Technology & Security Subcommittee Meeting Summary

March 9, 2021

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

The March 2021 meeting had the following goals:

- Discuss data classification
- Discuss California College Guidance Initiative's privacy and security policies
- Discuss the security framework
- Discuss recommendations from the Incident Response Plan homework team

The following representatives attended the meeting:

Formeka Dent, Antelope Valley Union High School District; Helen Norris, Association of Independent California Colleges and Universities; Clarissa Serrato-Chavez, Bureau for Private Postsecondary Education; Andy Manguia, California Commission on Teacher Credentialing; Barney Gomez, California Community College Chancellor's Office; Rodney Okamoto, California Department of Education; Karissa Vidamo, California Department of Social Services; Janet Buehler, California Department of Technology; Lloyd Indig, California Health and Human Services Agency; Greg Scull, California School Information Services; Subash D'Souza, California State University Chancellor's Office; Gurinder Bains, California Student Aid Commission; Ben Baird, California College Guidance Initiative; Todd Ibbotson, Employment Development Department; Dan Lamoree, Educational Results Partnership; Douglas Leone, Labor and Workforce Development Agency; Matthew Linzer & Hooman Pejman, University of California Office of the President

Update on Key Decisions by the Cradle-to-Career Workgroup

The meeting opened with Kathy Booth of WestEd providing an update on decisions made by the workgroup at its February meeting, including approving the definition of personally identifiable information (after removing county), the data classification protocol, the system disclaimer (with the caveat that its implementation should be addressed through the user centered design process), and the privacy policy.

Data Classification

Kathy Booth reviewed the definition that the workgroup adopted for personally identifiable information and clarified how this led a data classification protocol that identifies any information about an individual as *sensitive information*, and information about institutions as being *public information*.

WestEd applied this data classification to the data points that have been identified for the P20W data set and is currently circulating the list with the data providers for edits. This document includes other information that would be useful for Technology & Security Subcommittee members to review. For example, it provides an updated list of the information that will be in the data system. The Data Definitions Subcommittee has been reviewing each of the 160 data points that were approved by the workgroup in fall 2020 to further refine the content, source, and public display options for each item.

This review has expanded the data set to more than 200 data points, which will be helpful to take into account as the data providers plan for the process of data submission. The document that is being circulated further specifies which entities will provide each data point, given that some data points are not collected by all partners and, for some partners, some data points are of poor quality. Kathy Booth of WestEd asked that the Technology & Security Subcommittee members review the document by March 18 and provide comments, in advance of a discussion at the workgroup meeting.

Formeka Dent of Antelope Valley Union High School District asked for clarification on why CDE is not providing the number of a-g courses taken, given that local education agencies report this information. [*Post meeting note: in a subsequent exchange with CDE, they clarified that the data point is not validated. Given analysis that shows significant misalignment between local data systems and the a-g eligibility database maintained by UC, this data point is not of sufficient quality to include in the Cradle-to-Career Data System. However, with the upgrades to CALPADS planned as part of scaling CalifornaiColleges.edu, CDE anticipates that data quality will improve and the data point can be included in the future.*]

Formeka Dent of Antelope Valley Union High School District also asked what types of high school completion would be included. Kathy Booth of WestEd confirmed that the definition includes multiple forms of completion and noted that the recommended variables for each data point are provided on the project website here: https://cadatasystem.wested.org/meeting-information/definitions-subcommittee (click on the link to "View recommendations").

Chris Furgiuele of UC expressed concern that the data providers need more time to review the data points. He noted that it is important that each data point be examined to ensure it is of sufficient quality to be included, not simply whether the information is collected by a state agency.

Clarisa Serrato-Chavez of BPPE stressed that it will be important to note that not all data providers collect all data points included in the P20W data set.

Privacy and Security for CaliforniaColleges.edu

Ben Baird of the California College Guidance Initiative provided information on how his organization protects privacy and maintains security for CaliforniaColleges.edu. Given that the workgroup has recommended scaling this state project as part of the Cradle-to-Career Data System, it will need to conform to the privacy and security standards recommended by the Technology & Security Subcommittee.

The presentation covered essential facets of privacy and security including the types of information in the system, how data are collected and from which entities, legal agreements that support data exchanges and data ownership, opt out policies, data access policies, the encryption level for stored data, policies for traffic from outside the country, security audit requirements, multi-factor authentication, background checks and mandatory training for staff, and systems for tracking who accesses information. All of this information is available in a report shared in advance of the meeting and posted to the project website.

Mike Arakji of DGS expressed his support for the approach taken by CCGI. However, he cautioned that some hackers are able to use proxies such that it is not possible to tell they are not located in the country.

The Technology & Security Subcommittee voted unanimously to endorse the privacy and security approach currently implemented by CCGI and to advance this information to the workgroup.

Security Framework

Mike Arakji of DGS provided an analysis of the security framework that had been recommended by the Technology & Security Subcommittee in summer 2020, which is based on the Higher Education Community Vendor Assessment Toolkit (HECVAT) developed by EduCause. DGS was asked to conduct this review because it provides IT support and security services to GovOps, such as ensuring annual certifications of privacy and security compliance and supporting procurement so contracts comply with state and federal standards.

In order to evaluate the proposed security framework, to ensure it is compliant with the State Administrative Manual (SAM), Statewide Information Management Manual (SIMM), National Institute of Standards and Technology (NIST) cybersecurity framework, the Family Educational Rights and Privacy Act (FERPA), and the Health Insurance Portability and Accountability Act (HIPAA), Mike Arakji compiled the requirements in a single spreadsheet. This spreadsheet includes more recent standards than the ones that were in place when the security framework was developed last summer.

The group briefly discussed the benefits of using the HECVAT framework, which is optimized for education data and is aligned with both NIST and International Security Organization (ISO) cybersecurity standards. However, Subash D'Souza of CSU noted that HECVAT does not have sufficient content on cloud storage, which will need to be addressed. Mike Arakji of DGS clarified that GovOps will be required to conform with the NIST 800 series, as this is a state policy. He also suggested reviewing other frameworks to address gaps in the HECVAT, such as the one developed by the Cloud Security Alliance (CSA).

In response to a question from Rodney Okamoto of CDE about whether HECVAT applies for K-12, Baron Rodriguez of WestEd, who previously served as a federal technical assistance provider for state data systems, confirmed that the framework addresses the needs of K-12. The standards exceed those in FERPA because higher education needs to meet a higher standard to protect financial aid data.

Given that further revisions to state security requirements will be released shortly, subcommittee members recommended adopting the security framework and committing to revise it when the data system is developed. Baron Rodriguez of WestEd affirmed that this approach conforms with effective practices in other states. Mike Arakji of DGS noted that when the framework is revised, it could use more generic language, such as "latest published security and privacy standards," as opposed to a specific requirement such as "800-171."

While the spreadsheet that summarizes state and federal requirements will serve as an important resource for GovOps, particularly during the procurement process, it cannot be publicly shared. When a request for proposals is released, the content can be shared with bidders that sign a non-disclosure agreement so they can document how they will comply with the security framework.

A partially redacted version of the spreadsheet was shared with subcommittee members after the meeting. All parties were comfortable with using these additional specifications to evaluate whether GovOps and vendors are in compliance with the security framework when the Cradle-to-Career Data System is developed.

Incident Response Plan

Erin Carter of WestEd described the process for developing the proposed incident response plan, which is based on DGS's incident response plan. The homework team recommended that the plan be evaluated by the Legal Subcommittee to determine whether language should be added that is specific to FERPA.

Subcommittee members also noted that some portions of the plan will need to be filled in once the data system is under development, such as the tables that identify key staff. In addition to identifying specific individuals, it will be important to determine which types of staff should be on the response team and to develop greater detail on the communications plan for a breach—which should also name the data providers.

Next Steps

Given the further specificity cannot be developed until the data system is under way, this subcommittee will not meet again as part of the planning process. However, GovOps will likely reconvene the group in the fall to leverage their valuable expertise.