California Community Colleges

MEMORANDUM
August 11, 2022

DII 22-200-01 | 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: FY 22-23 Cybersecurity Self-Assessments (AB 178)

AB 178 (2022) provides on-going funds to help address local- and system-level disparities in information technology (IT) and security infrastructure, including hiring of local cybersecurity staff, upgrades for CCCApply and education technology platforms as well as the establishment of systemwide cybersecurity teams. **As a condition of receiving AB 178 funds**, each community college district must complete an annual cybersecurity self-assessment, and participate in a series of activities (i.e., submission of remediation updates, after-action reports, monthly and annual number of fraudulent and likely fraudulent admission applications and enrollments as well as fraudulent receipt of financial aid). More detail associated with these activities is described in the legislation here (see page 314 of 383 of the pdf file); how participation in these activities will be incorporated into the distribution of funds and will be addressed more thoroughly in a subsequent memo.

This memo provides information primarily about the annual Cybersecurity Self-Assessment referenced in AB 178, including the process to complete it, as well as timelines for webinars and "office hours," and submission during the fiscal year 2022-2023 (FY22-23). Information gathered as part of the annual cybersecurity self-assessment and monthly fraud reporting (since August 2021), the technology application inventory, and other input from participatory governance groups will ultimately help ensure funds from AB 178 and AB 183 are maximized effectively and equitably.

Background

The 2022 Budget Act, through AB 178 and AB 183, provides $25 million in ongoing and $75 million in one-time funds to help the California Community College system of 116 colleges and 73 districts

support implementation of technology and data security efforts. While work is underway to improve the systemwide application and associated technologies, a key system-level vulnerability is the lack of standards for local and system IT and security. Inequities in local IT infrastructure and security can adversely affect student experiences, prevent a system-level standard of 'adequacy,' as well as the ability identify and support appropriate local and/or system-level solutions.

Cybersecurity Self-Assessment Overview

Pursuant to the AB 178 legislation, one eligibility requirement for receiving cybersecurity funds is completing an annual Cybersecurity Self-Assessment. To expedite the process, in FY22-23 the Chancellor's Office will design the Cybersecurity Self-Assessment and obtain feedback from the Systemwide Architecture Committee (SAC) and other IT leaders. The assessment will reflect system-level priorities as well as other topics that can inform both local- and system-level distribution of ongoing but also one-time funds.

The Cybersecurity Self-Assessment will identify a district-specific risk level in alignment with the NIST Cyber Security Framework (CSF) and Center for Internet Security (CIS) controls. The risk level and other information gathered by the Chancellor's Office (e.g., the technology application inventory) will be used to guide the design of system-level security and other supports (i.e., Systemwide Cybersecurity Teams and Systemwide Security Operations Center).

The Cybersecurity Self-Assessment contains questions related to the current cybersecurity posture of each college and district and is organized into topics, including but not limited to, Asset Inventory, Data Protection, Network Defense, Audit Log Management, Vulnerability Management, Application Software Security, Email and Web Browser Protection, Audit Log Management, Malware Defenses, Data Recovery, Network Infrastructure, and Incident Response. The Chancellor's Office is mindful of variation in capacity, so steps have been taken to minimize the local workload associated with completing the self-assessment. As a result, the Cybersecurity Self-Assessment is structured with a series of questions with discrete response options (i.e., "Yes," "Partial," or "No") and relatively few requests for open-ended responses.

Learn about the Self-Assessment

The Chancellor's Office is hosting a series of webinars and office hours over the next month to ensure shared expectations and understanding on its content but also where, how, and when to complete the Cybersecurity Self-Assessment. There will be two 1-hour webinars for local leaders to obtain information:

- Friday, August 19 at 9:00 AM, and
- Monday, August 22 at 11:00 AM.

District CISOs (or equivalent point of contact) should register for one of the two informational webinars here.

The Cybersecurity Self-Assessment will be released on **Monday, August 22** to the district CISO contact. Districts should identify one point of contact and ensure they are able to receive necessary information.

Please make sure district CISO-list contacts are up-to-date with the Tech Center as noted under the "*How to Subscribe to the Alias List*," here. If the CISO contact will not serve as the self-assessment point of contact, please reach out to DII Technical Assistance Provider (TAP) Information Security Lead, Stephen Heath (sheath@cccco.edu) at your earliest convenience. Once appropriately validated, the self-assessment dissemination tool will be updated.

For colleges that share IT responsibility across a district, leaders are encouraged to collaboratively complete the self-assessment. The Chancellor's Office team expects that the self-assessment should take no more than approximately 2-hours to complete.

Self-Assessment Office Hours

The Chancellor's Office will host a series of virtual "office hours" to make space for relevant points of contact so they may ask questions about the Cybersecurity Self-Assessment and process for completion. District points of contact are encouraged to attend any of the 1-hour sessions as questions about the self-assessment surface. The office hours will leverage breakout rooms to provide

an appropriate level of confidentiality. The Chancellor's Office will also monitor RSVPs and attendance.

A link to register for office hours will be sent to CISO list-serve within the next week.

Office hours are the preferred venue for discussing the Cybersecurity Self-Assessment; however, the Chancellor's Office team will work with all districts to ensure timely completion of the self-assessment to prevent unnecessary delay in the allocation of one-time and ongoing funds. The Chancellor's Office will add office hours or provide additional guidance to the field, as needed.

The deadline for completing the FY22-23 Cybersecurity Self-Assessment is **Friday, September 30 at 5:00 PM**. Districts should proactively communicate with the Chancellor's Office if delays are anticipated.

Summary of Key AB 178 Milestones (as of August 11, 2022)

Key AB 178 Milestones	Timeline/Deadline
Cybersecurity Self-Assessment Overview webinars	August 19, 2022 and August 22, 2022
Cybersecurity Self-Assessment distributed	August 22, 2022
Cybersecurity Self-Assessment Office Hours	Multiple between August 2022 and September 2022 (to be distributed via the CISO list-serve)
Cybersecurity Self-Assessment due	September 30, 2022
Chancellor's Office review and engagement with DII participatory governance groups	October and November 2022
Allocation strategy announcements	December 2022
Bi-annual remediation updates due	January 15, 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)

The Chancellor's Office will continue to provide memos with updates on the allocation of FY22-23 IT and Data Security Funds prior to and likely after the First Principal Apportionment, as needed.

For questions about the self-assessment itself, related webinars or office hours, please contact DII TAP Information Security Lead, Stephen Heath (sheath@cccco.edu).

For any other questions or concerns, please do not hesitate to contact me at vlundywagner@cccco.edu.

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