LAO

The 2022-23 Budget:

Cybersecurity at the California Community Colleges

MARCH 2022

Summary. The Governor's budget provides a total of $100 million Proposition 98 General Fund ($25 million ongoing, $75 million one time) for the California Community Colleges (CCC) to upgrade their cybersecurity. Of the proposed funding, $92 million would be allocated to colleges, with the remaining funding intended for specified systemwide services. We recommend the Legislature approve $23 million ongoing for more district cybersecurity staff and direct the Chancellor's Office to develop an allocation method for these funds that ensures a minimum level of funding for each district. For the remaining $2 million ongoing, we recommend requesting better information, particularly on the roles and responsibilities of each of the proposed systemwide service providers. For the $69 million in one-time funding proposed for the colleges, we recommend the Legislature direct the Chancellor's Office to develop an allocation method that accounts for not only colleges' enrollment size but also their current level of cybersecurity preparedness. We also recommend requiring the Chancellor's Office to submit certain documentation that could help guide legislative decisions regarding the remaining one-time funds as well as any future cybersecurity funding.

Introduction

In this post, we provide background on cybersecurity issues at CCC, describe the Governor's proposal to provide funding for various cybersecurity upgrades, provide our assessment of the Governor's proposal, and make associated recommendations.

Background

Colleges Are Largely Responsible for Their Cybersecurity. The state subjects most state agencies, including the CCC Chancellor's Office, to cybersecurity standards developed by the California Department of Technology (CDT) and federal government. In addition, CDT and the California Military Department (and, in some cases, third party vendors) conduct audits to bolster state agencies' compliance with cybersecurity standards. In contrast, the state does not require community colleges to follow specific standards, and community colleges are not routinely subject to oversight or audits of their cybersecurity programs and processes. As locally governed entities, community colleges also make their own decisions about budgeting for technology and data security, including setting their associated staffing levels and deciding how much to spend on hardware and software purchases. Colleges typically use apportionments (general-purpose monies) to fund cybersecurity costs.

CCC Information Security Center Offers Some Assistance to Colleges. Though colleges manage their own information security, certain systemwide resources and tools are available to them through the CCC Technology Center, which is administered by Butte College. This center is funded by the state through a technology categorical program supported with ongoing Proposition 98 General Fund. In 2016-17, the center added a division, the Information Security Center, focused primarily on cybersecurity issues. In 2021-22, the Information Security Center is receiving $3 million ongoing Proposition 98 General Fund from the categorical program. The Information Security Center's services include making available sample security plans for colleges to adopt, offering vulnerability scans and risk analyses, providing recommendations to colleges in the event of a data breach, and enhancing colleges' security monitoring and "threat intelligence" (knowledge that helps identify security threats). The funding also supports a CCC systemwide committee that discusses current cybersecurity threats facing colleges.

Colleges Have Seen a Recent Surge in Fraud Attempts. CCC has a common online admissions application known as CCCApply. The Chancellor's Office contracts with the CCC Technology Center to administer the application platform. Colleges upload completed applications and process them. Through CCCApply, bad actors attempt to submit fraudulent applications—sometimes hundreds at a time at multiple colleges using automated technology. Upon acceptance, these bad actors can register for classes, allowing them potentially to gain access to certain financial aid benefits. Though some fraudulent activity occurred prior to the pandemic, such attempts increased notably with the availability of a significant amount of federal relief funds for student emergency financial aid.

Colleges Face Other Threats to Information Security. Colleges maintain databases with sensitive information on students (and their families) and staff. In addition, colleges operate other technology such as e-mail and phone systems. These types of systems are routinely the subject of cyberattacks, ransomware, and other malware of varying scales. Recently, several community colleges reported major cyberattacks on their information and other technology systems.

Proposal

Governor Proposes a Package of Cybersecurity Upgrades for Colleges. The package totals $100 million Proposition 98 General Fund, consisting of $25 million ongoing and $75 million one time. The $25 million ongoing is primarily for college cybersecurity staffing, whereas the $75 million one time is primarily for security network upgrades, general security software, and anti-fraud technology. Of the proposed funding, $92 million would be allocated directly to colleges. The Chancellor's Office would award the remaining $8 million via contracts with certain districts to provide specified systemwide services and oversight. The main goal of this package of proposals is to enhance colleges' information security to protect against enrollment scams and hacking. A secondary goal is to improve the user experience for students applying to CCC. **Figure 1** details the various components of the Governor's CCC cybersecurity package and describes how funds would be allocated for each component.

Colleges Would Have to Meet Certain Requirements to Receive Funds. Although not specified in budget or trailer bill language, the Chancellor's Office indicates that it plans to require districts to meet certain requirements as a condition of receiving any of the proposed ongoing or one-time cybersecurity funding. Specifically, colleges would be required to (1) complete an annual cybersecurity self-assessment based on state and national standards and identify needed improvements; (2) submit quarterly status updates on progress toward meeting state and national standards; (3) submit a monthly report on any incidents of application, enrollment, and financial aid fraud; and (4) submit a report of all cybersecurity incidents that resulted in a breach of personally identifiable information or disruption of services (such as through ransomware). The Chancellor's Office indicates that these requirements would be made through both systemwide guidance and changes in CCC regulations.

Budget Includes Two Proposed Positions at the Chancellor's Office in Support of Initiative. In addition to the $100 million Proposition 98 General Fund, the Governor's budget includes a proposal to add two new positions at the Chancellor's Office and an associated $314,000 non-Proposition 98 General Fund to support CCC cybersecurity efforts. This staffing proposal is part of a larger package of staffing proposals that we analyze in a separate post, *The 2022-23 Budget: CCC Chancellor's Office Staffing*.

Assessment

Given State's "Fifty Percent Law," Merit to Having an Ongoing Cybersecurity Categorical Program. Given the highly sensitive nature of the data that colleges maintain, together with the recent cyberattacks, colleges have a local interest in dedicating staff to cybersecurity issues and putting in place robust defensive systems. Colleges, however, receive no state funding specifically for these purposes. Moreover, under state law, colleges must use at least half of their general-purpose funding on salaries and benefits of classroom faculty and aides. Spending on other college staff, including information technology (IT) personnel, counts against the 50 percent requirement, as do other costs, such as anti-fraud software licenses and consulting

services with cybersecurity experts. Colleges that fall below the 50 percent mark can be subject to financial penalties by the Chancellor's Office. Because of this law, some colleges might refrain from using sufficient apportionment funding to achieve adequate ongoing cybersecurity protection. Given this consideration, we think the Governor's proposal to provide ongoing cybersecurity categorical program funds, which would not be subject to the fifty percent law, is reasonable.

Merit to Enhanced Ongoing State-Level Role for CCC Cybersecurity Issues... Beyond bolstering local cybersecurity staffing on an ongoing basis, we believe a stronger state-level role also is worth considering. While CCC has an advisory committee to discuss cybersecurity threats and incidents systemwide, community colleges currently lack a strong central information hub to detect patterns and promote coordination. Colleges do not have to report incidents of

Figure 1

Governor Provides Mix of Ongoing and One-Time Funds for Local and State-Level Purposes

Proposition 98 General Fund (In Millions)

Description	Proposed Amount	Purpose of Funding	Funding Allocation Method
Ongoing Funds			
District cybersecurity staff	$23.0	Hire staff to monitor and combat cyberattacks and fraud. (Districts with limited access to these staff may share staff on a regional basis.)	Funding for each district. (No specific formula is proposed.)
Statewide cybersecurity teams	1.0	Contract with independent consultants to assess district compliance with cybersecurity standards.	Chancellor's Office to contract with a district to administer on behalf of CCC system.
System-level oversight	0.5	Provide direction and oversight to district (and regional) staff and statewide cybersecurity teams on cybersecurity standards and incidence response. Provide support to colleges needing assistance.	Chancellor's Office to contract with a district to administer on behalf of CCC system.
CCCApply operations	0.5	Cover hosting and maintenance costs.	Chancellor's Office to contract with CCC Technology Center (Butte College).
Subtotal	($25.0)		
One-Time Funds			
College network security upgrades	$40.0	Obtain assessments of system vulnerabilities. Purchase hardware and software to prevent cyberattacks.	Funding for each college based on enrollment size, with larger colleges receiving a larger amount.
College enrollment anti-fraud technology	29.0	Purchase fraudulent application detection software. Provide anti-fraud training for staff.	Funding for each college based on enrollment size, with larger colleges receiving a larger amount.
CCCApply upgrades	5.0	Redesign platform (with input from student focus groups), adding and testing security features. Streamline number of questions applicants are required to answer. Add capacity to report data on applicants that started but did not complete application.	Chancellor's Office to contract with CCC Technology Center (Butte College).
CCCApply training	1.0	Once CCCApply upgrades are completed, provide training to college staff.	Chancellor's Office to contract with a district to administer on behalf of CCC system.
Subtotal	($75.0)		
Total	**$100.0**		

cyberattacks or suspected fraud to the Chancellor's Office. This is the case even though scams and cyberattacks often target multiple colleges simultaneously. Currently, districts also do not need to show that they are either meeting state and national cybersecurity standards or have adopted plans and are making progress toward meeting these standards. Providing more state direction and support in these areas could lead to overall improvements in colleges' cybersecurity programs and processes.

...But Potential Issues With How New Oversight and Support Model Would Work. The Governor's ongoing cybersecurity components include (1) creating statewide cybersecurity teams, (2) funding a system-level entity that oversees both local colleges and the statewide cybersecurity teams, and (3) providing two new positions at Chancellor's Office. This approach creates a complex organizational structure in which exactly what functions and role each entity would have is unclear. In some cases, the roles and responsibilities of the various entities appear to overlap. For example, under the Governor's proposal, the statewide cybersecurity teams would monitor colleges' compliance with cybersecurity standards. Yet, the system-level oversight entity also would be charged with monitoring standards and providing support to colleges, in addition to providing direction and oversight to the statewide cybersecurity teams. Moreover, the Chancellor's Office indicates it too would be charged with overseeing the statewide cybersecurity teams. We also have concerns that the administration's proposal could create a conflict of interest for the system-level oversight entity, which, as characterized by the Chancellor's Office, would help colleges with implementation while at the same time monitoring and holding colleges accountable for what they implement. Moreover, it is unclear if the Chancellor's Office's goal is for the statewide cybersecurity teams to assess all colleges annually or instead some subset of districts, with a focus on high-risk colleges.

Merit to Funding Cybersecurity Upgrades at Colleges... Based on anecdotal information, the Chancellor's Office has heard that community colleges vary in terms of their cybersecurity preparedness and anti-fraud detection capabilities. Whereas some colleges have staff dedicated to cybersecurity and relatively sophisticated defensive systems in place, other colleges rely on IT generalists that lack expertise in cybersecurity. Potentially, the state could strategically allocate funding, including the proposed one-time funding, to assist colleges in obtaining a certain level of cybersecurity preparedness.

...But Opportunities to Improve How One-Time Funds Would Be Allocated to Colleges. The Governor's proposed approach of allocating the one-time funds to colleges based on enrollment size has some merit, as potential cybersecurity and fraud risks can increase based on the technology usage at a college. A better approach, though, would be to base allocations on need as well—providing more funding to colleges that need more cybersecurity upgrades. Though there currently is no inventory of where each college is relative to state and national standards and what each would need to do to meet standards, the Chancellor's Office is in the process of identifying the current preparedness level for each college. The Chancellor's Office believes it might have the initial inventory prepared by June 2022. Such an inventory could be used to track need and allocate a share of 2022-23 funding accordingly.

Governor Proposes One-Time Funds for Ongoing Purposes. Though some initial one-time funding could help with initial cybersecurity upgrades among colleges, much of what the Governor has proposed as one-time costs are more likely ongoing costs. Typically, a college would be expected to undergo independent security assessments every few years, pay for network security and anti-fraud software licenses annually, and make network upgrades periodically. As a result of these factors, the proposed level of ongoing funding for college cybersecurity and anti-fraud detection likely is underestimated. Importantly, the administration and the Chancellor's Office have not yet identified what they believe to be entailed in terms of funding to ensure colleges have a minimum level of ongoing cybersecurity and fraud detection. Lacking clarity in this area, the existing budget back-up is inadequate, as it neither clearly distinguishes one-time from ongoing costs nor includes detailed cost estimates.

Administration Has Provided Incomplete Information on CCCApply Proposal. The Governor's cybersecurity packages includes $6 million one time primarily to upgrade CCCApply's anti-fraud features and provide related college training, as well as $500,000 ongoing for hosting and maintenance of the redesigned portal. We concur with the administration that such enhancements are warranted and would have systemwide benefits for colleges and students. The amounts proposed by the administration, however, have only been partially justified. Specifically, of the $6 million proposed for one-time purposes, the administration has only provided workload justification for $3.4 million. The remaining $2.6 million in proposed costs either have no backup details or are labeled in documents provided to our office as "TBD" (to be determined). The administration does not provide any backup on how it estimated the ongoing cost. Without such information, the Legislature is unable to determine whether the proposed amount is justified to accomplish the administration's objectives for CCCApply.

Recommendations

Approve Funds for College Cybersecurity Staff. As a starting point, we recommend the Legislature approve the $23 million in ongoing funding for district cybersecurity staff. We think the state has an interest in making sure every district has at least one staff person dedicated to cybersecurity. Multi-college districts, however, may warrant more funding. We recommend directing the Chancellor's Office to develop an allocation method for these funds that ensures a minimum level of funding for each district while accounting for any other relevant factors. (Districts with existing cybersecurity staff could be permitted to use their allocations to increase their number of staff or improve their cybersecurity preparedness in other ways.)

Request Better Information on Proposed State-Level Structure. We recommend the Legislature postpone consideration of the $1.8 million in ongoing funding for the proposed state-level cybersecurity structure ($1.5 million Proposition 98 General Fund and $314,000 non-Proposition 98 General Fund) pending receipt of better information. Specifically, we recommend the Legislature request the administration and Chancellor's Office to clarify the specific role and functions of: (1) the existing staff at the Information Security Center, (2) the proposed statewide cybersecurity teams, (3) the proposed system-level oversight body, and (4) the proposed two additional cybersecurity positions at the Chancellor's Office. As part of this reporting, the Chancellor's Office should clarify how the statewide cybersecurity teams would prioritize their work and how much workload they are expected to accomplish annually given the proposed funding.

Modify Allocation Methodology of One-Time Funding for Colleges. We recommend the Legislature appropriate the $69 million in one-time funding for the colleges but direct the Chancellor's Office to allocate this funding in a way that accounts not just for enrollment but also for need, with less prepared colleges receiving somewhat more funding than more prepared colleges of the same size. Colleges could use their allocations for independent security assessments, network upgrades, software licenses, and related technology costs. The Chancellor's Office's initial inventory of colleges' cybersecurity preparedness levels could be used as a basis for the allocation of the one-time funds. As discussed below, we recommend requiring the Chancellor's Office to work with districts and submit certain information to the Legislature prior to release of the one-time funding.

Use Additional Information From Chancellor's Office to Guide Allocation and Future Funding Decisions. Specifically, we recommend requiring the Chancellor's Office to submit documentation on (1) the basic requirements for colleges to achieve a minimum level of security, (2) estimates of the associated one-time and ongoing costs, and (3) a proposed formula for distributing the one-time funding to colleges in accordance with size as well as identified needs and costs. We recommend requiring the Chancellor's Office to provide this documentation to the administration and Legislature by October 15, 2022, with the findings informing release of the one-time funds as well as potential 2023-24 budget decisions.

With better information, the Legislature not only could identify how much one-time funding colleges need but also the annual amount of state funding needed to cover colleges' ongoing cybersecurity costs. If more ongoing funding is provided in the future, we recommend the Legislature consider at that time how best to allocate the additional funding among colleges. Ideally, over the next few years, the Chancellor's Office and colleges will learn more about the main risk factors underlying cyberattacks and enrollment fraud, such that the Legislature can align funding increases with those risk factors and potential cost drivers.

Direct Administration to Provide Cost Detail for CCCApply. Given the administration has provided workload justification for only $3.4 million in costs for CCCApply, we recommend the Legislature treat this amount as a starting point. We recommend the Legislature direct the administration to provide full justification for the remaining $2.6 million one-time funding it proposes as well as the $500,000 in proposed ongoing costs. The Legislature could give the administration until the May Revision to provide such information and use it to determine the amount to provide for 2022-23.

LAO PUBLICATIONS

This post was prepared by Paul Steenhausen, with assistance from Brian Metzker, and reviewed by Jennifer Pacella and Anthony Simbol. The Legislative Analyst's Office (LAO) is a nonpartisan office that provides fiscal and policy information and advice to the Legislature.