of Service per Year	K12 Staff	Reserved
Control of Institution	PS Institution	Active
Core Academic Course	K12 Course	Reserved
Corrective Action Type	K12 School	Reserved
Country Code	EL Child	Reserved
Country Code	EL Staff	Reserved
Country Code	K12 Student	Reserved
Country Code	PS Student	Reserved
Country of Birth Code	K12 Student	Reserved
County Federal Information Processing Standards Code	K12 School	Reserved

Element Name	Entity	Record Status
County Federal Information Processing Standards Code	LEA	Reserved
County Federal Information Processing Standards Code	PS Student	Active
Course Academic Grade	PS Section	Active
Course Begin Date	PS Section	Reserved
Course Code System	K12 Course	Reserved
Course Code System	K12 Section	Reserved
Course Code System	K12 Student	Reserved
Course Credit Units	PS Section	Reserved
Course Credit Value	PS Section	Reserved
Course Description	K12 Course	Reserved
Course End Date	PS Section	Reserved
Course Grade Point Average Applicability	K12 Course	Reserved
Course Grade Point Average Applicability	K12 Section	Reserved
Course Identifier	K12 Course	Reserved
Course Identifier	K12 Section	Reserved
Course Identifier	K12 Student	Reserved
Course Identifier	PS Section	Reserved
Course Level Characteristic	K12 Course	Active
Course Level Characteristic	K12 Section	Reserved
Course Level Characteristic	PS Section	Reserved
Course Override School	PS Section	Reserved
Course Quality Points Earned	PS Section	Reserved
Course Repeat Code	K12 Student	Reserved
Course Subject Abbreviation	PS Section	Reserved
Course Title	K12 Course	Reserved
Course Title	K12 Section	Reserved
Course Title	K12 Student	Reserved
Credential Expiration Date	K12 Staff	Reserved
Credential Issuance Date	K12 Staff	Reserved
Credential Type	K12 Staff	Reserved
Credit Type Earned	K12 Section	Reserved
Credit Type Earned	K12 Student	Active
Credits Attempted Cumulative	K12 Student	Reserved
Credits Earned Cumulative	K12 Student	Reserved
Crisis Code	Calendar	Reserved
Crisis Name	Calendar	Reserved
Crisis Start Date	Calendar	Reserved
Crisis Type	Calendar	Reserved
Cumulative GPA	PS Student	Active

Element Name	Entity	Record Status
Curriculum Framework Type	K12 Course	Reserved
Custodial Parent or Guardian Indicator	Parent/Guardian	Reserved
Daily Attendance Status	K12 Student	Reserved
Date State Received Title III Allocation	SEA	Reserved
Date Title III Funds Available to Subgrantees	SEA	Reserved
Days Available Per Week	EL Organization	Reserved
Days In Session	K12 School	Reserved
Degree Applicability	PS Section	Reserved
Degree or Certificate Conferring Date	EL Staff	Reserved
Degree or Certificate Seeking Student	PS Student	Reserved
Degree or Certificate Title or Subject	EL Staff	Reserved
Degree or Certificate Type	EL Staff	Reserved
Dental Insurance Coverage	EL Child	Reserved
Dental Screening	EL Child	Reserved
Dental Screening Date	EL Child	Reserved
Dependency Status	PS Student	Reserved
Desegregation Order or Plan	LEA	Reserved
Designated Graduation School Identifier	K12 Student	Reserved
Developmental Evaluation Finding	EL Child	Reserved
Developmental Screening	EL Child	Reserved
Diploma or Credential Award Date	K12 Student	Active
Diploma or Credential Award Date	PS Student	Reserved
Disability Status	K12 Student	Active
Disciplinary Action	Incident	Reserved
Disciplinary Action	K12 Student	Reserved
Disciplinary Action End Date	Incident	Reserved
Disciplinary Action End Date	K12 Student	Reserved
Disciplinary Action Start Date	Incident	Reserved
Disciplinary Action Start Date	K12 Student	Reserved
Discipline Action Length Difference Reason	Incident	Reserved
Discipline Action Length Difference Reason	K12 Student	Reserved
Discipline Method for Firearms Incidents	Incident	Reserved
Discipline Method for Firearms Incidents	K12 Student	Reserved
Discipline Method of Children with Disabilities	K12 Student	Reserved
Discipline Reason	Incident	Reserved
Discipline Reason	K12 Student	Reserved
Displaced Student Status	K12 Student	Reserved
Dual Credit Dual Enrollment Credits Awarded	PS Student	Reserved
Duration of Disciplinary Action	Incident	Reserved

Element Name	Entity	Record Status
Duration of Disciplinary Action	K12 Student	Reserved
Early Childhood Credential	EL Staff	Reserved
Early Childhood Program Setting	EL Organization	Reserved
Early Childhood Program Type Enrollment	EL Child	Reserved
Early Intervention or Special Education Services Received	EL Child	Reserved
Early Intervention or Special Education Services Setting	EL Child	Reserved
Economic Disadvantage Status	K12 Student	Reserved
Education Staff Classification	EL Staff	Reserved
Education Staff Classification	K12 Staff	Reserved
Educational Services After Removal	Incident	Reserved
Educational Services After Removal	K12 Student	Reserved
Electronic Mail Address	K12 Student	Reserved
Electronic Mail Address Type	K12 Student	Reserved
Elementary-Middle Additional Indicator Status	K12 School	Reserved
Elementary-Middle Additional Indicator Status	LEA	Reserved
Eligibility Status for School Food Service Programs	K12 Student	Active
Employment Separation Reason	K12 Staff	Reserved
Employment Separation Type	K12 Staff	Reserved
Employment Start Date	EL Staff	Reserved
Employment Status	EL Staff	Reserved
Employment Status	K12 Staff	Reserved
End of Term Status	K12 Student	Active
English Remedial Assessment	PS Student	Active
Enrollment Date	EL Child	Reserved
Enrollment in Postsecondary Award Type	PS Student	Reserved
Enrollment Status	K12 Student	Active
Entry Date	EL Child	Reserved
Entry Date	K12 Section	Reserved
Entry Date into Postsecondary	PS Student	Active
Entry Grade Level	K12 Student	Reserved
Entry Type	K12 Student	Reserved
Estimated Time Element	K12 Section	Reserved
Exit Date	EL Child	Reserved
Exit Date	K12 Student	Reserved
Exit Date	PS Student	Active
Exit or Withdrawal Status	K12 Section	Reserved
Exit or Withdrawal Status	K12 Student	Reserved
Exit or Withdrawal Type	K12 Student	Reserved
Facilities Identifier	K12 School	Reserved

Element Name	Entity	Record Status
Facilities Identifier	LEA	Reserved
Faculty and Administration Performance Level	K12 Staff	Reserved
Fall Attendance Status	PS Student	Active
Family Income	EL Family	Reserved
Federal Program Code	SEA	Reserved
Federal Programs Funding Allocation	LEA	Reserved
Federal Programs Funding Allocation	SEA	Reserved
Federal Programs Funding Allocation Type	SEA	Reserved
Federal School Code	PS Institution	Active
Financial Aid Award Amount	PS Student	Reserved
Financial Aid Award Status	PS Student	Reserved
Financial Aid Award Type	PS Student	Reserved
Firearm Type	Incident	Reserved
First English Course ID	PS Student	Active
First English Letter Grade	PS Student	Active
First Entry Date into a US School	K12 Student	Reserved
First Generation in College Status	PS Student	Reserved
First Instruction Date	K12 School	Active
First Math Course ID	PS Student	Active
First Math Letter Grade	PS Student	Active
First Name	EL Child	Reserved
First Name	EL Staff	Reserved
First Name	K12 Staff	Reserved
First Name	K12 Student	Active
First Name	PS Student	Active
First Name	Parent/Guardian	Reserved
First Name	Parent/Guardian	Reserved
First Name	K12 Student	Active
First Time Postsecondary Student	PS Student	Reserved
Fiscal Year	PS Calendar	Active
Full Year Expulsion	Incident	Reserved
Full Year Expulsion	K12 Student	Reserved
Funds Transfer Amount	LEA	Reserved
GED Preparation Program Participation Status	K12 Student	Active
Generation Code or Suffix	EL Child	Reserved
Generation Code or Suffix	EL Staff	Reserved
Generation Code or Suffix	K12 Staff	Reserved
Generation Code or Suffix	PS Student	Reserved
Generation Code or Suffix	Parent/Guardian	Reserved

Element Name	Entity	Record Status
Generation Code or Suffix	Parent/Guardian	Reserved
Generation Code or Suffix	K12 Student	Active
Gifted and Talented	K12 Student	Reserved
Grade Earned	K12 Section	Reserved
Grade Earned	K12 Student	Reserved
Grade Level when Assessed	K12 Student	Reserved
Grade Level when Assessed	Student Assessment Registration	Reserved
Grade Level When Course Taken	K12 Section	Reserved
Grade Level When Course Taken	K12 Student	Reserved
Grade Point Average	PS Student	Reserved
Grade Point Average Cumulative	K12 Student	Reserved
Grade Point Average Cumulative	PS Student	Reserved
Grade Point Average Given Session	K12 Student	Reserved
Grade Point Average Weighted Indicator	PS Student	Reserved
Grade Points Earned Cumulative	K12 Student	Reserved
Grade Value Qualifier	K12 Section	Reserved
Grade Value Qualifier	K12 Student	Reserved
Grades Offered	K12 School	Reserved
Graduation Rate Survey Cohort Year	K12 Student	Reserved
Graduation Rate Survey Indicator	K12 Student	Reserved
Gun Free Schools Act Reporting Status	K12 School	Reserved
Gun Free Schools Act Reporting Status	LEA	Reserved
Harassment or Bullying Policy Status	LEA	Reserved
Hearing Screening	EL Child	Reserved
Hearing Screening Date	EL Child	Reserved
High School	PS Student	Active
High School Course Requirement	K12 Course	Reserved
High School Course Requirement	K12 Section	Reserved
High School Diploma Distinction Type	K12 Student	Reserved
High School Diploma Type	PS Student	Active
High School Diploma Type	K12 Student	Active
High School Graduation Rate Indicator Status	K12 School	Reserved
High School Graduation Rate Indicator Status	LEA	Reserved
Highest Level of Education Completed	K12 Staff	Reserved
Highest Level of Education Completed	Parent/Guardian	Reserved
Highly Qualified Teacher Indicator	K12 Staff	Reserved
Hire Date	EL Staff	Reserved
Hire Date	K12 Staff	Reserved

Element Name	Entity	Record Status
Hispanic or Latino Ethnicity	EL Child	Reserved
Hispanic or Latino Ethnicity	K12 Staff	Reserved
Hispanic or Latino Ethnicity	K12 Student	Active
Hispanic or Latino Ethnicity	PS Student	Active
Hispanic or Latino Ethnicity	K12 Student	Active
Homeless Primary Nighttime Residence	K12 Student	Reserved
Homeless Serviced Indicator	K12 Student	Reserved
Homeless Unaccompanied Youth Status	K12 Student	Reserved
Homelessness Status	EL Child	Reserved
Homelessness Status	K12 Student	Reserved
Honors Description	K12 Student	Reserved
Hours Available Per Day	EL Organization	Reserved
IDEA Discipline Method for Firearms Incidents	Incident	Reserved
IDEA Discipline Method for Firearms Incidents	K12 Student	Reserved
IDEA Educational Environment for Early Childhood	K12 Student	Reserved
IDEA Educational Environment for School Age	K12 Student	Reserved
IDEA Indicator	K12 Student	Active
IDEA Interim Removal	Incident	Reserved
IDEA Interim Removal	K12 Student	Reserved
IDEA Interim Removal Reason	Incident	Reserved
IDEA Interim Removal Reason	K12 Student	Reserved
Identification System for Assessment	Assessment	Reserved
Identification System for Assessment	Assessment	Reserved
Identification System for Assessment	K12 Student	Reserved
Identification System for Local Education Agency	K12 Staff	Reserved
Identification System for Local Education Agency	K12 Student	Active
Identification System for Local Education Agency	LEA	Reserved
Identification System for Local Education Agency	PS Student	Active
Identification System for School	K12 School	Reserved
Identification System for School	K12 Staff	Reserved
Identification System for School	K12 Student	Active
Identification System for School	PS Student	Reserved
Identification System for Staff Member	K12 Section	Reserved
Identification System for Staff Member	K12 Staff	Reserved
Identification System for Student	K12 Section	Reserved
Identification System for Student	K12 Student	Active
Identification System for Student	PS Student	Active
IHE County	PS Institution	Active
IHE County	PS Institution	Active

Element Name	Entity	Record Status
IHE Region	PS Institution	Active
Immunization Date	EL Child	Reserved
Immunization Record Flag	K12 Student	Reserved
Incident Behavior	Incident	Reserved
Incident Cost	Incident	Reserved
Incident Date	Incident	Reserved
Incident Description	Incident	Reserved
Incident Identifier	Incident	Reserved
Incident Injury Type	Incident	Reserved
Incident Location	Incident	Reserved
Incident Reporter Type	Incident	Reserved
Incident Time	Incident	Reserved
Incident Time Description Code	Incident	Reserved
Included in Adequate Yearly Progress Calculation Indicator	K12 Student	Reserved
Income Calculation Method	EL Family	Reserved
Increased Learning Time Type	K12 School	Reserved
Individualized Program Type	EL Child	Reserved
Individualized Program Type	K12 Student	Reserved
Initial Enrollment Term	PS Student	Reserved
Initial License Date	EL Organization	Reserved
Innovative Dollars Spent	LEA	Reserved
Innovative Dollars Spent on Strategic Priorities	LEA	Reserved
Innovative Programs Funds Received	LEA	Reserved
Institute of Higher Education	PS Institution	Active
Institution IPEDS UnitID	PS Institution	Reserved
Institution Telephone Number Type	K12 School	Reserved
Institution Telephone Number Type	LEA	Reserved
Instruction Language	K12 Course	Reserved
Instruction Language	K12 Section	Reserved
Instructional Activity Hours Attempted	PS Student	Reserved
Instructional Activity Hours Completed	PS Student	Reserved
Instructional Activity Hours Type	PS Student	Reserved
Instructional Minutes	K12 School	Reserved
Instructional Recommendation	K12 Student	Reserved
Insurance Coverage	EL Child	Reserved
Integrated Technology Status	LEA	Reserved
Internet Access	K12 School	Reserved
Interscholastic Sport Participants - Female Only	LEA	Reserved
Interscholastic Sport Participants - Male Only	LEA	Reserved

Element Name	Entity	Record Status
Interscholastic Sports - Female Only	LEA	Reserved
Interscholastic Sports - Male Only	LEA	Reserved
Interscholastic Teams - Female Only	LEA	Reserved
Interscholastic Teams - Male Only	LEA	Reserved
Itinerant Teacher	K12 Staff	Reserved
K12 School Address	PS Student	Active
K12 School ID	PS Student	Active
K12 School Name	PS Student	Active
Kindergarten Daily Length	LEA	Reserved
Kindergarten Program Participation Type	K12 Student	Reserved
Language Code	EL Child	Reserved
Language Code	EL Staff	Reserved
Language Code	K12 Student	Reserved
Language Type	EL Child	Reserved
Language Type	EL Staff	Reserved
Language Type	K12 Student	Reserved
Last Instruction Date	K12 School	Active
Last or Surname	EL Child	Reserved
Last or Surname	EL Staff	Reserved
Last or Surname	K12 Staff	Reserved
Last or Surname	K12 Student	Reserved
Last or Surname	PS Student	Reserved
Last or Surname	Parent/Guardian	Reserved
Last or Surname	Parent/Guardian	Reserved
Last Qualifying Move Date	K12 Student	Reserved
Latitude	K12 School	Reserved
Learning Standard Document Creator	Learning Standard Document	Reserved
Learning Standard Document Description	Learning Standard Document	Reserved
Learning Standard Document Identifier	Learning Standard Document	Reserved
Learning Standard Document Jurisdiction	Learning Standard Document	Reserved
Learning Standard Document Publication Status	Learning Standard Document	Reserved
Learning Standard Document Subject	Learning Standard Document	Reserved
Learning Standard Document Title	Learning Standard Document	Reserved
Learning Standard Document Valid End Date	Learning Standard Document	Reserved

Element Name	Entity	Record Status
Learning Standard Document Valid Start Date	Learning Standard Document	Reserved
Learning Standard Document Version	Learning Standard Document	Reserved
Learning Standard Item	Assessment	Reserved
Learning Standard Item	Learning Standards Item	Reserved
Learning Standard Item Code	Learning Standard Item	Reserved
Learning Standard Item Identifier	Learning Standard Item	Reserved
Learning Standard Item Prerequisite Identifier	Learning Standard Item	Reserved
Learning Standard Item Statement	Learning Standard Item	Reserved
Learning Standard Item Type	Learning Standard Item	Reserved
Leave Event Type	K12 Staff	Reserved
Level of Institution	PS Institution	Active
Level of Specialization in Early Learning	EL Staff	Reserved
License Exempt	EL Organization	Reserved
Limited English Proficiency - Postsecondary	PS Student	Reserved
Limited English Proficiency Exit Date	K12 Student	Reserved
Limited English Proficiency Status	K12 Student	Active
Literacy Assessment Administered Type	K12 Student	Reserved
Literacy Goal Met Status	K12 Student	Reserved
Literacy Post Test Status	K12 Student	Reserved
Literacy Pre Test Status	K12 Student	Reserved
Local Education Agency Funds Transfer Type	LEA	Reserved
Local Education Agency Identifier	K12 Staff	Reserved
Local Education Agency Identifier	K12 Student	Reserved
Local Education Agency Identifier	LEA	Active
Local Education Agency Identifier	PS Student	Reserved
Local Education Agency Improvement Status	LEA	Reserved
Local Education Agency Operational Status	LEA	Reserved
Local Education Agency Supervisory Union Identification Number	LEA	Reserved
Local Education Agency Transferability of Funds	LEA	Reserved
Longitude	K12 School	Reserved
Magnet or Special Program Emphasis School	K12 School	Reserved
Marking Period	K12 Section	Reserved
Marking Period	K12 Student	Reserved

Element Name	Entity	Record Status
Math Remedial Assessment	PS Student	Active
Medical Alert Indicator	K12 Student	Reserved
Mid Term Mark	K12 Section	Reserved
Mid Term Mark	K12 Student	Reserved
Middle Name	EL Child	Reserved
Middle Name	EL Staff	Reserved
Middle Name	K12 Staff	Reserved
Middle Name	K12 Student	Active
Middle Name	PS Student	Active
Middle Name	Parent/Guardian	Reserved
Middle Name	Parent/Guardian	Reserved
Middle Name	K12 Student	Active
Migrant Education Program Eligibility Expiration Date	K12 Student	Reserved
Migrant Education Program Enrollment Type	K12 Student	Reserved
Migrant Education Program Participation Status	K12 Student	Reserved
Migrant Education Program Personnel Indicator	K12 Staff	Reserved
Migrant Education Program Project Based	K12 Student	Reserved
Migrant Education Program Project Type	LEA	Reserved
Migrant Education Program Services Type	K12 Student	Reserved
Migrant Education Program Session Type	LEA	Reserved
Migrant Education Program Staff Category	K12 Staff	Reserved
Migrant Prioritized for Services	K12 Student	Reserved
Migrant Status	K12 Student	Active
Migrant Student Qualifying Arrival Date	K12 Student	Reserved
Minutes Per Day	K12 School	Reserved
Multiple Birth Indicator	K12 Student	Reserved
Name of Institution	EL Staff	Reserved
Name of Institution	PS Student	Active
Name of Institution	K12 School	Active
Name of Institution	PS Institution	Active
Native Credit Hours Earned	PS Student	Active
Native Hawaiian or Other Pacific Islander	EL Child	Reserved
Native Hawaiian or Other Pacific Islander	K12 Student	Active
Native Hawaiian or Other Pacific Islander	K12 Student	Active
Native Hawaiian or Other Pacific Islander	PS Student	Active
Neglected or Delinquent Academic Achievement Indicator	K12 Student	Reserved
Neglected or Delinquent Academic Outcome Indicator	K12 Student	Reserved
Neglected or Delinquent Obtained Employment	K12 Student	Reserved
Neglected or Delinquent Program Type	K12 Student	Reserved

Element Name	Entity	Record Status
Neglected or Delinquent Status	K12 Student	Reserved
Non Traditional Program Enrollee Status	K12 Student	Reserved
Nonpromotion Reason	K12 Student	Reserved
Normal Length of Time for Completion	PS Student	Reserved
Normal Length of Time for Completion Units	PS Student	Reserved
Number of Credits Attempted	K12 Section	Reserved
Number of Credits Attempted	K12 Student	Reserved
Number of Credits Earned	K12 Section	Reserved
Number of Credits Earned	K12 Student	Active
Number of Credits Earned	PS Section	Active
Number of Days Absent	K12 Section	Reserved
Number of Days Absent	K12 Student	Reserved
Number of Days for Title III Subgrants	SEA	Reserved
Number of Days in Attendance	EL Child	Reserved
Number of Days in Attendance	K12 Section	Reserved
Number of Days in Attendance	K12 Student	Reserved
Number of Immigrant Program Subgrants	LEA	Reserved
Number of People in Family	EL Family	Reserved
Number of People in Household	EL Family	Reserved
Nursing Indicator	PS Student	Active
Nursing Indicator	PS Institution	Active
Office of Postsecondary Education Identifier	PS Institution	Reserved
Operation Date	EL Organization	Reserved
Operational Status Effective Date	K12 School	Reserved
Operational Status Effective Date	LEA	Reserved
Organization Name	LEA	Reserved
Organization Name	SEA	Reserved
Other Name	K12 Staff	Reserved
Other Name	K12 Student	Active
Other Name	PS Student	Active
Other Name Type	K12 Staff	Reserved
Other Name Type	K12 Student	Reserved
Other Name Type	PS Student	Reserved
Paraprofessional Qualification Status	K12 Staff	Reserved
Participation in School Food Service Programs	EL Child	Reserved
Participation Status for Math	K12 School	Reserved
Participation Status for Math	LEA	Reserved
Participation Status for Reading and Language Arts	K12 School	Reserved
Participation Status for Reading and Language Arts	LEA	Reserved

Element Name	Entity	Record Status
Pass Indicator	PS Section	Active
Perkins Limited English Proficiency Status	K12 Student	Reserved
Persistently Dangerous Status	K12 School	Active
Persistently Lowest Achieving School Status	K12 School	Reserved
Person Relationship to Learner Qualifier Type	Parent/Guardian	Reserved
Person Relationship to Learner Qualifier Type	Parent/Guardian	Reserved
Person Relationship to Learner Type	Parent/Guardian	Reserved
Person Relationship to Learner Type	Parent/Guardian	Reserved
Personal Information Verification	K12 Staff	Reserved
Personal Information Verification	K12 Student	Reserved
Personal Title or Prefix	EL Staff	Reserved
Personal Title or Prefix	K12 Staff	Reserved
Personal Title or Prefix	K12 Student	Reserved
Personal Title or Prefix	PS Student	Reserved
Personal Title or Prefix	Parent/Guardian	Reserved
Personal Title or Prefix	Parent/Guardian	Reserved
Position Title	K12 Staff	Reserved
Postsecondary Course Level	PS Section	Reserved
Postsecondary Course Title	PS Section	Reserved
Postsecondary Enrollment Action	K12 Student	Reserved
Postsecondary Enrollment Status	PS Student	Active
Postsecondary Enrollment Type	PS Student	Reserved
Pre and Post Test Indicator	K12 Student	Reserved
Prekindergarten Daily Length	LEA	Reserved
Pre-kindergarten Eligibility	LEA	Reserved
Pre-kindergarten Eligible Ages for Non-IDEA Students	LEA	Reserved
Present Attendance Category	K12 Student	Reserved
Pretest Results	Assessment Item Response	Reserved
Pretest Results	K12 Student	Reserved
Primary Assignment Indicator	K12 Staff	Reserved
Primary Disability Type	EL Child	Reserved
Primary Disability Type	K12 Student	Reserved
Primary Telephone Number Indicator	EL Organization	Reserved
Primary Telephone Number Indicator	K12 School	Reserved
Primary Telephone Number Indicator	K12 Student	Active
Primary Telephone Number Indicator	LEA	Reserved
Primary Telephone Number Indicator	PS Student	Reserved
Prior Early Childhood Experience	EL Child	Reserved

Element Name	Entity	Record Status
Prior to Secondary Course Identifier	K12 Course	Reserved
Prior to Secondary Course Identifier	K12 Section	Reserved
Professional Educational Job Classification	K12 Staff	Reserved
Proficiency Status	Assessment Item Response	Reserved
Proficiency Status	K12 Student	Reserved
Proficiency Target Status for Math	K12 School	Reserved
Proficiency Target Status for Math	LEA	Reserved
Proficiency Target Status for Reading and Language Arts	K12 School	Reserved
Proficiency Target Status for Reading and Language Arts	LEA	Reserved
Program Degree Level	PS Institution	Active
Program Degree Level	PS Student	Active
Program Discipline	PS Institution	Active
Program Discipline	PS Institution	Active
Program Eligibility	EL Child	Reserved
Program Exit Reason	K12 Student	Reserved
Program Identifier	Program	Reserved
Program in Multiple Purpose Facility	LEA	Reserved
Program Length Hours	PS Student	Reserved
Program Length Hours Type	PS Student	Reserved
Program Major	PS Student	Active
Program Major	PS Institution	Active
Program Name	Program	Reserved
Program Option Variation	EL Organization	Reserved
Program Participation Exit Date	EL Child	Reserved
Program Participation Exit Date	K12 Student	Reserved
Program Participation Start Date	EL Child	Reserved
Program Participation Start Date	K12 Student	Reserved
Program Sponsor Type	K12 Staff	Reserved
Program Taxonomy	PS Institution	Active
Program Type	K12 School	Reserved
Progress Level	K12 Student	Reserved
Projected Graduation Date	K12 Student	Reserved
Promotion Reason	K12 Student	Reserved
Proof of Residency	EL Family	Reserved
Public School Choice Funds Spent	LEA	Reserved
Public School Choice Implementation Status	LEA	Reserved
Public School Indicator	PS Student	Active
Public School Residence Status	K12 Student	Reserved

Element Name	Entity	Record Status
Qualifying Move From City	K12 Student	Reserved
Qualifying Move From Country	K12 Student	Reserved
Qualifying Move From State	K12 Student	Reserved
Quality Rating and Improvement System Participation	EL Organization	Reserved
Quality Rating and Improvement System Score	EL Organization	Reserved
Race	PS Student	Active
Reading Remedial Assessment	PS Student	Active
Reason Not Tested	K12 Student	Reserved
Receiving Location of Instruction	K12 Section	Reserved
Recognition for Participation or Performance in an Activity	K12 Student	Reserved
Reconstituted Status	K12 School	Reserved
Related Learning Standards	K12 Section	Reserved
Related to Zero Tolerance Policy	Incident	Reserved
Related to Zero Tolerance Policy	K12 Student	Reserved
Remedial Assessment Indicator	PS Student	Active
Reporter Identifier	Incident	Reserved
Required Immunization	EL Child	Reserved
Response Status	Assessment Item Response	Reserved
Response Status	K12 Student	Reserved
Responsible District Identifier	K12 Student	Reserved
Responsible District Type	K12 Student	Reserved
Responsible Organization Name	EL Organization	Reserved
Responsible School Identifier	K12 Student	Reserved
Responsible School Type	K12 Student	Reserved
Restructuring Action	K12 School	Reserved
Retirement Benefits	K12 Staff	Reserved
Rural Education Achievement Program Alternative Funding Status	LEA	Reserved
Safe and Drug Free Baseline	LEA	Reserved
Safe and Drug Free Baseline Year	LEA	Reserved
Safe and Drug Free Collection Frequency	LEA	Reserved
Safe and Drug Free Indicator Name	LEA	Reserved
Safe and Drug Free Instrument	LEA	Reserved
Safe and Drug Free Performance	LEA	Reserved
Safe and Drug Free Target	LEA	Reserved
Safe and Drug Free Year Most Recent Collection	LEA	Reserved
Salary For Teaching Assignment Only Indicator	K12 Staff	Reserved
SAT Math Score	PS Student	Active
SAT Verbal Score	PS Student	Active

Element Name	Entity	Record Status
Scale Score 25th Percentile	Assessment	Reserved
Scale Score 25th Percentile	Assessment Subtest	Reserved
Scale Score 25th Percentile	Performance Level	Reserved
Scale Score 50th Percentile	Assessment	Reserved
Scale Score 50th Percentile	Assessment Subtest	Reserved
Scale Score 50th Percentile	Performance Level	Reserved
Scale Score 75th Percentile	Assessment	Reserved
Scale Score 75th Percentile	Assessment Subtest	Reserved
Scale Score 75th Percentile	Performance Level	Reserved
School Choice Applied for Transfer Status	K12 Student	Reserved
School Choice Eligible for Transfer Status	K12 Student	Reserved
School Choice Transfer Status	K12 Student	Reserved
School Identifier	K12 School	Reserved
School Identifier	K12 Staff	Reserved
School Identifier	PS Student	Reserved
School Identifier	K12 Student	Active
School Improvement Allocation	LEA	Reserved
School Improvement Exit Date	K12 School	Reserved
School Improvement Funds Status	K12 School	Active
School Improvement Grant Intervention Type	K12 School	Active
School Improvement Reserved Funds Percentage	LEA	Reserved
School Improvement Status	K12 School	Active
School Level	K12 School	Active
School Operational Status	K12 School	Reserved
School Type	K12 School	Active
School Year	Calendar	Reserved
School Year	K12 School	Reserved
School Year Minutes	K12 School	Reserved
Secondary Course Identifier	K12 Course	Reserved
Secondary Course Identifier	K12 Section	Reserved
Secondary Course Level	K12 Course	Reserved
Secondary Course Level	K12 Section	Reserved
Secondary Course Subject Area	K12 Course	Reserved
Secondary Course Subject Area	K12 Section	Reserved
Secondary Incident Behavior	Incident	Reserved
Section 504 Status	K12 Student	Reserved
Sequence of Course	K12 Course	Active
Sequence of Course	K12 Section	Reserved
Service Entry Date	EL Child	Reserved

Element Name	Entity	Record Status
Service Exit Date	EL Child	Reserved
Session Begin Date	K12 Section	Reserved
Session Designator	K12 Section	Reserved
Session Designator	PS Institution	Active
Session End Date	K12 Section	Reserved
Session Type	K12 Section	Reserved
Sex	EL Child	Reserved
Sex	EL Staff	Reserved
Sex	K12 Staff	Reserved
Sex	PS Student	Active
Sex	K12 Student	Active
Shared Time Indicator	K12 School	Reserved
Shortened Expulsion	Incident	Reserved
Shortened Expulsion	K12 Student	Reserved
SIC Sector	PS Institution	Active
SIC Segment	PS Institution	Active
Single Parents Including Single Pregnant Women	K12 Student	Reserved
Single Sex Class Status	K12 Section	Reserved
Site Name	EL Organization	Reserved
Social Security Number	K12 Staff	Reserved
Social Security Number	PS Section	Reserved
Social Security Number	PS Student	Active
Social Security Number	K12 Student	Active
Source of Family Income	EL Family	Reserved
Special Education Age Group Taught	K12 Staff	Reserved
Special Education Exit Reason	K12 Student	Active
Special Education Paraprofessional	K12 Staff	Reserved
Special Education Related Services Personnel	K12 Staff	Reserved
Special Education Services Exit Date	K12 Student	Reserved
Special Education Staff Category	K12 Staff	Reserved
Special Education Teacher	K12 Staff	Reserved
Spring Attendance Status	PS Student	Active
Staff Compensation Health Benefits	K12 Staff	Reserved
Staff Compensation Other Benefits	K12 Staff	Reserved
Staff Evaluation Outcome	K12 Staff	Reserved
Staff Evaluation Scale	K12 Staff	Reserved
Staff Evaluation Score or Rating	K12 Staff	Reserved
Staff Evaluation System	K12 Staff	Reserved
Staff Full Time Equivalency	K12 Staff	Reserved

Element Name	Entity	Record Status
Staff Member Identifier	K12 Section	Reserved
Staff Member Identifier	K12 Staff	Reserved
Standardized Admission Test Score	PS Student	Reserved
Standardized Admission Test Type	PS Student	Reserved
State Abbreviation	EL Child	Reserved
State Abbreviation	EL Organization	Reserved
State Abbreviation	EL Staff	Reserved
State Abbreviation	K12 Staff	Reserved
State Abbreviation	K12 Student	Active
State Abbreviation	LEA	Active
State Abbreviation	PS Student	Active
State Abbreviation	SEA	Active
State Abbreviation	K12 School	Active
State Assessment Administration Funding	LEA	Reserved
State Assessment Standards Funding	LEA	Reserved
State Federal Information Processing Standards Code	SEA	Reserved
State Identification Code	PS Institution	Active
State of Birth Abbreviation	K12 Student	Reserved
State of Residence	PS Student	Reserved
State Poverty Designation	K12 School	Reserved
State Transferability of Funds	SEA	Reserved
STEM Indicator	PS Student	Active
STEM Indicator	PS Institution	Active
Student Attendance Rate	K12 Student	Reserved
Student Class Rank	K12 Student	Reserved
Student Growth	Assessment Item Response	Reserved
Student Growth	K12 Student	Reserved
Student Identifier	K12 Section	Reserved
Student Identifier	K12 Student	Active
Student Identifier	PS Section	Reserved
Student Identifier	PS Student	Reserved
Student Level	PS Student	Active
Student Progress	Assessment Item Response	Reserved
Student Progress	K12 Student	Reserved
Student Support Service Type	K12 School	Reserved
Sub Campus	PS Institution	Active
Supplemental Education Services Public School Choice Twenty Percent Obligation	LEA	Reserved

Element Name	Entity	Record Status
Supplemental Educational Services Funds Spent	LEA	Reserved
Supplemental Educational Services Per Pupil Expenditure	LEA	Reserved
Teacher of Record	K12 Section	Reserved
Teaching Assignment Contribution Percentage	K12 Section	Reserved
Teaching Assignment End Date	K12 Staff	Reserved
Teaching Assignment Role	K12 Section	Reserved
Teaching Assignment Start Date	K12 Staff	Reserved
Teaching Credential Basis	K12 Staff	Reserved
Teaching Credential Type	K12 Staff	Reserved
Technology Literacy Status in 8th Grade	K12 Student	Reserved
Technology Skills Standards Met	K12 Staff	Reserved
Telephone Number	EL Organization	Reserved
Telephone Number	K12 Student	Reserved
Telephone Number	LEA	Reserved
Telephone Number	PS Student	Reserved
Telephone Number	K12 School	Active
Telephone Number Type	K12 Student	Reserved
Telephone Number Type	PS Student	Reserved
Terminated Title III Programs Due to Failure	LEA	Reserved
Timetable Day Identifier	K12 Section	Reserved
Title I Indicator	K12 Student	Active
Title I Instructional Services	LEA	Reserved
Title I Program Staff Category	K12 Staff	Reserved
Title I Program Type	LEA	Reserved
Title I Program Type	K12 School	Active
Title I School Status	K12 School	Active
Title I School Supplemental Services Applied Status	K12 Student	Reserved
Title I School Supplemental Services Eligible Status	K12 Student	Reserved
Title I School Supplemental Services Received Status	K12 Student	Active
Title I Schoolwide Program Participation	K12 Student	Reserved
Title I Support Services	LEA	Reserved
Title I Targeted Assistance Participation	K12 Student	Reserved
Title I Targeted Assistance Staff Funded	K12 Staff	Reserved
Title III Accountability Progress Status	K12 Student	Reserved
Title III Immigrant Participation Status	K12 Student	Reserved
Title III Immigrant Status	K12 Student	Reserved
Title III Language Instruction Program Type	K12 School	Reserved
Title III Language Instruction Program Type	LEA	Reserved
Title III LEP Instructors Needed in Next 5 Years	LEA	Reserved

Element Name	Entity	Record Status
Title III Limited English Proficient Participation Status	K12 Student	Active
Title III Professional Development Type	LEA	Reserved
Title IV Participant and Recipient	PS Student	Reserved
Total Benefits	K12 Staff	Reserved
Total Number in Class	K12 Student	Reserved
Total Salary	K12 Staff	Reserved
Transfer-ready	PS Student	Reserved
Truant Status	K12 Student	Reserved
Tuition Residency Type	PS Student	Reserved
Type of Use of the Rural Low-Income Schools Program	LEA	Reserved
United States Citizenship Status	PS Student	Active
Uses of Funds for Purposes other than Standards and Assessment Development	SEA	Reserved
Visa Type	PS Student	Reserved
Vision Screening	EL Child	Reserved
Vision Screening Date	EL Child	Reserved
Web Site Address	K12 School	Reserved
Web Site Address	LEA	Reserved
Weeks of Gestation	EL Child	Reserved
Weight at Birth	EL Child	Reserved
White	EL Child	Reserved
White	K12 Staff	Reserved
White	K12 Student	Active
White	PS Student	Active
Years of Prior Teaching Experience	K12 Staff	Reserved

Appendix D – Data Elements for Policy Questions 2, 3, and 11

Policy Question 2 Data Elements	
Address Postal Code	Migrant Status
Address Street Number and Name	Name of Institution
Adequate Yearly Progress Status	Name of Institution
Birthdate	Persistently Dangerous Status
Career and Technical Education Completer	Postsecondary Enrollment Status
Career and Technical Education Concentrator	Race
Control of Institution	School Identifier
Disability Status	School Improvement Funds Status
Eligibility Status for School Food Service Programs	School Improvement Grant Intervention Type
Entry Date into Postsecondary	School Improvement Status
Exit Date	School Level
Federal School Code	School Type
First Instruction Date	Session Designator
Generation Code or Suffix	Sex
High School Diploma Type	Social Security Number
IDEA Indicator	State Abbreviation
Identification System for Student	Telephone Number
Identification System for Student	Title I Indicator
Last Instruction Date	Title I Program Type
Limited English Proficiency Status	Title I School Status
Middle Name	Title III Limited English Proficient Participation Status

Policy Question 3 Data Elements		
ACT Composite Score	First Name	Program Degree Level
ACT English Score	GED Preparation Program Participation Status	Program Discipline
ACT Math Score	High School	Program Major
ACT Reading Score	High School Diploma Type	Program Taxonomy
ACT Science Score	High School Diploma Type	Public School Indicator
Address County Name	Hispanic or Latino Ethnicity	Race
Admission Exemption	Identification System for Local Education Agency	Reading Remedial Assessment
American Indian or Alaska Native	Identification System for School	Remedial Assessment Indicator
Asian	Identification System for Student	SAT Math Score
Birthdate	IHE County	SAT Verbal Score
Black or African American	IHE Region	School Type

Policy Question 3 Data Elements		
Career and Technical Education Completer	Institute of Higher Education	Sequence of Course
Career and Technical Education Concentrator	K12 School Address	Sex
Cohort Year	K12 School ID	Sex
Course Academic Grade	K12 School Name	SIC Sector
Cumulative GPA	Math Remedial Assessment	SIC Segment
End of Term Status	Middle Name	Social Security Number
English Remedial Assessment	Name of Institution	Spring Attendance Status
Enrollment Status	Native Credit Hours Earned	State Identification Code
Fall Attendance Status	Native Hawaiian or Other Pacific Islander	STEM Indicator
First English Course ID	Number of Credits Earned	Sub Campus
First English Letter Grade	Number of Credits Earned	United States Citizenship Status
First Math Course ID	Nursing Indicator	White
First Math Letter Grade	Pass Indicator	

Policy Question 11 Data Elements	
Address Postal Code	Name of Institution
American Indian or Alaska Native	Native Hawaiian or Other Pacific Islander
Asian	Nursing Indicator
Birthdate	Other Name
Calendar End Date	Program Degree Level
Calendar Start Date	Program Discipline
Career and Technical Education Concentrator	Program Major
Collection Year	Race
County Federal Information Processing Standards Code	Sex
First Name	SIC Segment
Fiscal Year	Social Security Number
GED Preparation Program Participation Status	State Abbreviation
Hispanic or Latino Ethnicity	State Identification Code
IHE County	STEM Indicator
IHE Region	Student Level
Level of Institution	White
Middle Name	

Appendix E – List of Terms

Terms	
ACG Grants	Home Study
Acquired Citizenship	HS
Additional Credit Type Awarded	IDEA
Adjusted Cohort	IEP
Adult Basic Education (ABE)	Income level
AP	Individual or Student with Disabilities
Assessment	Initial cohort
Associate Degree	Institution of Higher Education
Attendance Pattern	Institutional Aid Total
Bachelor's degree	Institutional Grants
Birth Date	IPEDS
Certificate/Diploma (1-2 years)	K-12
Certificate/Diploma (2-4 years)	Lawful Permanent Resident
Certificate/Diploma of Economic Value with Industry Certification or Licensure	LEA
Charter Schools	LEP
CIP Code/Program Taxonomy	Less than 2-year institution
Cohort	Local Education Agency (LEA)
College Number	Market penetration
Community College	Maryland Local Education Agencies (LEA)
Completion	Maryland Postsecondary Institution
Completion ratio	MSA
Course completion	Outcome Metrics
Course level characteristic	P-16
Credit	P-20
Credit Accumulation	PARCC
Credit Course	Parent PLUS loans
Credit Hour	Part-Time Student
Credits to Degree	Pell Grant Program
CS	Pell Grants
Degree	Pell Recipient
Degrees Awarded	Postsecondary Education
Dependency and income	Private Institution
Dependency status	Progress Metrics
Developmental Course	PSAT
Diploma	Public Institution
Disadvantaged	Race/Ethnicity
Dual Credit	Remedial Course

Terms	
Dual Credit	Remediation
Dual Credit Dual Enrollment Credits Awarded	Retention Rate
Dual Enrollment	Revised Cohort
Dual-Enrollment Program	Section 504
Early College Access (ECA) Program	SMART grants
ELL	Special Services
Employer aid	SPED
Enrollment	Stafford loans
Enrollment in remedial education	Stafford subsidized loans
Entering Students	Stafford unsubsidized loans
ESOL	State aid total
Exclusions	State Assigned Student Identifier (SASID)
Exit	State Education Agency (SEA)
Exit Status	State grants
Fall enrollment	STEM
Federal aid total	Student loans
Federal campus-based aid	Sub-cohort
Federal grants	Subtest Score
Federal student loans	Success beyond remedial education
Federal Title IV aid	Success in first-year college courses
Federal Work-Study	SWD
FICE Code	Time to Degree
Financial Aid	Total aid
First-Time Student	Total grants
Four Year Institution	Transfer (At Entry)
Full-time equivalent student (FTE)	Transfer of credit
Full-year cohort	Transfer rates
Gender	Transfer-in student
GPA	Transfer-out rate
Graduate Assistantships	Transfer-out student
Graduate PLUS loans	Two Year Institution
Graduate Program	Undergraduate
Graduation Rate	Veterans benefits
High School Diploma or Recognized Equivalent	Visa
Hispanic or Latino (new & old)	Work-study