

# Legal Subcommittee Meeting Summary

June 9, 2021

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

The June 9, 2021 meeting had the following goals:

- Provide updates on the planning process
- Finalize the following items:
  - Participation Agreement
  - Master Data Exchange Agreement/Business Use Case Proposal
  - Incident Response Plan
- Determine how to finalize the third party legal agreement library

The following representatives attended the meeting:

Veronica Villalobos Cruz and Thomas Vu, Association for Independent California Colleges and Universities; Linh Nguyen, California Commission on Teacher Credentialing; Kathy Lynch, California Community College Chancellor's Office; Bruce Yonehiro, California Department of Education; Marina Feehan and Mike Arakji, California Department of General Services; Kary Marshall, California Department of Technology; Cynthia (Cyndi) Bosco and Margaret Porto, California Department of Health Care Services; Carolyn Kubish, California Department of Social Services; Jennifer Schwartz, California Health and Human Services Agency; Rima Mendez, California School Information Services; Ed Hudson, Ed Sullivan, Monique Shay, and John Walsh, California State University; Julia Blair, California Student Aid Commission; Kristine Beckley & Rebekah Gibson, GovOps; Jeanne Wolfe, Labor and Workforce Development Agency; and Stella Ngai, Chris Furgiele, and Matthew Linzer, University of California, Office of the President.

## Participation Agreement

Marion McWilliams of WestEd provided an overview of changes that had been made to the Participation Agreement (PA) by a homework team. There were two primary areas of work. First, the draft was edited to include technical and security provisions from the State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM), with support from security experts Matt Linzer of UC and Mike Arakji from DGS. Second, the text was streamlined to remove redundancy. Some partner entities subsequently provided comments on the draft, most of which are non-controversial and easy to incorporate. However, some agencies had yet to provide their feedback.

Kathy Booth of WestEd addressed the issue of including indemnification language, which had been raised at the previous meeting. At issue is that some attorneys felt that state policy prevents state agencies from indemnifying each other or third parties.

Stella Ngai of UC noted that Bruce Yonehiro of CDE had shared the code section that allows for indemnification between state agencies.

Kathy Booth of WestEd indicated that this approach does not align with the SAM. Including indemnification language in the PA could have implications for other state policies. She suggested that the group identify if there are other ways to address the underlying issues of cost and responsibility.

Chris Furgiuele of UC asked if the issue could be solved by including language in the trailer bill that allows for indemnification for the Cradle-to-Career Data System. He noted that his agency was currently in conversation with Chris Ferguson at the Department of Finance. UC will not be able to approve the PA until these negotiations are complete. Veronica Villalobos of AICCU and Ed Sullivan of CSU concurred.

Kathy Booth of WestEd noted that at the last meeting, the subcommittee had expressed interest in requiring GovOps to secure cybersecurity insurance as another potential solution. WestEd met with the state entity that procures such insurance and learned the following:

- Policies generally cover the costs of notifications, credit monitoring, and ransom
- Coverage is only for the named insured, however, it is unlikely that the data providers would be held liable unless they were responsible for the breach
- It will not be possible to estimate the full costs of coverage until GovOps is further in the implementation process because it will be dependent on how the technical systems are set up

She noted that the subcommittee could recommend that GovOps work from criteria used by insurers to assess risk to ensure its systems would be sufficient to secure coverage and minimize costs.

Stella Ngai of UC felt that this solution requires more review, particularly given that it does not address the possibility that data providers could be sued.

Bruce Yonehiro of CDE agreed, expressing concern that his agency would have to bear the cost of defending cases, including having to prove whether or not CDE was negligent. In his experience, the risk of CDE being found negligent would be minimal and he believed that insurers would agree—therefore the cost of covering data providers should be affordable. GovOps should be required to name both themselves and the data providers on the policy.

Kathy Booth of WestEd asked what level of risk would be acceptable for the data providers, given that it is impossible to fully protect against data breaches.

Bruce Yonehiro of CDE stated that it would be unreasonable to expect the partner entities to provide data if the managing entity could not obtain adequate protection—which is best accomplished by providing complete indemnity to the data providers. All risk and costs should be borne by GovOps.

Chris Furgiuele of UC concurred, and argued that it should not be left up to each partner entity to determine the appropriate level of risk, as this might result in some deciding not to participate. Tom Vu of AICCU agreed.

Julia Blair of CSAC suggested that this issue might be more appropriate for the government relations staff at the partner entities.

Stella Ngai of UC agreed, and noted that they are actively in discussion with the Department of Finance to try to find a solution.

Jeanne Wolfe of CLWDA suggested that one solution would be to have GovOps form a joint powers authority (JPA), which would allow the agencies to indemnify each other without having to change current statute.

Kathy Booth of WestEd responded that a JPA had been discussed when the type managing entity was being chosen, but the workgroup had not elected to pursue this approach.

Rebekah Gibson of GovOps wondered if a set of requirements could be established for her agency related to security protocols.

Kathy Booth of WestEd clarified that the workgroup had already recommended an extensive set of requirements that drew from state and federal requirements as well as best practices from other data systems. Many of these standards exceed those in place at the data providers. The workgroup could recommend that these requirements be cross-walked against cybersecurity insurance requirements.

Kathy Booth of WestEd further reflected that cybersecurity is becoming more urgent and wondered if it would be appropriate to raise this issue to a higher level. For example, a workgroup could be formed that includes experts from the Attorney General's office and other state experts to craft a policy that would work in contexts beyond the Cradle-to-Career Data System.

Jennifer Schwartz of CHHS wondered why risk for the Cradle-to-Career Data System would be different than other data sharing agreements. For example, currently, Medi-Cal shares data with CDE and UC, which entails accepting some risk. However, the risk should be worth it because of the benefits that the data system would provide.

Stella Ngai of UC agreed that her organization wants to use linked data to improve their work and understands that most things come with risk. However, UC is concerned about the potential fiscal costs—they do not have the budget to underwrite data breaches and lawsuits that stem from the Cradle-to-Career Data System.

Rebekah Gibson of GovOps thought that the issue of indemnifying third parties would be problematic. Bruce Yonehiro of CDE agreed, citing Gov Code 894.5, which he felt would not allow GovOps to indemnify independent colleges. He shared the code text:

[Government Code 895.4.](#)

*As part of any agreement, the public entities may provide for contribution or indemnification by any or all of the public entities that are parties to the agreement upon any liability arising out of the performance of the agreement.*

*(Added by Stats. 1963, Ch. 1681.)*

Jeanne Wolfe of CLWDA speculated that this code is only applicable to JPAs, based on earlier language in section 895.

Bruce Yonehiro of CDE indicated that he understood the code to be allowable in a broader range of cases and noted that indemnification language is standard in his agency's data agreements.

Marina Feehan of DGS shared the language from Government Code 895:

*As used in this chapter "agreement" means a joint powers agreement entered into pursuant to Chapter 5 (commencing with Section 6500) of Division 7 of Title 1 of the Government Code, an agreement to transfer the functions of a public entity or an employee thereof to another public entity pursuant to Part 2 (commencing with Section 51300) of Division 1 of Title 5 of the Government Code, and any other agreement under which a public entity undertakes to perform any function, service or act with or for any other public entity or employee thereof with its*

*consent, whether such agreement is expressed by resolution, contract, ordinance or in any other manner provided by law; but "agreement" does not include an agreement between public entities which is designed to implement the disbursement or subvention of public funds from one of the public entities to the other, whether or not it provides standards or controls governing the expenditure of such funds.*

*(Added by Stats. 1963, Ch. 1681.)*

Bruce Yonehiro of CDE asserted that the PA meets the definition of an agreement in Government Code 895, because it expressly provides that GovOps is "performing institutional functions" for data providers, i.e., "transferring functions of a public agency."

Julia Blair of CSAC worried that some of the proposed legal agreements, such as the Master Data Exchange Agreement (MDEA) and Business Use Case Proposals (BUCP)—which include non-state agencies such as AICCU—would not be covered by this code.

Bruce Yonehiro of CDE suggested that one way to provide protections would be to include language in the PA that states GovOps shall indemnify the data providers to the extent allowed by Government Code 895.4. He agreed to create draft language for others to review, building on language that was being circulated among many of the education-related partner entities.

Tom Vu of AICCU noted that the solution had to cover nonprofit colleges and universities in addition to state agencies. In the future it may also need to cover other private entities such as day care providers.

Rebekah Gibson of GovOps noted that she would take back the proposed language and consider whether an indemnification clause would address the issue of liability, such as litigation costs.

Bruce Yonehiro of CDE stated that his understanding is that having a cybersecurity insurance policy would mean that the insurer would be responsible for defense costs of a lawsuit, particularly if an indemnity clause in the PA makes GovOps liable.

Rebekah Gibson of GovOps responded that this depends on the scope of the policy. She wondered if the issue was too big to resolve in this subcommittee. However, she noted her commitment to try to find a way to address the partner entities' concerns.

Stella Ngai of UC indicated that it would be hard to finalize the PA before the final workgroup meeting on June 17, particularly given the ongoing negotiations about the trailer bill language. Her colleague Chris Furgiuele underscored that UC would be unwilling to approve an agreement that did not include indemnification. Tom Vu of AICCU agreed.

Tom Vu of AICCU asked for clarification on the difference between limited liability and indemnity.

Marion McWilliams of WestEd explained that a limited liability provision would be an agreement that caps liability between the parties, such as between an independent college and GovOps in the event of a breach. This would help to address direct costs that an independent college might have, such as supporting notifications to breached parties. But limited liability does not help in cases where there are claims from third parties. For example, a third party like a student might sue an independent college to recoup damages after a breach. Indemnification (if it were legal) would mean that GovOps would cover the costs of the independent college's liability.

Bruce Yonehiro of CDE asked why indemnification can't be provided to private institutions.

Rebekah Gibson of GovOps referenced the provision on gifts of public funds. Julia Blair of CSAC agreed.

Although there was not a consensus on the indemnification question, the subcommittee members agreed to review the remainder of the PA. Marion McWilliams of WestEd volunteered to create a clean draft that incorporates comments from the group. Subcommittee members were given until June 14 to send their comments. WestEd will send out the revised version on June 15, and subcommittee members will provide additional comments by June 28 at 9am. The subcommittee also agreed to hold another meeting on June 29 to try to finalize the PA and any other remaining legal documents.

### Third Party Agreements

Kathy Booth of WestEd reminded the group that they had planned to prepare four templates that would be used for approved data requests with entities that are not data providers or institutional members of the governing board. The templates would be based on the two relevant FERPA exemptions, the HIPAA business associate agreement, and allowable use of financial aid data under the Higher Education Act (HEA). WestEd had gathered templates already used by the partner entities that address these allowable uses. She proposed that WestEd align these templates with language from the PA and MDEA/BUCP and send them out to the subcommittee for review at the June 29 meeting.

Julia Blaire of CSAC noted that for financial aid data, some data points required FERPA exceptions, while others require the HEA language. She wondered how a single template could be used if the requested data points also included health information that required the business associate language.

Bruce Yonehiro of CDE thought that it would be preferable to create templates that are specific to agencies rather than by allowable use exemptions. That way, the templates could be kept up to date to address evolving requirements from the data providers. Stella Ngai of UC concurred.

Bruce Yonehiro of CDE noted that one of the factors that slows down data sharing agreements is the requestor wanting to negotiate portions of the agreement, or having difficulty clearly describing their research question and determining the appropriate data points to request.

Kathy Booth of WestEd reminded the group that the data request process already approved by the workgroup had several provisions to address these common sticking points, such as forcing requestors to pick from a list of data points in the P20W data set and GovOps playing a role in helping the requestors to craft coherent proposals. The subcommittee could also recommend provisions like requiring the requestor to use the template—no negotiation allowed.

Rebekah Gibson of GovOps was concerned that foreclosing negotiation could be overly limiting.

Jeanne Wolfe of CLWDA wondered who would be responsible for keeping the library of data provider-specific templates up to date and ensuring that they comply with the law.

Kathy Booth of WestEd noted that the managing entity responsibilities include tasks like working proactively with data providers to document changes that would affect information in the system. For example, GovOps will need to reach out each year to determine whether there have been changes in underlying data sets or definitions that could affect the information in the dashboards. It will also need to regularly update contact information for policies like the incident response plan. Checking on legal templates, and ensuring that the data provider agrees that they are correctly constructed, could be another responsibility for the managing entity.

Marion McWilliams of WestEd noted that it may not be possible to edit the templates until the specifics of the secure data enclave are determined. For example, the templates provided by the partner entities include extensive provisions based on an assumption that the requestor will take possession of the data, which would not be relevant. The examples also don't include a third party (GovOps) providing access to the data.

Chris Furgiuele of UC agreed that it would be important to make these adjustments, which will greatly streamline the agreement forms. Bruce Yonehiro of CDE concurred.

Chris Furgiuele of UC further suggested that when implemented, the requestor should sign separate agreements with each data provider, rather than trying to create a single legal agreement that includes all data providers. Jennifer Schwartz of CHHS clarified that these agreements would need to be created at the department, as opposed to agency, level. For example, there may need to be separate agreements for DHCS and CDSS because different requirements might apply based on the types of data each collects. The full subcommittee endorsed this approach.

### MDEA/BUCP

Marion McWilliams of WestEd reminded the group that the MDEA would only be used when sharing P20W data between the data providers and institutional board members for purposes beyond the Cradle-to-Career Data System tools. The BUCP specifies data terms and conditions for each disclosure under either MDEA or the Interagency Data Exchange Agreement (IDEA). After the last meeting, several updates had been made to these agreements, including incorporating a more extensive version of the business associate addendum and adding language necessary for the HEA.

Kathy Booth of WestEd noted that the version of the BUCP that had been emailed to the subcommittee was not the most current draft.

Julia Blair of CSAC indicated that financial aid data can also be subject to FERPA and requested an opportunity to review the document to ensure that the appropriate provisions were included.

The group agreed that—once the CSAC feedback was incorporated—they would provide any edits by June 28, for review and final approval on June 29.

### Incident Response Policy and Plan

Marion McWilliams of WestEd described edits made to the document by a homework team, including adding language that addresses FERPA requirements and ensuring that data providers will be notified in the case of a breach. The homework team also recommended that the policy and plan be updated in fall 2021.

Subcommittee members had no questions or concerns.

### Next Steps

Kathy Booth of WestEd suggested that she provide an update at the June 17 workgroup meeting that summarizes the progress of the Legal Subcommittee and outlines their core remaining concerns. She can also ask whether the workgroup would be willing to adopt the recommendations of the Legal Subcommittee regarding the PA, MDEA, and BUCP that will be determined at the June 29 meeting, for inclusion in the final report to the legislature, which is due on June 30. Subcommittee members agreed with this approach.