California Community Colleges

MEMORANDUM
December 5, 2022

DII 22-300-05 | Via Email

TO: Chief Executive Officers
Chief Information System Officers
Chief Business Officers

FROM: Valerie Lundy-Wagner, PhD
Vice Chancellor, Digital Innovation and Infrastructure

RE: FY 22-23 December Cybersecurity Information Updates

The 2022 Budget Act included Assembly Bill (AB) 178 and AB 183, which allocates $25 million in ongoing and $75 million in one-time funds to help the California Community Colleges (CCCs) improve, among other things, data security oversight, fraud mitigation, and IT infrastructure. This memo provides background context about systemwide information technology (IT) and information security (InfoSec) before providing updates about recent activity, including a brief overview of the cybersecurity self-assessment findings and subsequent strategy, penetration testing and security reviews, reminders about fraud monitoring, and information about upcoming funding allocations.

Background

Community college districts are responsible for maintaining an adequate and secure IT infrastructure in compliance with the Accrediting Commission for Community and Junior Colleges (ACCJC) standards for Technology Resources. In comparison, the Chancellor's Office has historically held responsibility for developing systemwide technology licensing or purchasing agreements and providing a limited set of support services to all districts. Historically, the Chancellor's Office has had no insight into local organization, staffing, or security vulnerabilities. This approach is problematic as known disparities in local resources translates into uneven staffing capacity, inequitable ability to adopt technology or take up state-subsidized services and constrains the system's ability to maximize state funding for technology purchases, staffing, and support. Further, persistent issues with fraud and the increase in cyberattacks across higher education, both nationally and systemwide, point to the need for evolution in our approach to IT and InfoSec.

The 2022 State Budget Act provides funds to facilitate development of a more robust and comprehensive support for IT and InfoSec (FY22-23 IT and Data Security funds). While one-time funds from AB 183 are flexible, ongoing funds from AB 178 are structured around specific eligibility requirements, such that districts must do all of the following (summarized below):

- Complete an annual cybersecurity self-assessment, and
- Participate in the following regularly scheduled submission of:
    - Remediation updates twice per year on vulnerability and other issues identified,
    - Detailed after-action reports of all cybersecurity incidents,
    - The total number of "likely fraud" and fraudulent applications, and
    - Information requested on suspected fraudulent enrollments, fraudulent receipt of financial aid.

AB 178 resources set the foundation to gain statewide insight on IT infrastructure and inform future resource allocations that will enable local and systemwide security improvements.

UPDATES ON AB 178 ACTIVITY IN FY 22-23

Overview of Cybersecurity Self-assessment Findings

The first annual cybersecurity self-assessment was released in August 2022 and submitted by all 73 districts. The self-assessment (described here), which included more than 100 questions, was designed to quickly provide the Chancellor's Office with information about district security profiles and inform development of a comprehensive system-level approach to risk.

The Chancellor's Office reviewed the self-assessment data in October and November 2022, sharing initial observations and select findings with key system stakeholders, including the Technology and Telecommunications Advisory Committee (TTAC), Systemwide Architecture Committee (SAC), and the Chief Information System Officer Association (CISOA) leadership. Overall, self-assessment responses highlighted five key needs that coincide with previous, more ad-hoc system feedback:

1. **Information Security Training** to address gaps in employee support.

2. **Decommissioning End-of-Life Software** to reduce risk associated with outdated tools.
3. **Third-Party Risk Management Support** to improve capacity to discover and monitor risk.
4. **A systemwide Security Operations Center** (SOC) to mitigate oversight and monitoring gaps.
5. **IT Staffing** to ensure structural alignment with local needs and national standards.

Each of these is briefly described below alongside information about work in progress and/or next steps.

Information Security Training

As noted in this Harvard Business Review article title, "your employees are your best defense against cyberattacks," and a key tool for reducing cyberattacks is to ensure employees regularly complete information security training. More than half of the 73 districts indicated a gap in Security Awareness Training in the self-assessments. The Vision Resource Center (VRC) provides a no-cost, on-demand online IT and InfoSec training available to all districts that can be found here. In addition to leveraging these resources, the Chancellor's Office encourages all districts to develop or mature a policy for regular security awareness training for all employees. The Tech Center has updated the Security Center webpage to include a security awareness training template to help inform or catalyze local efforts. Districts should align information security training needs with training policies and accreditation standards.

Decommission End-of-Life Operating Systems and Infrastructure

To improve operational efficiency and benefit from up-to-date InfoSec technology, institutions must decommission end-of-life operating systems and infrastructure. According to the self-assessments, security features widely used in personal matters and in private industry, such as multi-factor authentication for remote access to networks and external cloud applications, are underutilized by the system. Additionally, the self-assessment showed that common security controls such as Endpoint Detection and Response (EDR) are only partially in place, and high-risk End-of-Life (EOL) operating systems and infrastructure are still in use. To address this, the Chancellor's Office has adopted a multi-staged approach.

First, the Chancellor's Office purchased a systemwide license for the Microsoft A5 Security Suite in September 2022, complementing the locally purchased Microsoft A3 licenses. This provides all districts with access to a comprehensive set of security tools.

Second, the Chancellor's Office initiated a pilot implementation of the Microsoft A5 Security Suite at select districts in October 2022 to understand the feasibility of system-level professional support services across diverse local contexts and security profiles. The pilot will serve as a proof point for development of the systemwide or regional cybersecurity teams (referenced in AB 178) that will provide professional IT services in ways that should minimize local burden, improve local and system performance, attend to local resource inequities, reduce costs, and optimize state investment. Lessons learned from this pilot will be described in a subsequent memo, as will any changes related to systemwide support for servers and classroom devices.

Finally, the Chancellor's Office will leverage the overall cybersecurity self-assessment scores and district security profiles to inform allocation of funds, especially AB 183 (one-time) funding to address EOL replacement. Districts are responsible for identifying and decommissioning EOL operating systems and infrastructure.

Third-Party Risk Management Support

The cybersecurity self-assessments also revealed gaps in local ability to discover and monitor InfoSec risk associated with technology vendors and services. Third-Party Risk Management (TPRM) is a process for evaluating vendors based on their risk to the organization and requesting documentation to ensure data is being properly secured. The Chancellor's Office is evaluating options to provide the system with TPRM support beginning in FY2023-24, but in the meantime, it is strongly recommended that districts ask critical vendors for due diligence documentation such as a Service Organization Control (or SOC) 2 report or Higher Education Community Vendor Assessment Toolkit (HECVAT), described here.

Local IT Staffing and Security Operations Center

According to Educause, a national organization supporting IT in education, the average staffing in two-year colleges should be 4.4 per 1,000 Full Time Equivalent (FTE) staff, faculty, and students. The

cybersecurity self-assessment reveals that the average and median local staffing across the CCC system is 3.2 / per 1000 FTE and 2.8 / 1000 FTE respectively, confirming widespread understaffing. Feedback from Chief Information System Officers (CISOs), their association and other system stakeholders indicate challenges prior to the COVID-19 pandemic in filling local IT positions generally, and InfoSec roles specifically.

Districts should discuss local action to address these shortages. To optimize funding and address local staffing shortages, the Chancellor's Office will actively use, along with other information, the cybersecurity self-assessment results to pilot development of regional teams and plan a systemwide Security Operations Center (also referred to as a SOC). The regional teams would assist local staff with security-related initiatives such as vulnerability and patch management, end-of-life replacements, and other security response and remediation initiatives. A SOC would improve the ability to proactively monitor and respond to security incidents as they occur locally and across the system. Any SOC offering would include an ability to triage security incidents and ensure that potential cyberattacks can be stopped in partnership with local staff, a service that is sorely needed.

The Chancellor's Office team is also finalizing a list of districts that would benefit most from a SOC pilot in the near term, with implementation ideally by the end of the current fiscal year. In parallel, the agency and CCC Technology Center (Tech Center) are working collaboratively to plan a systemwide SOC that optimizes existing solutions (e.g., Splunk and Tenable) and defines criteria and service level agreements for 24x7x365 support. In collaboration with system stakeholders, an RFI will be released to vendors for the initial pilot, primarily those already providing related services to CCCs, the California State University or University of California systems. More information about the SOC, including both the pilot and full implementation planning (which may include a request for proposals), as well as the regional teams will be shared in a subsequent memo.

The fall 2022 cybersecurity self-assessments represent a necessary and critical step toward financially prudent investment that will reduce the system's risk profile, ultimately improving operations and processes that impact student experiences. In response to feedback from CISOA and other IT leaders, the Chancellor's Office will provide a summary of district-specific cybersecurity gaps and suggest remediation strategies via the same portal on Monday, December 12th. At that time, staff will be able

to review their district's self-assessment findings and pose questions directly to the Chancellor's Office Team within the portal.

Bi-Annual Cybersecurity Remediation Reports

In addition to the cybersecurity self-assessments, AB 178 notes that districts must "submit remediation updates twice per year, for the fall and spring semester terms, on vulnerability and other issues identified in the previous self-assessment or triennial assessment." These remediation reports will allow the Chancellor's Office to monitor and report on remediation progress, direct resources where needed, and identify persistent security gaps that require system-level intervention and/or advocacy. Remediation reports will be due in January and July of each year as noted in a previous memo, *DII 22-300-03: September 2022 Cybersecurity Strategy Updates*.

On Monday, December 12, the district-identified representative(s) will use this same portal to submit remediation reports that focus on priorities planned for the next six months (January 1 to June 30, 2023); such reports should prioritize issues surfaced in the self-assessment including for example, InfoSec Training, End-of-Life Software, implementing Microsoft A5 Security, improving Vulnerability and Patch Management, and Penetration Testing. **Remediation reports will be due by 5:00 PM on Friday, January 20, 2023**.

The Chancellor's Office will provide three webinars to inform completion of the remediation reports:

- Monday, December 12, from 11:00 AM to 12:00 PM
- Tuesday, December 20, from 8:00 AM to 9:00 AM
- Monday, January 9, from 1:00 PM to 2:00 PM

Registration information will be sent to the same contact(s) used for the self-assessments on or shortly after Monday December 5 (not the CISO list-serve). The Chancellor's Office encourages each district representative to attend just one of these sessions. For questions about the remediation reports or the related webinars, please contact the Chancellor's Office DII Technical Assistance Provider InfoSec Lead, Stephen Heath (sheath@cccco.edu).

Triennial Security Review and Penetration Testing

A key step within any security program is the active evaluation of in-place security controls to ensure that they are functioning as expected, and that no new gaps have been introduced over time. Despite availability in previous years, district participation in free security reviews and penetration testing was extremely low. Yet, within the fall 2022 cybersecurity self-assessments, 84% of districts requested support in this area during the current fiscal year.

To acknowledge local feedback and demand, the Chancellor's Office has funded the development of and begun a security review and penetration testing program that is intended to succeed the service previously offered by the Tech Center. Five (5) districts are currently set for pilot, which is set to run through December 2022. The Chancellor's Office is prioritizing this service and aims to complete security reviews and penetration testing for all districts that requested it by June 2023.

The Chancellor's Office will contact each district requesting this service before February 2023 to establish a schedule, first prioritizing districts that have not engaged in a security review since 2020 and then as requested in the fall 2022 self-assessment.

Fraud Monitoring and Mitigation

Application, enrollment and financial aid fraud are persistent threats, despite the multiple enhancements to CCCApply that have positively impacted districts. To continue our proactive approach to combat fraud, all districts should continue to ensure that fraud is reported as requested, by individual college and in monthly increments. Such reporting is implicated in AB 178 and any district with questions or concerns should contact either Gary Bird, Information Technology Specialist II (gbird@cccco.edu) or InfoSec lead, Stephen Heath (sheath@cccco.edu).

In addition, the Chancellor's Office published an RFI to evaluate Identity Proofing technology to reliably confirm applicant identity while ensuring equitable access for real students. This is expected to further reduce the local burden of fraud mitigation on faculty and staff upon implementation. The RFI Review Committee has identified two finalists, and scheduled interviews in December to facilitate a recommendation to the Chancellor's Office as soon as January 2023. Final implementation decisions

will attend to integration capability at the system and local levels. Input from the system's technology stakeholders will continue to be solicited as this process concludes.

IT INFRASTRUCTURE AND SECURITY FUNDING ALLOCATION UPDATES

The Chancellor's Office is prioritizing FY22-23 funds in ways that align with relevant legislation, the *Vision for Success,* as well as other policy and technology priorities described below (and summarized in the following table).

In addition to the $50,000 per college each districted received in September/October, the Chancellor's Office will distribute funds in February 2023 based on information from the 2022 technology inventory, cybersecurity self-assessments (i.e., timely submission and content), as well as adoption of systemwide technology initiatives. Once finalized, details about those allocations will be shared in a memo before mid-January.

Summary of Key AB 178 Milestones (as of December 2, 2022)

Key AB 178 Milestones	Timeline/Deadline
Monthly Fraud Reporting **(by college)**	Ongoing, due by the 10th of each month
Cybersecurity Self-Assessment due	September 30, 2022
Chancellor's Office review of self-assessments and engagement with DII participatory governance groups and key stakeholders	October and November 2022
Allocation strategy updates	December 2022
Bi-annual remediation updates due	~~January 15, 2023~~ **January 20, 2023**
Allocation of FY22-23 IT and Data Security funds	At latest February 2023 (First Principal Apportionment, or P1)

Bi-annual remediation updates due	July 30, 2023
FY23-24 Cybersecurity Self-Assessment released	August 2023 (Anticipated)

In addition to the February 2023 allocation, the Chancellor's Office anticipates an additional spring 2023 allocation informed by information from the remediation reports, any after-action reports, professional services pilots, and other input from CISOs and relevant system stakeholders.

Security Upgrades for CCCApply and Quality Online Education

To ensure a smooth student application and enrollment process and high-quality online educational experiences, the system must have a reliable and secure online infrastructure. The absence of system-level IT standards alongside chronically under-resourced districts has resulted in diverse local technology ecosystems that inhibit within-system opportunities to share IT capacity. Of note, the cybersecurity self-assessments requested district feedback about how the Chancellor's Office might better support local InfoSec efforts. The most common response was for the agency to provide more cybersecurity guidance and standards which, among other things, would establish stronger protections of Personally Identifiable Information (of students and all employees) but also facilitate a more robust IT infrastructure that ensures students' have access to the on-demand resources they increasingly expect.

In response, the Chancellor's Office will use available funding to address historical and ongoing concerns about CCCApply security in at least two ways. First through the systemwide implementation of Identity Proofing in 2023. Second, the Chancellor's Office has been working to determine the extent to which a systemwide application redesign or overhaul is needed to address security vulnerability. This work is being done in partnership with the Tech Center and California Virtual Campus (CVC) teams, as well as external consulting support that is charged with engaging a diverse set of system stakeholders. As part of that review, and in addition to ongoing enhancements to the security of CCCApply, the Chancellor's Office will also conduct a comprehensive review of the systemwide application content and user experience in 2023. This will continue efforts to improve its performance and early student experiences with colleges in our system. More information about CCCApply security upgrades will be shared, as relevant.

Prior to FY22-23, the Chancellor's Office has also requested adoption of technologies meant to improve systemwide performance; however, some have yet to be fully implemented by districts. For example, SuperGlue (housed at the Tech Center) was adopted more than four years ago to provide a common integration platform that would accommodate diversity in local technology operations. Nearly a decade ago, the Course Exchange (hosted by CVC) was developed to provide students with access to online courses across the system without needing to submit an additional application. Uneven adoption of these tools hamstrings the system's ability to benefit from economies of scale for technology purchases and contracting, including solicitation of professional services to support local work. Further, this diversity can burden students, faculty and staff who must negotiate many more technology tools and platforms than is necessary. Feedback from the TTAC, SAC, CISOA and local leaders in and outside of IT consistently note that adoption of these and other systemwide technology investments often stalls due to lack of local IT capacity. Full implementation is necessary to address the system's security profile but also impact other critical issues associated with quality online education.

Regional teams are being designed to prioritize existing state-level technology investments. Along with development of stronger security guidelines and standards, these implementation support teams are expected to accelerate systemwide technology adoption, facilitate simplification of the IT ecosystem, and simultaneously increase systemwide IT capacity. This will improve opportunities for more within-system learning to complement existing district IT and security strategies. For example, system-supported professional development to improve institutional effectiveness, like Peer Resource Teams, could be used more frequently to help offset staffing deficiencies in IT.

The CCC IT infrastructure and security strategy is complex, reflecting an unprecedented state investment in IT that necessitates shifts in local and system-level work. Districts are responsible for local decision-making and the Chancellor's Office remains committed to partnership that will support compliance with ACCJC standards, reductions in vulnerability, and expansion of access that reflects contemporary issues of access and security. Of note, the self-assessments requested that the Chancellor's Office help by supporting local implementation, training, security audits and compliance, sharing templates, providing and advocating for additional funding, nearly all of which is accounted for in the multi-year plans described previously and in this memo that will continue to evolve.

For any questions or concerns, please do not hesitate to the designated staff or me at vlundywagner@cccco.edu.

cc: Daisy Gonzales, Interim Chancellor
Lizette Navarette, Interim Deputy Chancellor
John Hetts, Executive Vice Chancellor
Marty Alvarado, Executive Vice Chancellor
Gary Bird, Information Technology Specialist II