Legal Subcommittee Meeting Summary

May 25, 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 May 25, 2021 meeting had the following goals:

- Provide an update on recent developments
- Discuss the following legal templates:
    - Master data exchange agreement
    - Participation Agreement
    - Third party data sharing agreements
- Discuss recommendations on security-related items

The following representatives attended the meeting:

Veronica Villalobos Cruz and Thomas Vu, Association for Independent California Colleges and Universities; Freshta Rasoli, Bureau for Private Postsecondary Education; Kathy Lynch, California Community College Chancellor's Office; Bruce Yonehiro, California Department of Education; Marina Feehan, California Department of General Services; Kary Marshall, California Department of Technology; Cynthia (Cyndi) Bosco, California Department of Health Care Services; Carolyn Kubish, California Department of Social Services; Courtney Hansen and Margaret Porto (for Jennifer Schwartz), California Health and Human Services Agency Rima Mendez, California School Information Services; Ed Hudson and John Walsh, California State University; Julia Blair, California Student Aid Commission; Gabriel Ravel and Kristine Beckley, GovOps; Jeanne Wolfe, Labor and Workforce Development Agency; and Stella Ngai, University of California, Office of the President

Updates

The meeting opened with Kathy Booth of WestEd providing an update on the May Revise that was issued on May 14, 2021 by the Department of Finance.

- May Revise details are here.
- References to the Interagency Data Exchange Agreement have been replaced with references to the Participation Agreement.
- Language has been added that clarifies that the data being shared will be referenced in the Participation Agreement.
- The May 27 Workgroup meeting will include a Q&A session with Chris Ferguson from the Department of Finance.

She also alerted the subcommittee that GovOps has posted the first three positions for the Office of Cradle to Career.

Public Comment

There was no request for public comment.

Master Data Exchange Agreement (MDEA) and the Business Use Case Proposal (BUCP)

Marion McWilliams of WestEd provided an overview of the MDEA/BUCP. The MDEA documents the broad framework for data sharing among the data providers, the institutional members of the Governing Board (including AICCU), and state agencies of public higher education. Signatories to the MDEA will create separate BUCPs for each specific data-related sharing instance with the relevant entities that includes items such as a specific list of data elements, purposes, and requirements. BUCPs also incorporate broad terms of the MDEA.

Julia Blair of CSAC noted that the data they provide is subject to the Higher Education Act (HEA). A general reference should be added, such as in the definitions section, that would allow CSAC to provide financial aid data and others to access it. She will send her edits to Marion McWilliams.

Stella Ngai of UC wondered if MDEA should reference a privacy law like the Confidentiality of Medical Information Act (CMIA) (Civil Code, Section 56.10 et seq.). Marion McWilliams will follow-up offline.

Cynthia Bosco from DHCS noted that she sent an updated Business Associate Agreement (BAA) that needs to be added to the MDEA because the version in IDEA was too brief.

Kathy Booth of WestEd asked if the MDEA/BUCP was ready to forward to the Workgroup, and Stella Ngai of UC asked for one more review of the document.

Participation Agreement (PA)

Marion McWilliams of WestEd led a discussion about the three remaining issues for the Participation Agreement (PA):

- Type of agreement
- Technical and security requirements
- Indemnification

Type of Agreement

Thank you to Bruce Yonehiro of CDE for providing language to create a bilateral agreement—all data providers will sign a single agreement. The agreement clarifies that enforcement rights flow only between each data provider and the managing entity.

Julia Blair of CSAC asked if the PA would be the correct agreement in which to reference the HEA and provide the language needed to establish the formal relationship that is required for receiving data. Julia Blair offered to review the PA and MDEA, and notify Marion McWilliams where to add the language.

Technical and Security Requirements

Marion McWilliams of WestEd noted that a subset of the PA Homework Team will meet to dive into various agreements that contain security provisions, to see where there are gaps that need to be addressed in the PA. Earlier drafts of the PA had included a number of placeholders based on templates provided by the partner entities. Given subsequent work, some exhibits and terms are no longer needed and will be removed. For example, the PA will refer to approved technology standards and policies, rather than try to list specific technology procedures within the agreement.

Indemnification

Marion McWilliams of WestEd noted that GovOps has preliminary language to propose regarding who bears costs and responsibilities for a breach. She also reminded the group that existing legal provisions

such as the California Information Practices Act (Civil Code Section 1798) and the State Administrative Manual (SAM) impose certain requirements and responsibility for breach notification.

Gabriel Ravel of GovOps noted that if there is a breach that is the result of negligence by GovOps or its employees, then GovOps will take responsibility for breach notification and indemnification. GovOps cannot be responsible for entities that are not GovOps' employees because they are not agents of GovOps. He also clarified that the language is not final and still needs approval, to ensure that it is consistent with the SAM.

Bruce Yonehiro of CDE describe a potential scenario: what if a hack happens that is not the result of GovOps' negligence, but still results in all data providers being sued? If there is an inadvertent breach, there needs to be a coordinated plan. The breach cost should not come from the data providers' budgets, which could cause the agencies to cut back on programming. Instead, the legislature should fund non-negligent breach-related expenses as part of the cost of the data system. He also wondered if GovOps would work with data providers to provide notices to protect the individuals affected by the breach.

Gabriel Ravel of GovOps noted that breach notification is a separate matter. He indicated that it does not seem right for the responsibility to be placed on GovOps if there are multiple sources of a breach—in the scenario described, arrangements for a joint defense would be needed.

Tom Vu of AICCU reminded the group that not all partner entities are public entities.

Ed Hudson of CSU noted that the Cradle-to-Career Data System will be a target since the data is in a central location. Phishing attacks are common, especially for insufficiently protected environments. CSU has over 9 million records, and that could result in over $1 billion in costs—CSU is not prepared to cover that expense. This is a sticking point that must be addressed before the CSU can sign off on the proposed legal agreements.

Gabriel Ravel of GovOps appreciated the perspectives of the group. He reminded the group that although GovOps will maintain the system, it is not the only agency with access.

Kathy Booth of WestEd asked if the permissions protocol and incident response plan and policy should be addressed in the legal agreement to help address this concern.

Stella Ngai of UC, Bruce Yonehiro of CDE, Ed Hudson of CSU, and Tom Vu of AICCU agreed that these issues should be addressed in the legal agreement.

Bruce Yonehiro of CDE noted that indemnity does not deal with technical standards. He asked whether a phishing incident would be covered. For example, if training was provided and a phishing incident still occurred—the responsible party would be considered negligent. This topic is a policy issue that needs to be addressed, to ensure that participating in the data system does create a financial risk. If it is not addressed, it will be a disincentive for participation, which jeopardizes the cooperation needed to create the state system.

Bruce Yonehiro of CDE and Tom Vu of AICCU suggested that statute and the PA should both address indemnification.

Gabriel Ravel of GovOps noted that there is a SAM provision where the receiving entity bears the cost when the receiving entity acts negligently. Adding an indemnity clause would be broader than what is standard in state agreements.

Julia Blair of CSAC noted that this is a policy issue for the legislature and felt that the Legal Subcommittee cannot dictate how to respond. Courtney Hansen of CHHS concurred and felt it would be inappropriate to indemnify other entities beyond what the SAM requires.

Ed Hudson of CSU noted that when a system is compromised, it is de facto indication of inadequate protection.

Carolyn Kubish of CDSS countered that there is no way to 100% protect against breaches.

Tom Vu of AICCU noted that since AICCU is not a public entity that would benefit from state breach protections, it would be difficult to incentivize individual independent colleges to participate. When they give their data to the state, it is no longer under their control.

Gabriel Ravel of GovOps stated that private parties cannot be indemnified—this is not permitted by statute due to constitutional barriers.

Stella Ngai of UC asked for clarity on the term "agents."

Gabriel Ravel of GovOps noted that a vendor would be an agent. He indicated that employees are also agents and the agreement should be clear that the other participants in the agreement are not GovOps' agents.

Third-Party Data Sharing Agreements

Marion McWilliams of WestEd noted that, in the case where a third party such as a researcher is given permission to access anonymized, individual-level data, GovOps will use a library of templates to streamline the legal agreement process. The library of templates can be amended over time to address emerging needs so that GovOps does not have to recreate agreements every time a third party is approved to receive data.

There will be two templates for FERPA and one for HIPAA. Julia Blair of CSAC noted that she had provided examples that comply with HEA requirements for FAFSA-related data. Marion noted that the CSAC Data Sharing Agreement can be added as a fourth template.

Cindy Bosco of DHCS asked why the Business Associate Agreement is included, and if this is for all third-party requests or just for research. Marion noted that this is for third parties that want data that are not a part of the public-facing tools. Cindy Bosco noted that research requires another review process.

Kathy Booth of WestEd clarified that research requests would go through the CHHS Committee for the Protection of Human Subjects (CPHS). If, for example, a researcher wanted to understand the relationship between Medi-Cal participation and CSU degree attainment, then the request would be sent to the two relevant data providers. If the two entities approved of the request, then it would be reviewed through the CPHS' institutional review board (IRB) process. A researcher would only be able to access the data in a secure data enclave and the final results would be evaluated by a disclosure review board before they could be removed from the system. Cindy Bosco of DHCS said that she would be OK with this process and had no concerns.

Kathy Booth of WestEd noted that we will send the templates again in advance of the next meeting.

Technology and Security

Kathy Booth of WestEd provided an overview of the status of the documents that were listed in the Legal and Technical Model that was approved by the workgroup in summer 2020:

- Data exchange agreement (MDEA/BUCP) (in progress)
- Legal agreement with the managing entity (Participation Agreement) (in progress)
- Data classification scheme (approved)
- Data request process (approved)
- Data security framework (approved; to be reviewed in fall due to constant updates)
- Deidentification policy, renamed as the Data Suppression Protocol for Summary Data (will be considered for approval at the May workgroup meeting)
- Payment policy (on hold—the Participation Agreement states that GovOps can't charge data providers, but the policy for third-party requestors will be determined once the managing entity knows more about the secure data enclave structure)
- Permission protocol (in progress)
- Personally Identifiable Information definition (approved)
- Third Party MOUs (in progress)

In addition, the following items have been created:

- Incident response policy/plan (in progress)
- Opt-out policy (approved)
- Privacy policy (approved)
- System disclaimer (approved)

Kathy Booth of WestEd asked if there were any questions or concerns.

Stella Ngai of UC asked if the responsibility portion of the incident response plan was already included in the PA.

Marion McWilliams of WestEd stated that this issue is referenced in the PA, which the homework team will review. The intent is to reference external documents such as the SAM/SIMM, without being too specific (for example, the PA would not specify the number of characters that a password should contain).

Stella Ngai of UC requested that breach notifications and costs be added to the PA.

Kathy Booth of WestEd asked Baron Rodriguez of WestEd—who is a national expert on security for longitudinal data systems—about the appropriate way to address responsibilities and cost if there is a breach, based on how other states handle this issue.

Baron Rodriguez of WestEd stated that most states carry breach liability insurance at the state level—breach costs are borne by the state and not addressed in MOUs. For example, in Oregon, legal agreements include breach provisions, but do not address costs. The language focuses on communication of an incident, notifications, and timelines.

Kathy Booth of WestEd asked how other states handle indemnification for independent colleges that are not public entities. Baron Rodriguez of WestEd noted that while some states integrate private college data, some legal interpretations do not allow for a mix of data from private and state entities.

Tom Vu of AICCU outlined a potential scenario: what would happen if a student sued an individual UC, the UC Office of the President, and AICCU's member colleges after a data breach occurred at GovOps?

Baron Rodriguez of WestEd noted that most public agencies have cybersecurity insurance. The agency provides the monitoring and compensation due to an individual. However, most states are not as large as California, so the magnitude is different. The PA could include a requirement that GovOps carry cybersecurity insurance for the entities that are not covered under the state's cybersecurity policy.

Ed Hudson of CSU noted that their cybersecurity insurance would not extend to GovOps, and added that the CSU is not a state agency under the statutory definition or covered by SAM. His agency just went through the renewal process for cybersecurity insurance and found that it is getting harder to qualify because of numerous payouts. CSU's insurance carrier would have to review GovOps' policies. He also was concerned that legal notifications would be put back on the data providers, which would be problematic because the cost and efforts of notifications are not covered by their budgets.

Baron Rodriguez of WestEd stated that it would be difficult for GovOps to do outreach to CSU students in the case of a breach. He speculated that CSU would want a level of control of the messaging, even if the breach was the fault of a third party. So, while GovOps would be responsible, CSU might support the effort to contact its students.

Ed Hudson of CSU stated that his agency does joint communications with their vendors in the case of a breach. CSU can send a mass email to everyone affected, but this may not meet the requirements of the Information Practices Act. He also noted other challenges, like contacting impacted individuals who reside outside of California. There are different notification requirements in other states. For example, in Vermont, the state Attorney General's Office has to be notified if there are more than 500 people impacted.

Baron Rodriguez of WestEd suggested that there be secondary conversations about breach notification to address issues such as how GovOps would know if individuals are in other states. GovOps may need to have incident response plans that align with each data provider's requirements, rather than trying to develop a singular breach response policy.

Ed Hudson of CSU noted that it could become unwieldy for GovOps to manage this—it is ideal to have a single standard about when participating agencies are notified, along with timelines. He felt that the subcommittee needed to agree on a minimum standard for agency notifications. They could use the Information Practices Act, which specifies when an entity is considered to be in possession of the data and has to notify other agencies.

Marina Feehan of DGS noted that she will ask Mike Arakji of DGS to see if his team can handle different data breach responses for each agency.

Marion McWilliams of WestEd noted that the data providers will be members of the security incident response team. The proposed policy defines incidents and the procedures that will be followed. The proposed plan has a few items that cannot be completed until implementation of the data system is underway, such as listing specific individuals at each entity and their contact information. She indicated that the policy could include specific documentation for each agency, such as CSAC's protocols. Some laws require notification within 24 hours, but the FAFSA requires a one-hour notification.

Ed Hudson of CSU stated that he supported the incident response plan because it was thorough.

Tom Vu of AICCU noted that indemnity is a separate issue that needs to be sorted out, but he supported the response policy and plan. AICCU has 115 member institutions and would like to see a broad indemnification for the nonprofit colleges. Without indemnity, small colleges would not be adequately protected, even if they have cybersecurity insurance.

Bruce Yonehiro of CDE noted that having separate incident plans for each entity could be problematic because laws may change and evolve over time. One simple solution would be to require the managing entity to respond and provide notices in accordance with all applicable laws, with indemnity if GovOps fails to follow those laws. An insurer would not pay a third-party for a breach unless indemnity was attached. For example, your car insurance would not pay someone else unless you have liability coverage.

Kathy Booth of WestEd reflected that the issue of who is responsible is an issue that is causing concern. She raised another scenario: what if a CDE staff member who has permission to access that agency's repository is caught in a phishing scam and does something to create a breach? Would GovOps be responsible if it was CDE's security that was compromised? Gabriel Ravel of GovOps stated that this is precisely the scenario GovOps is worried about.

Bruce Yonehiro of CDE said GovOps would have to indemnify CDE's conduct. For example, if there is a fraud claim, all participating entities could be sued. GovOps should be funded to handle these claims. It is a policy that needs to be addressed, because it is a cost of the system. It is unfair to place these costs on participating entities that are providing data, including private colleges. If he was counsel to the private colleges, he would tell them not to go forward without indemnity.

Ed Hudson of CSU asked what would happen if it was a GovOps' employee or administrator who caused the breach? If it was a CSU staff person, there is a different liability. He would need to defer to his legal counsel.

Marion McWilliams of WestEd asked Stella Ngai of UC about indemnity in the event that UC or its agents are negligent or cause willful misconduct.

Stella Ngai of UC stated that UC needs indemnification. She will discuss this topic with her experts.

Gabriel Ravel of GovOps stated that the proposal is asking GovOps to provide guarantees that go further than what is in the SAM, especially for private parties. Due to lack of authority, what is being requested is prevented by the California constitution.

Mike Arakji of DGS—who serves as GovOps' Information Security Officer—joined the meeting to answer questions.

Stella Ngai of UC asked who would handle future lawsuits for breaches.

Mike Arakji of DGS stated that breach policies have provisions where the cost of a breach is covered by those who contributed to the breach. If a DGS staffer is negligent due to clicking on a phishing link, then DGS would bear the cost. If a CSU user contributed to the breach, the cost of the investigation would fall on CSU. Budgets are borne by each state entity. For indemnification, he does not believe DGS can be responsible for others' breaches. It is incumbent on GovOps to provide a resilient and secure system and to use due diligence and care. Unfortunately, no matter how much is spent, no system can be 100% secure.

Bruce Yonehiro of CDE stated that this framing includes an assumption that there is a cause. But there will be times when it may be difficult to say who caused the breach. Also, someone must bear the cost of attorneys' fees in defending a lawsuit. GovOps is in the best position to cover those costs, as opposed to each data provider.

Mike Arakji of DGS described a scenario where a contractor causes a breach due to willful neglect. The contractor would hire a cybersecurity firm, which would coordinate the investigation with the contractor and keep GovOps in the loop. In this case, GovOps would handle breach notification. Procuring cybersecurity insurance is considered a best practice and is not too costly, but this cost has to be budgeted for the data system.

Ed Hudson of CSU returned to the scenario where someone at a data provider clicks on a phishing email, and bad actors get access to the system. If there is not adequate segmentation and separate backups, there will be an issue.

Bruce Yonehiro of CDE suggested that GovOps purchase cybersecurity insurance to a certain dollar limit, as part of its budget for the data system, and provide indemnity up to the limit of the cybersecurity insurance.

Courtney Hansen of CHHS was not sure the proposed approach would be satisfactory. Indemnification is still statutorily prohibited, so it would not solve constitutional issues. Jeanne Wolfe of the Labor Agency concurred.

Kathy Booth of WestEd asked if it would be appropriate to add a provision to the participation agreement that requires GovOps to buy cybersecurity insurance.

Mike Arakji of DGS stated this could work because no one wants an unfunded liability, but Gabriel Ravel of GovOps stated that he would need to investigate and follow up on this proposal.

Mike Arakji of DGS clarified that the cost of insurance is based on the types of policies, procedures, and protections that are in place. Insurance companies have brackets based on the level of risk. GovOps could buy the appropriate insurance, at the point that contractors are selected to build the data system.

Stella Ngai of UC wanted more information on what is covered by cybersecurity insurance. How is the value of the asset determined?

Bruce Yonehiro of CDE reiterated that insurance and indemnity should not be tied to negligence or willful misconduct. The constitutional issue need to be addressed for private entities. Indemnity language should be broad enough to address any limitations to the insurance policy.

Kary Marshall from CDT noted that, because Gabriel Ravel of GovOps had to leave the meeting, this issue should be tabled until all pertinent parties are present.

Kathy Booth of WestEd reminded the group that some of the information necessary to establish insurance levels may not yet be available. For example, the list of data points being provided by each partner entity will not be finalized until the workgroup meeting later this month. After that, the data providers will need to do document how many records they expect to upload to cloud repositories. In addition, there may be time to address the issue of indemnification related to independent colleges because they would not be providing data until 2022-23. Then she asked the group if they had the information they needed about the broader security and privacy framework.

Stella Ngai of UC stated that she did not have all the information she needs. She also asked when the data providers would upload their information.

Kathy Booth of WestEd said that the timeline is unclear because the legislature is requesting that an additional planning process be implemented before procuring data tools (the Project Approval Lifecycle). This means it could be a year before data are submitted.

Bruce Yonehiro of CDE said that approval of the privacy and security documents would not be a simple majority vote—if individual data providers are not confident in the protections, they may elect to not participate in the data system. The concerns raised by this subcommittee should be addressed in the trailer bill.

Kathy Booth of WestEd reminded the group that there would not be a majority vote regarding the way the trailer bill is amended—this is the purview of the Department of Finance and the legislature. She asked what steps could be taken through the planning process that would enable data providers to sign the PA.

Baron Rodriguez of WestEd suggested that data contributions could be contingent on resolving the breach cost and indemnification issue.

Bruce Yonehiro of CDE suggested that the final report to the legislature could summarize the concerns raised about funding the cost of cybersecurity insurance and responding to breaches and suggest possible solutions, such as a line item in the budget and broad indemnity for the participating entities. The report could acknowledge that some issues are constitutional. He also felt that GovOps should prepare possible solutions.

Stella Ngai of UC stated that indemnification and data security are related, but separate issues.

Bruce Yonehiro of CDE clarified that indemnification and data security are the only major legal issues that have not been resolved. However, the PA still needs cleanup, which should be completed before the next Legal Subcommittee meeting. Ed Hudson of CSU agreed that the subcommittee was close to finalizing its documentation.