California Community Colleges

MEMORANDUM

January 20, 2023

DII 23-300-01 | Via Email

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

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

RE: FY 22-23 January IT Infrastructure and Cybersecurity Funding Updates (RE-NUMBERED)

The 2022 Budget Act included Assembly Bill (AB) 178 and AB 183, which allocate $25 million in ongoing and $75 million in one-time funds to the California Community Colleges (CCCs). This legislation seeks to improve, at both the local and system level, among other things, data security oversight, fraud mitigation, and information technology (IT) infrastructure. This funding will help ensure continuous delivery of education and supports for all CCC applicants and students, regardless of their address or preferred modality. This memo provides information about six goals in calendar year 2033 and the associated distribution of funds.

IT Infrastructure and Cybersecurity Priorities

Chronic underfunding of CCC IT departments, as well as ongoing threats of fraud and cyberattacks have exposed inequities in districts' ability to manage the rapidly evolving technology landscape in recent years – a challenge facing most community colleges nationwide. Although the Chancellor's Office previously had no insight into local IT infrastructure and operations, a favorable 2022 State Budget shifted this, and facilitated development of a strategy to better understand local gaps to better direct state funding.

To improve the CCC system's security profile, the Chancellor's Office solicited information to inform the first enterprise-level understanding of IT via:

1. Submission of monthly fraud reporting by college or district (since August 2021),
2. Completion of the technology inventory results (March/April 2022), and
3. Submission of the fall 2022 Cybersecurity Self-Assessment (September 2022).
4. Submission of bi-annual remediation reports (due January 20, 2023)

All 116 colleges and 73 districts have provided requested information to date. Analysis of these initial, cross-sectional data points revealed uneven adoption of system technology investments across colleges and districts as well as a pervasive need to improve IT infrastructure and security. The results point to **six goals that could reasonably be achieved by December 31, 2023**, and will fundamentally support long-term delivery of online education, improve the local and system IT infrastructure as well as the system's security profile:

- **Systemwide implementation of the Microsoft A5 Security Suite** – cybersecurity basics like Multi-factor Authentication, Endpoint Detection and Response, Local Single Sign-On, and Privileged Access Management should be part of any local security program
- **Systemwide implementation of Vulnerability Scanning** – local awareness of vulnerabilities can ensure leaders understand their district's risk and manage it appropriately, leveraging system-supported tools as appropriate
- **Systemwide adoption of SuperGlue** – given local variation in IT operations and delivery of education this integration platform can help ease the local burden on data management, reporting and fraud monitoring
- **Systemwide implementation of the Course Exchange** – to take advantage of existing system-level investment, bolster efforts to meet the increased demand for online education and help alleviate persistent enrollment declines

- **All districts progress on eliminating End-of-Life (EOL)** technology – operating systems, hardware and software products without vendor support have vulnerabilities that attackers can exploit and should be removed from service as soon as possible
- **All districts mature Information Security training** – industry best practice includes annual training for all employees, which all districts have access to for free within the Vision Resource Center

Achieving these goals by December 31, 2023, would allow the Chancellor's Office to support districts on myriad other IT issues (e.g., transitions to the cloud, technology solution changes, adoption of technology to support enrollment, like Competency-based Education, preparation for implementation of the Cradle to Career data system, penetration testing, etc.). These steps are anticipated to significantly improve local institutions' operations, ability to secure cyber insurance and long-term cost savings.

LOCAL FUNDING AND RESOURCE ALLOCATIONS

District Allocations

To achieve the six goals above by December 31, 2023, districts were organized into three levels of need based on the following factors and weights:

Scoring Factors	Approximate Weights
Fall 2022 Cybersecurity Self-assessment	50%
Recent victim of and similarity to recent district(s) facing cyberattack	20%
IT staffing level	15%

Scoring Factors	Approximate Weights
End-of-Life software risk	5%
Information Security staffing level	5%
Systemwide technology implementation	5%

Districts will be notified of their identified level of need through an automated email from the self-assessment and remediation reporting portal to designated contacts.

The corresponding one-time funding allocation of AB 178 funds to districts will be:

Level of District Need	District Allocation
HIGH	$200,000
MODERATE	$150,000
LOW	$100,000

District Implementation Support Vehicles

In FY22-23, implementation support to districts will focus primarily on the Microsoft A5 Security Suite, Tenable, and the Course Exchange. Feedback from the CCC Technology Center (Tech Center), California Virtual Campus (CVC), Chief Information System Officer Association (CISOA) and other IT staff suggests that implementation support will be necessary for many districts. In response, and to accelerate timely progress on these goals, the Chancellor's Office will subsidize implementation

support annually through two vehicles: “implementation teams” and “regional support teams.” Whereas the former will support more discrete, one-time implementations, the latter will provide districts with direct ongoing assistance to fill gaps associated with chronic IT staffing shortages.

There is already local support available at no cost for some goals. The Tech Center (which also hosts the Security Center) provides implementation support for SuperGlue and holds a license for Tenable; for information, please contact your College Relationship Manager at crms@ccctechcenter.org. CVC provides implementation support for the Course Exchange; for assistance, please contact support@cvc.edu. The license for Microsoft is available through CollegeBuys.

The Chancellor’s Office will use results of the Microsoft A5 Security Suite implementation pilot currently underway to inform the final design of implementation teams in February 2023. All districts will have access to Microsoft implementation teams with three levels of service that correspond to the district levels of need:

- High need = full implementation service to be completed by a certified third-party vendor, paid for by the Chancellor’s Office with state funds
- Moderate need = local district implements basic components with completion of the integration by a certified third party, paid for by the district
- Low need = local district implements fully and completes a ‘health check’ by a certified third party, paid for by the district

Each Microsoft implementation team service package will be available to all districts as part of the existing systemwide contract and with negotiated pricing. High-need districts are strongly recommended to use the high-need implementation service package and schedule support by the end of Q3 FY22-23 (to satisfy the implementation target of December 31, 2023). The moderate and

low-need implementation team service packages are recommended for the corresponding districts, though they may choose alternative approaches.

Additional FY22-23 District Funding Allocations

The Chancellor's Office anticipates using a combination of AB 178 and AB 183 funds to support local decommissioning of End-of-Life (or EOL) operating systems, hardware, and software and based largely on remediation report submissions. However, EOL is a long-term and ongoing project for any enterprise and systemwide support will be contingent upon remaining funding, goals, and priorities. Districts should report on each goal in the June 2023 remediation report and any subsequent required reporting to inform the Chancellor's Office of progress.

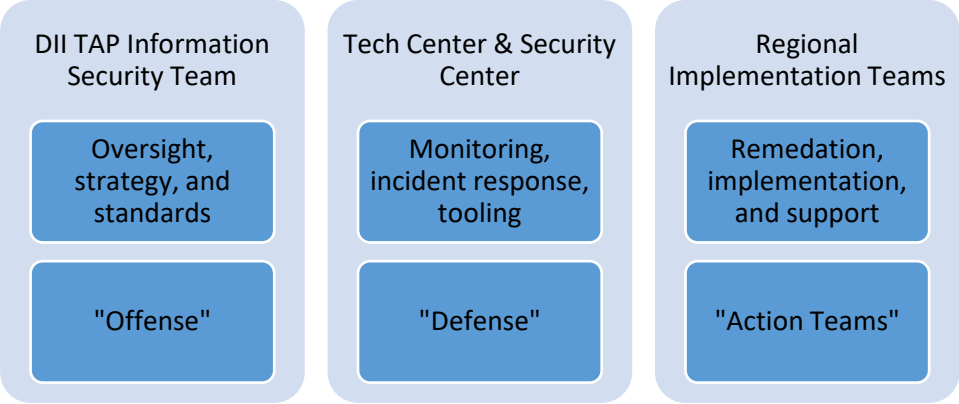
SYSTEM FUNDING AND RESOURCE ALLOCATIONS

State investment also includes funding for system-level support to improve both system and local IT operations, online education, and security for the benefit of CCC students. A security strategy frames this work, but also attends to existing technology initiatives and readiness for the future education and workforce training need.

System Security Strategy

The 2022 State Budget reflects an unprecedented investment in CCCs IT infrastructure with notable, albeit limited resources. The Chancellor's Office is working to establish a new operational model to sustainably and systematically support local alignment with the Governor's Cal-Secure framework of cybersecurity capabilities (see page 7 here), while simultaneously encouraging statewide technology initiatives already underway. By using the Cal-Secure framework, the Chancellor's Office can better guide state investments that accelerate local adoption and optimize existing resources.

The current FY22-23 approach to security for the CCC system can be characterized by the following diagram:



Note: DII TAP refers to the Digital Innovation and Infrastructure Technical Assistance Provider team

This was designed and vetted with system stakeholders starting in July 2022 to ensure a comprehensive system-level strategy that attends to diverse local need. As the system-level strategy evolves, this framework and partners will be updated. The reporting required under AB 178 complements this framework by ensuring consistent formal communication between the field and Chancellor's Office, as well as facilitating timely response by the agency through funding and resource allocations.

FY22-23 System Security Priorities

- **Support for local compliance with AB 178 to maximize district allocations** by issuing guidance, hosting office hours or webinars, and providing support to ensure timely and accurate submissions (e.g., fraud monitoring, annual self-assessment, after-action reports, or bi-annual remediation reports). In FY22-23, this is supported through AB 183.
- **Additional support for basic cybersecurity controls** through purchase of the Microsoft A5 Security Suite licenses for all colleges in FY22-23 and the Microsoft Defender for Servers starting in FY23-24. Based on district submissions to date, these annual subscriptions will cost

approximately $5.5M under the existing CollegeBuys-negotiated contract, which runs through FY25-26. These subscriptions will be funded through a combination of funding sources, and eventually just through AB 178. Renewal and future costs will be renegotiated and communicated before end of FY25-26.

- **Implement an ID Proofing Solution to reduce application fraud** in summer/fall 2023 at the system-level, through the Tech Center, to minimize local burden as much as possible. Initially, this will be funded through a combination of AB 178 and AB 183, and eventually just AB 178.
- **Pilot a Security Operations Center (SOC) to provide logging, monitoring and detection support, and provide basic response capabilities to block bad actors** in partnership with the Tech Center/Security Center starting during FY22-23. Lessons learned through FY23-24 will be used to inform a systemwide SOC to be implemented no sooner than FY24-25. This will be funded through AB 178 and AB 183.
- **Pilot implementation and regional support teams to complement local IT capacity** by learning from pilots and revisiting roles and responsibilities of other all system-level supports, including the Enabling Services unit, Security Center, Course Exchange implementation team, Digital Innovation and Infrastructure Technical Assistance Provider (TAP) team, and Partnership Response Teams.
- **Fund Penetration Testing and Cybersecurity Reviews** to validate that local and systemwide security controls are working as expected and with confirmation through districts AB178 reporting. The Chancellor's Office will complete a pilot of this service in FY22-23 with five districts, which will inform additional system-level support.
- **Improve Incident Response and Recovery Guidance** to support the continuity of local operations and the restoration of services for institutions under attack. The Chancellor's Office is working with local IT leaders who have already begun to develop a detailed Incident Response and Recovery playbook for dissemination by July 1, 2023. AB 183 funds will be used to support this effort.

Additional FY22-23 System Funding Allocations

In addition to coordinating previously mentioned work, the Chancellor's Office initiated contracts to facilitate engagement on two long-standing issues. In response to student, educator, legislator, advocacy and system stakeholder concerns about the length, complexity, and accessibility of the systemwide application (CCCApply), the agency has begun interviews with the Tech Center, Consultation Council, and other technology-focused participatory governance groups. The goal is to gather input that will inform the evolution of the systemwide application, state-level advocacy, and local technology investments.

Building from decades long conversation about the immature systemwide data management strategy and resultant local reporting challenges, the Chancellor's Office has also initiated stakeholder interviews and focus groups about a common, systemwide enterprise resource planning (ERP). Part of the Governor's Recovery with Equity Roadmap, this major long-term effort requires attention to myriad stakeholders to ensure shared understanding of the opportunity, anticipate challenges, define a realistic scope, develop action plans, and ensure local technology readiness. These efforts are being funded primarily through AB 183.

The Chancellor's Office understands that IT is the backbone of college and district operations, and as such, will continue to collaborate with local leaders, participatory governance groups and other stakeholders to support awareness of and provide support for IT infrastructure issues, especially those that implicate student experiences, security, and delivery of online education. The proposed timeline is ambitious, but the Chancellor's Office will work with all parties to accelerate work and optimize outcomes.

For any other questions or concerns about this memo, please do not hesitate to contact 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
Russell Grant, Information Technology Specialist I