COLERIDGE INITIATIVE

20 F Street NW, 7th Floor
Washington, DC, 20001 US
(929) 379 - 3239

Testimony on Maryland Senate Bill 56
Maryland Longitudinal Data System Center - External Data Sharing - Multistate Reporting - Authorization

To:	Chair Feldman, Vice Chair Kagan, and members of the Senate Committee on Education, Energy, and Environment
From:	Jonathan Mills, Vice President, Data Enclave Operations The Coleridge Initiative, Inc.
Date:	February 4, 2026
Position:	Favorable

Chair Feldman, Vice Chair Kagan, and members of the Senate Committee on Education, Energy, and Environment. Thank you for the opportunity to speak.

My name is Jonathan Mills, and I serve as Vice President of Data Enclave Operations at The Coleridge Initiative. We are a 501(c)(3) non-profit organization focused on working with government agencies to enable the effective, secure use of administrative data for evidence-based policymaking.

I am here today to talk about Coleridge's Initiative's Administrative Data Research Facility (ADRF), a FedRAMP-authorized, secure cloud-based data platform for government, researchers, and policymakers.[1]

About Coleridge Initiative

The Coleridge Initiative was founded in 2018 as a research effort within NYU focused on improving how administrative data is used for evidence-based policymaking. It was grounded in the idea that government administrative records—data collected in the course of running programs—hold tremendous public-policy value if they can be used responsibly and securely. In August 2020, Coleridge became a stand-alone, 501(c)(3) non-profit organization.

Coleridge's mission is to work with government agencies to enable the effective use of data for public decision-making. Coleridge has partnered with multiples state and federal agencies to achieve this goal by:

[1] FedRAMP (Federal Risk and Authorization Management Program) is a U.S. government–wide program that standardizes security assessment, authorization, and continuous monitoring for cloud services used by federal agencies, based on security standards established by the National Institute for Standards and Technology (NIST).

20 F Street NW, 7th Floor
Washington, DC, 20001 US
(929) 379 - 3239

- Building new technologies and tools that enable secure access to and sharing of confidential microdata
- Building comprehensive data systems
- Training agency staff to build capacity in modern data analytical skills
- Developing research and data products to communicate findings

Coleridge is supported by a blend of philanthropic investment, competitive grant funding, and state and federal service agreements.

The Power of Administrative Data

Senate Bill 56 would allow Maryland to share student and workforce data with authorized third-party data centers like Coleridge to allow for the examination of critical policy questions. Such data include state workforce and employment data, K12 education data, post-secondary completion data, etc.

These data offer the potential to answer important policy questions like:

- Do job-training or reskilling programs actually increase earnings over time?
- Which credentials or certifications lead to stable employment, not just initial placement?

These data are, however, sensitive. They are powerful for research purposes because they contain personally identifiable information (PII), which allows for linking different datasets to one another (e.g., K12 school records to postsecondary enrollment and completion). Thus, it is critical that data sharing is governed by strict data security and privacy standards. Under SB 56, third-party data centers must demonstrate they have rigorous security, use PII only for data matching, employ privacy techniques (e.g., data hashing), and report results in the aggregate, not at the individual level. Coleridge's Administrative Data Research Facility (ADRF) is an example of a secure data sharing platform that meets SB 56 requirements.

What is the ADRF?

The Administrative Data Research Facility (ADRF) is Coleridge's secure, FedRAMP-authorized cloud-based platform. It's a specialized, highly protected environment where approved researchers can safely use confidential government data to answer important policy questions that support communities. FedRAMP (Federal Risk and Authorization Management Program) is a U.S. government program that sets standardized security and authorization requirements for

20 F Street NW, 7th Floor
Washington, DC, 20001 US
(929) 379 - 3239

cloud systems used by federal agencies. FedRAMP-approved platforms must successfully pass rigorous independent audits and are continuously monitored to meet over 300 of the highest federal security requirements. For states, FedRAMP-authorized platforms offer a widely recognized security benchmark for handling sensitive but unclassified data and can reduce risk, due-diligence burden, and approval time when partnering with federal agencies or sharing data across jurisdictions.

The ADRF was created with support and guidance from key federal agencies, including the Census Bureau and the Office of Management and Budget, to ensure policymakers have strong evidence for their decisions. The ADRF's innovative approach to secure data access was recognized with a Government Innovation Award in 2018.

The ADRF is built on the "Five Safes" data security model. This is a framework used by governments worldwide to ensure that sensitive data is used safely and responsibly.

It covers five layers of protection.

- **Safe Projects**: Only agency-approved projects are hosted in the ADRF, with project environments isolated and access restricted to approved users who have signed agreements.
- **Safe People:** Only authorized, trained researchers who have signed the required agreements can access data. All their activity is monitored.
- **Safe Settings**: The platform provides secure, authorized methods for transferring sensitive agency micro-data (including Personally Identifiable Information) into the ADRF.
- **Safe Data**: Sensitive data is hashed before transmission to the ADRF, and data stewards monitor who is accessing their data, how it is being used, and the status of user agreements.
- **Safe Exports**: Unauthorized removal of any information from the secure environment is prevented.

Important Features of the ADRF

Coleridge works with existing government administrative data—such as education, workforce, and benefits records—allowing approved analysis in secure enclaves without broadly sharing the underlying data. The following sections provide information on how Coleridge accomplishes this through the ADRF.

20 F Street NW, 7th Floor
Washington, DC, 20001 US
(929) 379 - 3239

Secure Access through a FedRAMP Authorized Environment

Rather than sending copies of data to researchers:

- Data stays in a secure, isolated environment
- Researchers are granted approved, time-bound access
- Raw data never leaves the enclave
- Outputs undergo multistage disclosure reviews before release

These measures significantly reduce:

- Re-identification risk
- Unauthorized reuse
- Accidental disclosure

Strong Data Governance

Strong data governance is at the core of our approach. Coleridge emphasizes that technology alone is not sufficient by using approved protocols that facilitate an agency's data governance and oversight requirements.

Before anyone accesses data:

- Clear legal authority and data-use agreements are established
- Research questions must be approved by authorized data stewards
- Roles, responsibilities, and accountability are explicitly defined
- Agencies retain authority over who, why, and how data is used

This ensures:

- Agencies do not lose control
- Use is purpose-limited
- Decisions are defensible in audits or hearings

Approved Access for Approved Purposes

Only those individuals who are approved by data providers to access data can do so in the ADRF.

- Identifiable data is tightly restricted
- Most users work with de-identified or linked datasets[2]

[2] In collaboration with data curators and technology partners, the Coleridge Initiative developed ADRF Hasher, an application that agency collaborators can use to protect the privacy and confidentiality of their data prior to its transmission to ADRF. The application allows data providers to de-identify data containing personally identifiable or other sensitive information prior to ingestion by replacing sensitive fields with hashed values.

20 F Street NW, 7th Floor
Washington, DC, 20001 US
(929) 379 - 3239

- Access is limited to what is strictly necessary
- All activity is logged and auditable

Output Controls and Disclosure Review

Users are prevented from unauthorized removal of any information within the secure environment.

The ADRF requires:

- Review of results before export
- Checks for small cell sizes or indirect disclosure
- Approval workflows for publications or downloads

This ensures insights can be released without exposing individuals or sensitive programs.

Use Case: The Multi-State Postsecondary Report

The Multi-State Postsecondary Report (MSPSR) is a collaborative, secure dashboard tool developed by the Kentucky Center for Statistics (KYSTATS) with support from Coleridge Initiative and partner state agencies.[3] It originated to help post-secondary institutions located near state borders to be able to report on the workforce outcomes of their graduates. This reporting was previously difficult due to graduates moving and finding employment across state borders.

The MSPSR integrates linked administrative education and workforce data from multiple states within the Coleridge Initiative's ADRF. This provides comparative insights for policymakers and analysts.

Key features include:

- Cross-State Outcomes: Tracks employment and earnings of completers across participating states.
- Common Standards: Uses agreed-upon definitions for comparable analysis.
- Multi-State Scope: Expanded from Kentucky and Ohio to include Indiana, Tennessee, New Jersey, and Virginia.
- Interactive Dashboard: Allows data exploration by institution, credential, major, and demographic group for evidence-informed policymaking.

[3] More information on the Multi-State Postsecondary Report is available at: https://kystats.ky.gov/Latest/MSPSR

COLERIDGE INITIATIVE

20 F Street NW, 7th Floor
Washington, DC, 20001 US
(929) 379 - 3239

In essence, the MSPSR uses securely linked data to illuminate education-to-employment pathways and evaluate college and workforce outcomes across state lines.

Closing

In summary, Senate Bill 56 establishes a standardized process for external collaboration based on high-level security and privacy benchmarks. The legislation will allow the state to collaborate with third-party data centers, such as Coleridge's ADRF, that meet data security and privacy standards. Through these collaborations, the state can examine complex policy questions regarding education and workforce pathways while maintaining strict governance over its data. This approach ensures that individual privacy is protected through mandatory de-identification and aggregate reporting, allowing Maryland to gain actionable insights without compromising security or jurisdictional control.