California Community Colleges

MEMORANDUM
September 28, 2022

DII 22-300-03 | Via Email

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

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

RE: September 2022 Cybersecurity Strategy Updates

The 2022 Budget Act included AB 178 (2022) and AB 183 (2022) which allocate $25 million in ongoing funds and $75 million in one-time funds to help the California Community Colleges improve, among other things, data security oversight, fraud mitigation, and IT infrastructure. This memo provides specific information about recent activity and funding decisions related to those topics, eligibility for and key milestones related to AB 178 funding, and fraud-related updates.

RECENT FUNDING DECISIONS

Seed Funding

As noted in memo *DII 22-300-01: Preparation for Allocation of FY22-23 IT and Security Funding*, the Chancellor's Office is allocating to districts $50,000 per college within each district in September 2022. These funds are intended to support completion of the Cybersecurity Self-Assessment (described below) as well as other planned or in-progress work.

Microsoft A5 Security Licensing

To raise the security baseline of all colleges and districts, the Chancellor's Office purchased the Microsoft A5 Security Suite for the entire system in September 2022. This will cover the cost of upgrading from Microsoft A3 licensing (that colleges already have) to include the A5 Security Suite.

The Chancellor's office has received questions about how the Microsoft A5 Security Suite license will affect districts that primarily use Google Workspaces and Gmail. The benefits of this license will be realized by all districts given the Endpoint Detection and Response capabilities and Microsoft Defender for Cloud Apps, regardless of the choice to use Microsoft Office and Office365 or Google Workspaces and Gmail. For more information on how the A5 Security Suite supports Google Workspaces, please visit: https://learn.microsoft.com/en-us/defender-cloud-apps/protect-google-workspace

Given that local districts may not have capacity to fully implement features of the A5 Security Suite, the Chancellor's Office is collaborating with Microsoft to support districts who need additional assistance. In addition, the Chancellor's Office also recognizes that the A5 Security Suite covers endpoints only and thus is evaluating the cost of providing additional security licensing for servers (both on premises and cloud). Eligibility for assistance related to implementation capacity and servers will be determined after the Cybersecurity Self-Assessments are reviewed.

UPDATES ON ELIGIBILITY FOR AB 178 (ONGOING) FUNDS IN FY 22-23

Eligibility for ongoing funds through AB178 includes completion of the annual cybersecurity self-assessment, bi-annual remediation updates, a triennial security review and penetration testing, as well as regular fraud reporting. The annual technology application inventory will be released for local validation in spring 2023.

Cybersecurity Self-Assessment

The Cybersecurity Self-Assessment, described here, was released in late August 2022 and is due **Friday, September 30, 2022 at 5:00 PM**. To date, more than half of the system's districts have completed the self-assessment and all have made notable progress. Local leaders are encouraged complete the self-assessment on time to maximize eligibility for AB 178 funds. Information from the self-assessment will be used by the Chancellor's Office to determine how remaining AB 178

funds will be allocated to make the greatest impact on improving data security, fraud mitigation, and IT infrastructure across the system.

Bi-Annual Cybersecurity Remediation Reports

Pursuant to AB 178, 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 be due on January 15 and July 30 of each year and will be completed via the same portal as the Cybersecurity Self-Assessment (unless otherwise noted).

Instructions for how to complete remediation reports will be sent to each district's primary contact in November and May of each year. Additional details related to the remediation reports will be provided in a subsequent memo.

Triennial Security Review and Penetration Testing

Starting in October 2022, the Chancellor's Office will begin providing a full security review and penetration test to each district once every three years. This service will be performed collaboratively with districts and is intended to assist in validating the effectiveness of in-place security controls, as well as identifying gaps in and providing an actionable remediation plan for each district's current security infrastructure. This service is intended to replace the penetration testing service previously provided by the California Community Colleges Technology Center (Tech Center).

Districts who wish to perform the Triennial Security Review and Penetration Test in the current fiscal year, should indicate their interest within the Cybersecurity Self-Assessment or by contacting Stephen Heath (sheath@cccco.edu). Priority will be given to districts who have not performed a similar assessment since FY20-21.

Monthly Fraud Reporting

Since August 2021, the Chancellor's Office has requested reporting on suspected and confirmed fraudulent activity monthly by college. Data should continue to be submitted by the 10th of each month **for each individual** college using the same process. To maximize AB 178 funding available, colleges will need to consistently report on fraud each month, including if there was no fraud detected that month. Colleges or districts who need support for this reporting should reach out to the Technical Assistance Provider (TAP) Information Security Lead, Stephen Heath (sheath@cccco.edu) or their College Relationship Manager (crms@ccctechcenter.org) for assistance.

The Chancellor's Office has received requests to modify the current fraud reporting protocol and is evaluating alternatives that reduce local burden but will still allow for timely system-level monitoring and action. Any changes to the process will be communicated to the field in advance of implementation.

Summary of Key AB 178 Milestones (as of September 28, 2022)

Key AB 178 Milestones	Timeline/Deadline
Monthly Fraud Reporting	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

Key AB 178 Milestones	Timeline/Deadline
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)

OTHER FRAUD-RELATED UPDATES

ID Proofing RFI

Identity Proofing (or ID Proofing) attempts to establish and confirm a valid digital identity for any given person and has been used by many public and private institutions to reduce fraud. As noted in previous memos, the Chancellor's Office sees this technology as a viable systemwide option for reducing application, enrollment, and financial aid fraud within the California Community Colleges.

A non-binding request for information (RFI) was issued in May 2022 to obtain vendor proposals for ID Proofing solutions. A cross-functional review committee comprised of system leaders in IT, Student Services, Financial Aid, and Security at the system and local levels was assembled to review RFI submissions. Recommendations from the committee and the TAP team will be used to determine next steps for an RFP and/or procurement by December 2022. Additional information will be shared about a systemwide ID Proofing solution as it becomes available.

Increasingly Sophisticated Fraud

Colleges and districts have reported an increase in the sophistication of fraud actors targeting our system. Details on these new attack vectors are being distributed to the appropriate district

contacts via the Tech Center College Relationship Managers (CRMs). If you are unaware of your CRM, please email crms@ccctechcenter.org.

In response to this evolution and to provide updates on other anti-fraud activity, the Chancellor's Office will host a webinar on **Thursday, October 27, 2022, from 11:00 AM to 12:30 PM**. Topics for discussion will include an update on the ID Proofing RFI process, the systemwide implementation of IP Quality Score, and recent fraud techniques observed by district staff, the Chancellor's Office and Department of Education Office of the Inspector General. While oriented largely toward IT and security staff, stakeholders across local institutions are welcome. Registration details for this webinar will be released soon but please hold time on calendars in the meantime.

Security Operations Center Planning

In July 2022, the Chancellor's Office began investigating options for a systemwide Security Operations Center (SOC). The goal is to provide a proactive first line of defense for the system, allowing districts to detect and respond to cyberattacks like ransomware, before they become a full-fledged cyber incident. The end goal of a SOC is to provide a service that would include:

- SIEM platform
- 24x7x365 coverage
- Service Level Agreements based on criticality
- Ability to perform triage based on playbook
- Threat Hunting and Incident Response support

The Chancellor's Office is eager to learn from local system leaders and our state partners to inform an equitable, system-level approach, including how to better leverage the Security Center. A survey will be distributed via the CISO list-serve in coming weeks to solicit information from the field about existing local SOC contracts, including scope, terms, cost, etc.

In addition, the Chancellor's Office has been in touch with the California State University Chancellor's Office, University of California Office of the President, and the California Department of Technology to learn about their solutions and experiences with using and/or implementing a SOC. Collated information about potential SOC options will be shared with relevant participatory governance groups and other stakeholders for their input and advice.

The Chancellor's Office is working to minimize system-level vulnerabilities as soon as possible, so timely submission of requested data is critical to the FY 22-23 strategy. Please expect monthly memos through 2022 to learn about updates related to the system's IT infrastructure and cybersecurity strategy. In the meantime, should you have any questions or need further assistance, please contact me at vlundywagner@cccco.edu or 916-322-1928.

cc: Daisy Gonzales, Interim Chancellor
Lizette Navarette, Interim Deputy Chancellor
John Hetts, Executive Vice Chancellor
Marty Alvarado, Executive Vice Chancellor
Rebecca Ruan-O'Shaughnessy, Vice Chancellor
Aisha Lowe, Vice Chancellor