California Community Colleges

MEMORANDUM
August 4, 2022

DII 22-300-01 | Via Email

TO: Chief Executive Officers
Chief Information Systems Officer Association
Chief Business Officers

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

RE: Preparation for Allocation of FY 22-23 Information Technology and Security Funding (UPDATE)

In recognition of persistent college and district security risks and ongoing efforts to improve data security oversight, fraud mitigation, and online learning quality, the 2022 Budget Act, through AB 178 and AB 182, provides $75 million in one-time and $25 million in ongoing funds toward the implementation of local and systemwide technology and data security efforts.

This memo outlines key steps colleges and districts should take prior to the complete allocation of funds, a timeline of deliverables, and a plan for supporting districts throughout the process. During the first quarter (Q1) of fiscal year (FY) 2022-2023, colleges and/or districts are expected to complete the local technology inventory, implement the systemwide Identity and Access Management (IAM) license, and complete the Cybersecurity Self-Assessment. The Chancellor's Office will support the system by providing the Microsoft M365 A5 Security Suite license for IAM, facilitating completion of the Identity Proofing technology review, and planning for a systemwide Security Operations Center, as outlined below.

Summary of Key Dates (as of August 1, 2022)

Deliverable	Timeline
Technology Inventory completed systemwide	ASAP
Systemwide Microsoft M365 A5 Security Suite license secured	August 2022

Cybersecurity Self-Assessment released	August 2022
ID Proofing vendor submission review begins	August 2022
IT and Data Security base funds provided to districts ($50,000 per college)	September 2022
Cybersecurity Self-Assessments review begins	September 2022
Allocation of IT and Data Security funds	First Principal Apportionment (P1) February 2023

STEPS TO PREPARE FOR LOCAL ALLOCATIONS

Complete the Local Technology Inventory

In alignment with the *Vision for Success,* the Chancellor's Office is firmly committed to digital equity and ensuring the protection of all 116 colleges and 73 districts as well as the students they serve. To understand disparities related to information technology (IT) infrastructure across the system, for the first time, the Chancellor's Office rolled out a technology application inventory in March 2022. The purpose of this inventory was to better understand the extent to which systemwide technology investments were being leveraged, and surface initial information about the type of capacity colleges and districts have for IT, security, and accessibility. This information will be used in concert with the cybersecurity self-assessment (mentioned later in this memo) for design of the one-time and ongoing funding allocations.

As of today, 106 of 116 colleges have completed this inventory. If you are unsure if your college has completed this inventory or if you have questions about it, please contact Rupal Shah, Chancellor's Office Technical Assistance Provider (TAP) Lead Enterprise Architect at rshah@cccco.edu or your college relationship manager at the California Community Colleges Technology (Tech) Center via crms@ccctechcenter.org.

Implement Identity and Access Management

In FY21-22, the Chancellor's Office directed the DII TAP and Tech Center team to review Identity and Access Management (IAM) options shared by the Telecommunications and Technology Advisory Committee (TTAC) and partner groups (e.g., Chief Information Systems Officers Association leadership). IAM is a system that manages, maintain, and protects an individual's identity. A thorough analysis was conducted on two vendors focusing on current offerings, strategy, market presence, technology costs, local implementation capacity needs, and other known information (e.g., from the technology inventory).

To ensure that all colleges can benefit from the systemwide IAM investment (near) **immediately**, the Chancellor's Office will use one-time AB 182 funds for an extended period contract to purchase the Microsoft M365 A5 Security Suite for all colleges and districts starting in FY2022-23. This cost associated with this will shift to ongoing funds no sooner than FY2024-25.

The Microsoft M365 A5 Security Suite includes many advanced security features beyond IAM, including Multi-Factor Authentication, Endpoint Detection and Response, Data Loss Prevention, Privileged Identity Management, Identity Governance and Auditing, as well as many other technical features that may not be currently available to colleges.

The Chancellor's Office is in ongoing discussion with CollegeBuys, Microsoft, ComputerLand, and the Tech Center to ensure this plan moves forward. Colleges subscribing to the full M365 A5 Security Suite can expect a $31.44 per Education Qualified User (EQU) discount off the regular CollegeBuys price offered by ComputerLand for the September 2022 anniversary order, and those newly subscribing to the M365 A3 + the M365 A5 Security Suite will receive a price of $0 for the M365 A5 Security Suite. Please review communications from ComputerLand for pertinent deadlines.

Given that many colleges and districts are likely to face challenges implementing the M365 A5 Security Suite license, one-time funding for professional services will be available to colleges with limited capacity to ensure that this investment is maximized. Additional details on how to request these services will be provided in a forthcoming memo and based at least in part on the technology inventory and cybersecurity self-assessments.

Complete the Cybersecurity Self-Assessment

Pursuant to the AB 178 legislation, as a condition of receiving cybersecurity funds and services, districts must complete an annual Cybersecurity Self-Assessment. This will provide the Chancellor's Office with information that helps ensure local vulnerabilities are prioritized and remediated through a combination of the one-time and ongoing state funds. The cybersecurity self-assessment will be used to determine alignment with the National Institute of Standards and Technology (NIST) Computer Systems Laboratory (CSL) score and report on their current phase in Cal-Secure standards.

The Chancellor's Office has requested feedback on the cybersecurity self-assessment from members of the Systemwide Architecture Committee (SAC), a subset of TTAC. This feedback will be used to help the Chancellor's Office reduce the local burden so college and/or district leaders can complete it in a timely manner.

The Chancellor's Office will release a memo by mid-August describing the process for completing the self-assessment, which will be sent via the CISO list-serve. Please note staff are added to the CISO list based on district-specific designation with local IT offices. For colleges that share IT responsibility across their district, please consider working together in order to complete the self-assessment as necessary and relevant.

Information on how to complete the self-assessment will be provided in upcoming webinars and virtual office hours in August and later as necessary. Registration information for these sessions will also be disseminated on the CISOA list-serv over the next few weeks. Following the webinars, questions regarding the self-assessments should be directed to TAP Information Security Lead, Stephen Heath (sheath@cccco.edu).

Immediate Funds to Districts

Pursuant to the AB 182 legislation, $75 million is available for in one-time funds to implement technology and data security measures. Given ongoing work to improve IT infrastructure and security, the Chancellor's Office will distribute base funds of $50,000 **to each district** in September 2022. Such funding should be used to support local and system priorities in alignment with AB 182 and may be

used to support timely completion of the technology inventory and forthcoming cybersecurity self-assessment.

Review of Identify (ID) Proofing Options

Systemwide ID Proofing systems will help reduce fraud by reliably confirming the identity of admission applicants in OpenCCC and CCCApply and is expected to significantly reduce the local workload by staff in Admissions and Records, Financial Aid and IT departments. After engaging TTAC and CISOA members, a request for information (or RFI) was opened in May 2022 to understand the ID Proofing market. The Chancellor's Office received multiple vendor responses and in coming days, a review committee – comprised primarily of SAC members - will review vendor submissions and provide the Chancellor's Office with a criteria-based recommendation for systemwide investment and inform appropriate next steps.

Security Operations Center

A long-identified need of the system is a centralized Security Operations Center (or SOC) that can provide Security Incident and Event Manager (SIEM) technologies as well as Managed Detection and Response (MDR) services. The purpose of establishing a systemwide SOC is to establish a team of experts that proactively monitor cybersecurity capabilities, coordinate around incident response and mitigation, as well as remediation and compliance support. The Chancellor's Office has already begun to engage with the Tech Center and Security Center, as well as TTAC and SAC, to refocus systemwide security supports made available and how to determine a baseline level of Incident Response for the system. In addition, the Chancellor's Office will engage with other public education segments and state agencies to understand scope, costs, efficiencies, etc. The Chancellor's Office anticipates completing a draft plan for a systemwide Security Operations Center this fall.

More information on the systemwide strategy for IT and security, including the allocation of one-time and ongoing funds to colleges and districts will be shared in more regular memos (likely monthly). The Chancellor's Office encourages timely completion of the technology inventory, self-assessment, and any subsequent asks so that decisions can be made equitably and expeditiously.

In the meantime, if you need assistance related to your local cybersecurity posture, please reach out to DII TAP Information Security Lead, Stephen Heath (sheath@cccco.edu). For any other questions or concerns, do not hesitate to contact me at vlundywagner@cccco.edu or 916-322-1928.

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