MLDS Center
Maryland Longitudinal Data System

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

Memorandum

TO: MLDS Governing Board

FROM: Tejal Cherry, CIO

DATE: June 5, 2026

SUBJECT: MLDS Information Technology Update

Purpose

The purpose of this agenda item is to provide information to the Governing Board regarding two information technology projects:

1. Statewide Digital Accessibility Project
2. MLDSC Audit/Penetration Testing

Digital Accessibility Project

Background

Web accessibility is both a legal obligation and a public-service responsibility for Maryland state agencies. The Americans with Disabilities Act (ADA) and Section 508 of the Rehabilitation Act require government websites to be accessible to individuals with disabilities. **WCAG 2.2**[1] is the standard against which this compliance is measured. The Center has been working in coordination with the Maryland Department of Information Technology (DoIT) to update the MLDS Center Website to be in compliance with the accessibility standards.

The project is focused on achieving compliance with WCAG 2.2 guidelines across all publicly accessible pages of mldscenter.maryland.gov.

Project Timeline

- January 16 - Begin accessibility initiative in collaboration with DoIT
- January 26 - Recite Me Tool was granted access to MLDSC; initial full-site scan completed with Assistance from DoIT. Baseline established - 1,502 issues across 146 pages.
- January 26 - March 19 - First remediation phase. Staff reviewed all 148 HTML pages and applied 596 individual fixes using WCAG 2.1 AA guidelines.
- March 19 - Recite Me Tool scan re-run - 98% accessibility rating and only 86 findings remaining.
- April -May - Second remediation phase. Targeted work on responsive-image markup, layout-table semantics, data-table cell associations, and HTML5 footnote anchor modernization. Standard upgraded from WCAG 2.1 to WCAG 2.2 Level AA.
- May 29 - Latest Recite Me scan completed; Overall rating 96%; Level A 95%, Level AA 98%.

[1] Web Content Accessibility Guidelines developed by the World Wide Web Consortium

Examples of Remediation Work Completed

- Semantic Markup (H49) — Legacy <font> and <div align> replaced with semantic HTML. This fixed Legacy meeting materials and info brief pages on the website.
- Image Alt Text (H37) — Alt attributes added to all PDF icon images. This fixed All Governing Board meeting materials pages.
- HTTP → HTTPS Links — all insecure links updated to HTTPS.
- Search Button Labelling — aria-label and .sr-only text added.
- Logo Alt Text — updated to a meaningful description.
- Accordion Section Labels. Changed the website format to remove the presentation content from accordion menus. This fixed Archive, Center Reports, Dashboards, Presentations, Published Research, Research & Reporting Summaries, Research Reports, Research Series, and External Research Reports etc.

Analysis of Remaining Issues

The remaining findings in the latest scan fall into a small number of categories. The vast majority are outside the MLDSC HTML codebase — either inside Power BI iframe content or on the Oracle Web Center portal. The Center plans to phase out use of the Oracle Webcenter content.

Next Steps

MLDSC will be sending the current results, PDF checklist and updated website to DoIT's Accessibility Specialist for review. Staff will also work on Power BI and other dashboards to ensure they are also accessible.

MLDSC Audit/Penetration Testing

Summary

The MLDS Center requested DoIT's assistance in obtaining a cybersecurity audit. DoIT along with Cyber Defence Technologies will conduct a comprehensive, multi-phase adversarial penetration test to evaluate the Maryland Longitudinal Data System (MLDS) Center's security posture from an external attacker's perspective. , using post-compromise internal analysis. This engagement emphasizes realistic threat actor behaviors and aligns with MLDS's requirement to complete an annual security assessment. This assessment will support the Center's mission of safeguarding statewide education and workforce data by identifying weaknesses across external assets, the internal network, cloud-hosted virtual desktop systems, user interactions, and the controls protecting sensitive database systems. The team will provide both technical and executive-level insights in prioritizing corrective actions and strategic improvements.

Phase 1 – Reconnaissance & External Attack Simulation

Phase 1 focuses on conducting an external reconnaissance and attack simulation to evaluate the Center's exposure from the perspective of a real-world threat actor. During this phase, the test team will perform a comprehensive enumeration of the organization's internet-facing assets, public web presence, DNS records, cloud endpoints, and any associated external services. Testing will include analysis of website components, add-ons, and configuration weaknesses, as well as an assessment of email security controls through a controlled phishing campaign designed to evaluate user susceptibility to credential harvesting or malicious content. The testers will attempt to identify entry points, vulnerabilities, or misconfigurations that could provide an attacker with an initial foothold into the MLDS environment. The objective of Phase 1 is to determine whether an adversary can gain unauthorized access or gather the information necessary to support further compromise.

Phase 2 – Assumed Breach Assessment

Phase 2 focuses on an assumed-breach scenario designed to evaluate the Center's internal security posture once an attacker has already obtained limited access, such as through compromised credentials or a low-privileged user account. In this phase, the test team conducts internal reconnaissance to map the environment, identify trust relationships, and analyze authentication mechanisms. Testing includes attempts to escalate privileges, harvest additional credentials, and move laterally across systems and network segments. The testers will evaluate the resilience of internal defenses, segmentation controls, and monitoring capabilities, and will then assess whether an adversary could reach sensitive systems, including MLDS's core database infrastructure. The objective of Phase 2 is to determine how far a compromise could realistically progress and to identify the key vulnerabilities and misconfigurations that enable deeper infiltration.

Phase 3 – Reporting, Analysis & Executive Review

In the final phase, the team will consolidate all findings, evidence, and attack paths into a comprehensive reporting package tailored to both technical and leadership audiences.

Final deliverables will include:

- Full technical penetration testing report
- Detailed vulnerabilities with evidence, severity scoring, and remediation steps
- Attack path diagrams (external → internal → objective)
- Business-focused executive summary
- Recommendations for strengthening security posture across identity, network, cloud, and end-user layers
- Optional board-level presentation of results and recommended priorities

Schedule

We are planning to implement this between June 2026 and August 2026.