California Cradle-to-Career Workgroup Meeting Summary

June 17, 2021

The California Cradle-to-Career Data System Workgroup, which is comprised of partner entities named in the authorizing legislation, provides recommendations to the Governor's Office regarding data system development.

This document provides a summary of the key points that emerged from substantive discussion over the course of the June 17, 2021 Workgroup meeting. More information about the meeting, including support materials, a recording of the meeting, and the PowerPoint, are available at https://cadatasystem.wested.org/meeting-information/Workgroup (click on "Meeting Materials").

The following Workgroup representatives attended the meeting:

Thomas Vu, Association of Independent California Colleges and Universities; Leeza Rifredi, Bureau for Private Postsecondary Education; John Hetts, California Community College Chancellor's Office; Mary Nicely, Sarah Neville-Morgan, and Cindy Kazanis, California Department of Education; Brenda Bridges Cruz and Tim Murphy, California Department of Technology; Natasha Nicolai, California Department of Social Services; Elaine Skordakis, California Health and Human Services Agency; Amy Fong and Greg Scull, California School Information Services; Ed Sullivan, California State University; Patrick Perry, California Student Aid Commission; Amy Faulkner, Employment Development Department; Joy Bonaguro, GovOps; Amy Faulkner for Jeanne Wolfe, Labor and Workforce Development Agency; Sara Pietrowski, State Board of Education; Chris Furgiuele, University of California Office of the President

Celebration

The meeting began with celebrating the hard work of the workgroup over the past 18 months, including sharing favorite memories from the planning process.

Updates

Project Approval Lifecycle Process

Kathy Booth of WestEd described a recent meeting with CDT about the Project Approval Lifecycle (PAL) process. CDT indicated that the workgroup had already completed most of the tasks necessary for both phase one and phase two. WestEd will now commence with filling out the related forms.

Legislative Process

Chris Ferguson from the Department of Finance (DOF) noted that funding for the Cradle-to-Career Data System was included in legislature's version of the 2021-22 budget. However, work is still proceeding on the trailer bill.

Indemnification

Chris Ferguson of also addressed questions regarding indemnification that had been raised in the Legal Subcommittee. Some partner entities have requested that language be included in the trailer bill that indemnifies the data providers related to costs and responsibilities associated with data breaches. However, DOF cannot support the inclusion of this language for several reasons. First, many of the data providers are state agencies, which would mean that the state would be indemnifying itself against itself. Second, in reviewing data systems in other states, indemnification is not a practice that has been adopted to address cybersecurity risks. DOF recommends that, in the event that the data providers incur

legal costs associated with a breach, they should use the established practice of a Budget Change Proposal to cover those costs. However, given the mitigation efforts that have been outlined in the privacy and security recommendations, it is highly unlikely that the data providers would incur such costs.

Ben Chida of the Governor's Office paused to acknowledge the productive and collaborative approach that the workgroup has taken to problem solving, which is how the planning process has been able to develop recommendations on so many topics that were stymied in prior efforts. The recommendations also go further than prior efforts because they simultaneously serve students and families, share out research findings, improve data quality, and use a streamlined technology approach.

Then, Ben Chida of the Governor's Office addressed the indemnity issue, noting that privacy and security was one of the central requirements for the data system. Even with the extensive security protocols that have been proposed, it is appropriate for the partner entities to raise issues of liability, particularly related to costs. Recent experiences, both in the broader public and among the partner entities, have shown that cybersecurity is a pressing issue. However, it is not a reason to halt the development of the data system. He noted that the data system will generate many benefits for the common good, so the partner entities should continue to use their problem-solving skills to identify a way forward. If other states have been able to build intersegmental data systems without indemnifying data providers, despite the risk of breach, then California can too.

Chris Ferguson of DOF noted that it would not be appropriate to include indemnification in the Cradle-to-Career Data System legal agreements because doing so would require the legislature to appropriate funding for future years. This should not be implemented using legal contracts and should instead be done through established budgetary processes.

Mike Arakji of the Department of General Services (DGS), who serves as the information security officer for GovOps, highlighted that with appropriate protocols in place—as will be the case for the Cradle-to-Career Data System—any breaches would be the result of individuals failing to comply with established policies and protocols. He reminded the group that any vendors selected to implement the data system will need to comply with security requirements that will be spelled out in the request for proposals. He also noted that GovOps could procure cybersecurity liability insurance and establish requirements that its contractors implement the recommended security practices for that insurance. To ensure that GovOps would be able to secure such a policy, he compared the policies recommended by the workgroup against checklists of recommended practices from cybersecurity insurance providers. He found that most required practices have already been addressed.

Tom Vu of AICCU asked whether the state would assist independent colleges participating in the data system with breach-related costs and if AICCU members could be covered under GovOps' cybersecurity insurance policy.

Chris Ferguson of DOF indicated that AICCU could work with BPPE and DOF to identify possible solutions related to costs. He also suggested that GovOps look into whether cybersecurity insurance policies can be extended to data providers.

Chris Furgiuele of UC asked for clarification—is the intention to not address indemnification in either the trailer bill or the legal documents, and rather to wait until the point of a breach to address the concern? And if so, are there any written policies regarding seeking funding to cover breach costs?

Chris Ferguson of DOF indicated that a decision to provide indemnification among data providers for this project would have implications for other statewide linked data sets. Any solution should be crafted in this broader context. However, indemnification language could be used in the legal agreements with third parties, such as those going through the data request process. For the issue of funding, a Budget Change Proposal, specifically section 9840 on unanticipated costs, is the appropriate vehicle. These proposals can be submitted at any point. There is precedent for covering legal costs through this mechanism.

Ed Sullivan of CSU shared that his agency's information security officer estimated that the cost of a breach for CSU would be $1 billion. Given the size of the overall data system, GovOp's cost for a breach could be $10 billion. He expressed deep concern that if CSU was expected to bear their share of these costs, it would result in a reduction of services to students.

Baron Rodriguez of WestEd, who formerly worked with the U.S. Department of Education's Privacy Technical Assistance Center, noted that figures of this magnitude are normally associated with breaches of financial information, not educational information.

Ed Sullivan of CSU noted that the figure was based on the Ponemon Institute, which is considered the *de facto* authority on the cost per record of a breach to an institution. These costs encompass the effort to investigate, remediate, notify, and provide credit monitoring. The low water mark is $145 per record and extends to $225 at the upper end if a compromised record includes healthcare information. The $1 billion number was derived from the CSU providing records on 9 million individuals.

Baron Rodriguez of WestEd underscored that this figure relates to financial data, which is subject to more stringent laws than education data. He also noted that in the event of a breach, a large share of the people affected do not utilize the offered services—in his experience, the uptake is between 30-50%. Finally, he pointed out that heath and employment data are far more sensitive than education data, but EDD and CHHS have not expressed concerns about the breach risk.

Joy Bonaguro of GovOps suggested it would be helpful to estimate costs based on historical examples of costs associated with HIPAA disclosures.

Patrick Perry of CSAC reported that Ponemon Institute estimated that in 2020, the cost of education data breaches was about $4 million per incident.

Chris Ferguson of DOF asked how CSU is currently mitigating the risk on its existing records.

Ed Sullivan of CSU noted that his organization had strict data access controls and holds cybersecurity insurance.

Joy Bonaguro of GovOps highlighted the importance of strict access controls, but reflected that it is impossible to reduce the risk to zero. Risk must be weighed against the associated value of the data system. There is also a risk to students of not linking data sets, because without the data system, it will be difficult to understand longer-term and cross-segmental impacts of agency-specific actions. She also noted that if the proposed security requirements exceed those of many data providers, that should also factor into the risk analysis.

Kathy Booth of WestEd noted that notification and credit monitoring costs would be covered by cybersecurity insurance.

Cindy Kazanis of CDE asked whether GovOps was required to have cybersecurity insurance in the trailer bill and if the cost of cybersecurity insurance was included in the first-year budget for the data system.

Chris Ferguson of DOF noted that this provision is not currently in the trailer bill, but that DOF expected cybersecurity insurance to be covered by the budget. He also stated that Civil Code section 1798.29 establishes a breach notification requirement when the state houses data, whether or not it owns that data. This should help to address the liability concerns raised by the partner entities.

Ben Chida of the Governor's Office underscored the value of a risk/benefit analysis. California is one of the few remaining states that has not linked its data to yield insights that will improve public investments. There is a cost to being unwilling to share data due to a potential risk.

Chris Furgiuele of UC reflected that this analysis of risk and reward focuses only on the risks to the state, not to the data providers. If the data providers will be expected to provide funding on the order of a billion dollars, participation is an enormous risk. Furthermore, the data providers will bear a reputational cost. If information that is not under the data provider's control is breached, it could have a chilling effect on students' willingness to share their information with the data providers. This will in turn affect what information the partner entities are willing to put into the data system.

Ben Chida of the Governor's Office noted that indemnification would not address reputational risk. He encouraged the partner entities to resume their focus on student benefits, rather than focusing on agency-specific interests.

Ed Sullivan of CSU countered that his concerns are grounded in student impacts—if the data providers have to redirect their resources to breach-related expenses, the quality of the education that students receive will suffer.

Chris Ferguson of DOF noted that a scenario where data providers are spending enormous amounts on breach responses is unlikely given the proposed cybersecurity insurance policy, paired with strong security policies and protocols and an established process for recouping breach costs through the Budget Change Proposal process.

Kathy Booth of WestEd walked through the policies and procedures that had been recommended by the workgroup and outlined how they met or exceeded policies in place at the partner entities. She reminded the group that these policies and procedures had been developed and approved by information security experts from the partner entities, working with national experts. Members of the workgroup had no questions about these policies.

Legal Documents

Marion McWilliams of WestEd reflected on the collaborative spirit and level of commitment shown by the attorneys from the partner entities to develop shared agreements. Then she described the three types of legal documents under development:

- the Participation Agreement (PA), which will establish terms between the data providers and GovOps
- the third party library, which that will establish terms between individual data providers, GovOps, and third parties granted access to information through the data request process

- the Master Data Exchange Agreement (MDEA) and Business Use Case Proposal (BUCP), which will be used to allow data providers and institutional members of the governing board to share information from the P20W data set with each other for agreed-upon purposes

The workgroup had no questions about the proposed set of agreements.

Marion McWilliams of WestEd noted that the PA is very close to complete, outside the questions of cybersecurity insurance and indemnification. The third party library will not be finalized until after the secure data enclave is developed, to ensure that each agreement appropriately addresses security considerations. The MDEA/BUCP only needs to have a final review related to the inclusion of more comprehensive documentation related to health information.

Kathy Booth of WestEd clarified that the Legal Subcommittee will be meeting on June 29 to try to finalize the PA, MDEA, and BUCP. The workgroup will need to decide how the recommendations from the Legal Subcommittee should be included in the final report, given that the workgroup will not have time to meet again before the June 30 deadline.

Ed Sullivan of CSU indicated that if all members of the Legal Subcommittee were comfortable with each document, then he would be willing to delegate the recommendation to them. However, if even one attorney still had concerns, then he would not want the documents to be considered recommendations. He would not want his organization to be forced to sign a document, just because a majority of the attorneys on the subcommittee were comfortable with it.

Joy Bonaguro of GovOps recommended that if any of the attorneys have concerns, those concerns should be documented and forwarded to the leadership of their organization for consideration—their opinions should inform the decision of their agency but that attorneys do not make final determinations. This is also true for issues of cybersecurity. Generally, a senior executive is charged with creating a document that lays out the risk to the organization and then the leadership determines whether that risk is acceptable or not.

Kathy Booth of WestEd suggested that the meeting notes be used to document the concerns of each attorney.

VOTE ON LEGAL DOCUMENTS

Almost all workgroup members voted to approve the following:

If the Legal Subcommittee agrees unanimously to endorse the legal documents on June 29, the workgroup also endorses the documents. In cases where any legal representative does not endorse any legal document, the partner entity will go on record in the subcommittee meeting notes with the specific legal concerns and provide a risk assessment to inform each entity's decision about whether to sign the documents.

Cindy Kazanis of CDE agreed with reservations because her agency's attorney was not present to weigh in on the proposal.

Breach Mitigation

The workgroup discussed whether to recommend that GovOps secure cybersecurity insurance and proactively put in place procedures recommended by cybersecurity insurers.

Elaine Skordakis of CHHS felt that the existing data security framework already addressed best practices, and so taking the extra step of asking GovOps to follow procedures recommended by cybersecurity insurance providers may not be necessary.

Ed Sullivan of CSU asked whether GovOps' cybersecurity insurance would provide coverage to the data providers.

Kathy Booth of WestEd indicated that the entity that secures cybersecurity insurance for the state had told the planning team that this is not normally covered. However, this question could be asked of potential insurers.

Chris Furgiuele of UC asked for clarification about limitations of the insurance policy related to the stage of the data within the data system—for example, would it be covered when being uploaded by the data providers, stored in the provider-specific cloud repositories that can be accessed by both data providers and GovOps, matched in the master data management solution, or compiled into the deidentified P20W data set?

Mike Arakji of DGS clarified that the data would be covered in all of these stages because it would be considered under the control of GovOps (even when the control is shared during the upload and when in the provider-specific cloud repositories). However, the policy would not cover information when it is in the data providers' source data systems, before it is transmitted to GovOps. He also clarified that coverage for a similar system is about $5 million per year.

Ed Sullivan of CSU noted that the lawyer from GovOps indicated that agencies would be responsible for lawsuit and breach costs if GovOps caused a breach or were breached.

Joy Bonaguro of GovOps asked whether the data providers carry cybersecurity insurance.

Ed Sullivan of CSU shared that his agency had cybersecurity insurance.

Chris Furgiuele of UC asked whether the PA would include a requirement that GovOps get cybersecurity insurance.

Marion McWilliams of WestEd indicated that this provision was under discussion, but the concern was that this item may not belong in a legal agreement because it is a budgetary issue. However, if the workgroup recommends that cybersecurity insurance be required, the attorneys can craft appropriate language.

VOTE: CYBERSECURITY INSURANCE

The majority of the group recommended that GovOps must be required to have cybersecurity insurance and proactively implement the best practice security processes and procedures found on cybersecurity insurance checklists.

Tom Vu of AICCU, Ed Sullivan of CSU, and Chris Furgiuele of UC voted yes with reservations because they were concerned this approach would not be sufficient to address the cost of data breaches to the data providers.

Joy Bonaguro of GovOps abstained.

VOTE: WORKGROUP ON BREACHES IN LINKED DATA SETS

Most of the workgroup recommended that the Governor's Office convene a workgroup to determine how to handle breach responsibilities and costs for linked data sets.

Ed Sullivan of CSU voted yes with reservations because he felt that breach responsibilities needed to be handled in the Cradle-to-Career Data System legal agreements.

Chris Furgiuele of UC voted yes with reservations because he felt there were too many dependencies to know if this workgroup would be helpful to address his organization's concerns.

Incident Response Policy and Plan

Kathy Booth of WestEd described the origins of the incident response policy and plan and how they had been amended by both the Technology & Security and Legal Subcommittees.

Mike Arakji of DGS underscored the comprehensiveness of the approach, including providing incident response procedures that are tailored to each data provider. The document meets the requirements laid out in checklists provided by cybersecurity insurance carriers to evaluate risk and conforms to practices mandated by external auditors such as CDT's Office of Information Security. Finally, he reminded the group that this document would be amended each year to keep pace with cybersecurity developments.

Chris Furgiuele of UC asked who would do the notification in the event of a breach.

Mike Arakji of DGS noted that this would be GovOp's responsibility. However, as is the case at DGS, they might hire a company to handle breach notifications.

Chris Furgiuele of UC asked how GovOps would know who to contact about data breaches in the combined P20W data set, given that similar information might come from multiple data providers or it might be unclear who caused a breach.

Mike Arakji of DGS clarified that GovOps will have tools that allow them to know the source of each data point and also how each entity that has had access to the data set interacted with each data point.

VOTE: INCIDENT RESPONSE PLAN AND POLICY

The workgroup voted nearly unanimously to adopt the incident response policy and plan, understanding that they will be updated in fall 2021 and regularly by the governing board based on advice from an ad hoc committee.

Chris Furgiuele of UC abstained.

Permission Protocol

Kathy Booth of WestEd described modifications made by a homework team to the protocol that had been initially discussed at the March workgroup meeting, including clarifying that the document refers to data repositories associated with the P20W data set and noting that parents would not have access to the underlying P20W data set. The homework team also recommended postponing the inclusion of a chart that lays out responsibilities related to permissions until after the liability issues are resolved.

VOTE: PERMISSION PROTOCOL

The workgroup voted unanimously to adopt the revised permissions protocol, with the understanding that it will be updated in the fall with roles and responsibilities.

Advisory Group Input

Kathy Booth of WestEd reported that members of the two advisory groups were supportive of the policies that were adopted by the workgroup in the May and June meetings. They also have provided ideas for ways they can support community outreach once the data system is under development.

Final Legislative Report

Kathy Booth of WestEd noted that she will send out the draft report later in the day, which will include alternate language in the case that 1) the Legal Subcommittee unanimously finalizes the legal agreements or 2) describes the status of the legal agreement development if there is not a unanimous opinion. Workgroup members have until June 23 to provide comments. The document will be submitted to the Legislature on June 30.

Employment and Earnings

Kathy Booth of WestEd noted that EDD had determined that the "location of employment" data point should be removed from the P20W list, given that half of the information in the wage file come from payroll services, which means that addresses are highly unlikely to represent where individuals are employed.

She also reminded the workgroup that volunteers are needed for a homework team that will meet over the summer to work on an evidence-based calculation for annual earnings and related data points.

Governing Board

Workgroup members that will be data providers were asked to contact WestEd with their agency's nomination for the governing board, so that WestEd can schedule meetings to provide background on the data system. They should also send official notification to Ben Chida at the Governor's Office by June 25.

Thank You

The meeting closed with a picture of the workgroup members and gratitude to all who participated in the planning process.