Technology & Security Subcommittee Meeting Summary

June 16, 2020

This document provides a summary of key points that emerged over the course of a half-day meeting. More information about the meeting, including the materials, the PowerPoint, and a meeting recording are available at https://cadatasystem.wested.org/meeting-information/technology-security-subcommittee.

The June 2020 meeting had the following goals:

- Update on key decisions
- Share examples of security frameworks
- Develop recommendations for a base security framework
- Establish homework teams to write a draft security framework

The following representatives attended the meeting:

Formeka Dent, Antelope Valley Union High School District; Helen Norris, Association of Independent California Colleges and Universities; Jason Piccione, Bureau for Private Postsecondary Education; Barney Gomez & Daryl Lal, California Community College Chancellor's Office; Rodney Okamoto & Alan Nakahara, California Department of Education; Vitaliy Panych, Michele Robinson & Janet Buehler, California Department of Technology; Lloyd Indig, California Health and Human Services Agency; Karissa Vidamo, California Department of Social Services; Ed Sullivan, California State University; Amy Fong & Greg Scull, California School Information Services; Gurinder Bains, California Student Aid Commission; Dan Lamoree, Educational Results Partnership; Todd Ibbotson, Employment Development Department; Douglas Leone, Labor and Workforce Development Agency; Jenni Abbott, Modesto Junior College; and Chris Furgiuele, Matthew Linzer & Hooman Pejman, University of California Office of the President

Key Decisions and Framework

The meeting opened with the facilitator providing an update on the Master Data Management (MDM) Request for Proposal, work being done by other subcommittees, decisions made by the Cradle-to-Career Workgroup at the May 30 meeting, and the proposed legal and technical framework for the data system.

One subcommittee member asked for information about federal policies regarding using unemployment insurance data in the state data system. The facilitators clarified that the requirements could be addressed in the payment policy and provided the following resource, which describes the joint U.S. Department of Education and Workforce Innovation and Opportunity Act guidance: https://www2.ed.gov/policy/gen/guid/fpco/pdf/final-ferpa-tegl-report.pdf

Another requested that a visual diagram of the technical structure be provided. WestEd will provide a document by the July subcommittee meeting.

Finally, one participant noted that the use of color coding in the framework document to connote the level of deidentification does not work for black-and-white printing and requested that the levels be more clearly described in writing as well.

Security Frameworks

Baron Rodriguez from WestEd described core attributes of commonly used security standards, followed by presentations by the University of California (UC) and the California Department of Technology (CDT) about their security frameworks.

The notes below reflect both small group breakouts based on segment (K-12, postsecondary, and other data types) and a full group discussion on a possible security framework.

Some members of the group felt that it would be difficult to adopt the National Institute of Standards and Technology (NIST) framework because the requirements are more stringent than could reasonably be implemented by the entities contributing data to the system. For example, NIST requires rigorous and frequent external reviews. Many entities are working with legacy systems that cannot be upgraded to meet the federal standards. Furthermore, some participants reported that cloud-based providers have been unable to meet NIST Federal Risk and Authorization Management Program (FedRAMP) requirements. Finally, NIST is designed to protect some types of data—such as credit card information—that will not be included in the state data system. Therefore, while it will be important to include and budget for external security reviews to ensure the data system is protecting individuals' data, the process should be aligned to the specifics of the Cradle-to-Career Data System. Participants were encouraged by the UC and CDT examples that demonstrated how policies can be adapted.

Some participants were comfortable with adapting the NIST Cyber Security Framework (CSF). Others recommended using the International Organization for Standardization (ISO) framework. However, another noted that Health Insurance Portability and Accountability Act (HIPAA) requires standards more like NIST. Furthermore, CDT uses NIST, which should establish the standards for a state data product. One way to address this issue is to crosswalk requirements across frameworks. UC has already developed this type of crosswalk, which could be referenced for developing the state data system policy.

Another option would be to adopt the framework that best fits the specific data being provided for the use case, with the goal of adopting the more conservative relevant standard. For example, if the data sets only include education information, ISO could be applied. If the set includes both education and social service data, NIST could be applied. Subcommittee members requested the most current list of proposed data elements for the dashboards and query tools to help them better evaluate the options.

Baron Rodriguez clarified that the security policy will only apply once data are loaded into the state data system and while it is being stored within the system, so local entities would not have to conform to the security framework. However, one way to safeguard the data would be to have researchers access deidentified unitary information from within a secure environment that meets the state data system standards, rather than sending data files outside of the system. One participant noted that this approach would help to ensure that smaller, less well-resourced entities could access the data while keeping it secure.

Another participant raised a concern about the managing entity being able to access identified unitary data and wondered if the partner entities could provide deidentified data or if matching could be done by each contributing partner entity. Baron Rodriguez clarified that the proposed model would only have the Employment Development Department doing its own match (which would be based solely on social security numbers), and that the MDM solution had been recommended as the matching mechanism earlier in the planning process.

Finally, the group raised broader governance issues that should be addressed, such as the specific protocols for managing data breeches, ensuring that only appropriate data are loaded into the state data system, addressing issues of data quality provided by local institutions to the partner entities, providing training on the standard being used to help improve local security practices, and establishing policies on data access and deidentification.

After clarifying that the recommendation specifies using existing standards rather than creating new standards, the group voted unanimously to approve the following statement:

> **Develop an information security standard based on NIST or ISO 27001, and tailor it specifically to the Cradle-to-Career system, based on the data source.**

Next Steps

- Subcommittee members will receive meeting notes by June 19 and should provide comments by June 26.
- Subcommittee members were urged to discuss the legal and technical framework with their agency representative in advance of the June 30 Cradle-to-Career Workgroup meeting, as the partner entities will be voting on whether to move forward with this framework.
- Subcommittee members volunteered for two homework teams:
  - *Security Framework*: Greg Scull, CSIS; Helen Norris, AICCU; Lloyd Indig, CHHS; Michele Robinson, CDT
  - *MDM RFI Evaluation*: Helen Norris; AICCU; Jenni Abbott, Modesto Junior College; Michele Robinson, CDT