California Community Colleges

MEMORANDUM
May 3, 2024

DII 24-200-02 | 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: Systemwide Security Priorities: Pentesting, SOC, and Immutable Cloud Backups

The 2022 Budget Act included Assembly Bill (AB) 178 and AB 183, which allocated ongoing and one-time funds for the California Community College (CCC) districts to, among other things, implement local and systemwide technology and data security measures. Since 2022, the system has made significant progress to mature local district and systemwide cybersecurity capabilities; however, district's AB 178 reporting highlight challenges in identifying and procuring local risk management services.

This memo provides a response to district requests for assistance with technology-related procurement and inform leaders about relevant system-supported resources via the CollegeBuys Program in three priority areas focal to the recent memo, *FY23-24 Allocation of LSTADS One-Time Funds*, DII 24-100-01: penetration testing, immutable cloud backups, and Security Operations Center (SOC) or (SIEM) Services. Work to implement these local activities are anticipated to reduce the number of cybersecurity incidents and impacts in cases where bad actors are successful.

Background

Development of a systemwide security initiative for the CCCs relies on a diverse set of centralized and decentralized subscriptions, licenses, tools, and services. Districts are responsible for local operations management and procurement and have access to various resources like the CCC Technology Center, CCC Tech Connect, as well as the CollegeBuys Program. The latter was established at the Foundation for California Community Colleges to provide support as the systemwide procurement and contracting hub. CollegeBuys leverages the CCCs' economies of scale to develop compliant strategic sourcing agreements that result in cost savings, standardization of terms, risk mitigation, and source optimization for various commodities and services including, but not limited to software and technology products. Additionally,

A11Y 5/6/24

CollegeBuys agreements eliminate the need for districts to bid a project that is over the bid limit (see California Public Contract Code 20661).

The sections below briefly describe each of the three priority areas for systemwide security, and then provides a list of vendors with CollegeBuys contracts, or available through CollegeBuys' technology reseller agreements with CDW and/or SHI, that districts may want to use. **It is important to note that the vendor options are highlighted *only* as service providers with existing CollegeBuys contracts—they have not been independently evaluated by the Chancellor's Office**. A vendor's inclusion in this memo or CollegeBuys is not an endorsement from the Chancellor's Office. Districts are encouraged to make local assessments of which vendors will best integrate with their systems and meet their needs. Please consult with your local Chief Information Systems Officer or other relevant IT leadership and staff to optimize comprehension of subsequent information.

Penetration Testing

All organizations should undergo penetration testing (pentesting) between one and four times a year, if not more frequently. Historically, the Chancellor's Office has made free pentesting available to districts through the CCC Technology Center and in more recent years through the Technical Assistance Provider (TAP) team. Since 2022, the Chancellor's Office has provided one pentest and triennial review to districts at no cost every other year, with fewer than 5 spots open through December 2024. (For more information about pentesting, please contact Gary Bird, gbird@cccco.edu.)

Best practice for penetration testing is to diversify vendors in order to maximize insights. The following vendors currently provide pentesting services through CollegeBuys contracts:

Pentest Provider	CollegeBuys Contract Options
Black Hills	SHI
CDW	CDW
CrowdStrike	SHI
Ferrilli	Ferrilli
Guidepoint	SHI
Kroll	SHI
PaloAlto	SHI
Redlegg	SHI
SecureWorks	SHI

Strata Information Group (SIG)	SIG
ThreatHunter.ai	SHI

Information about system support for pentesting in calendar year 2025 and beyod will be shared in a forthcoming memo in FY24-25.

Security Operation Center (SOC) Services

The Chancellor's Office explored the value of a single, systemwide SOC service provider; however, that approach is not currently feasible. Many districts have requested help with identifying quality vendors and contracts to implement SOC services locally. The table below includes information on vendors available through CollegeBuys that provide 24x7x365 managed detection and response (MDR), Security Orchestration and Automation Response (SOAR) capabilities and if integration is required with additional security information and event management (SIEM) services. **Information included in the table has been reported by the relevant contract partner (in the far-right column) and has not been independently verfied.**

SOC Vendor	Security Orchestration and Automation Response Capability	SIEM Integration Requirements	CollegeBuys Contract Options
Arctic Wolf	Some	Standalone SIEM solution	CDW, SHI
Bitdefender	No	Standalone SIEM solution	CDW
Bluevoyant	No	MS, Splunk, and/or Cribl	CDW, SHI
CDW	No	PAN Cortex EDR	CDW
Cisco	No	Standalone SIEM solution	CDW
Critical Start	Some	Standalone SIEM solution	SHI
CrowdStrike	Some	Standalone SIEM solution	CDW, SHI
Fortinet	No	Standalone SIEM solution	CDW
Guardian 365	Some	MS 365 Security	Forsyte
Oxford	Some	Azure Lighthouse & Sentinel	Oxford
Palo Alto	No	Standalone SIEM solution	CDW

Quadrant Info Security	No	Standalone SIEM solution	NetXperts
Rapid7	Some	Standalone SIEM solution	SHI
Red Canary	Some	Standalone SIEM solution	CDW, SHI
Redlegg	Some	MS, Splunk, Qradar, LogRhythm and/or others	CDW
SecureWorks	No	Standalone SIEM solution	CDW, SHI
Sentinel One	No	Standalone SIEM solution	CDW
Sophos	Some	Standalone SIEM solution	CDW, SHI
ThreatHunter.ai	Some	Standalone SIEM solution	SHI
TrendMicro	No	Standalone SIEM solution	CDW

Immutable Cloud Backups

In addition to SOC services, colleges are encouraged to implement immutable cloud backups to limit and prevent irretrievable loss of data in a cybersecurity event. Like the above, a range of options are readily available through existing CollegeBuys contracts. These options include:

Cloud Backup Provider	CollegeBuys Contract Options
Amazon Web Services	Amazon Web Services
Cohesity	CDW, SHI
Commvault	CDW, SHI
Dell Technologies	CDW
Druva	CDW, SHI
IBM	CDW
Metallic	CDW
Rubrik	CDW, SHI
Unicon	Unicon
Unitrends	SHI
Veeam	CDW, SHI

Veritas	CDW, SHI
Zerto	CDW

System Discussion

In response to district feedback, the Chancellor’s Office is partnering with the Chief Information Systems Officer Association and CollegeBuys to organize virtual meetings in which district and college personnel will have the opportunity to discuss their experiences with various vendors for these services. These meetings will focus on which vendors are being utilized across the system, how they were selected, and what successes and challenges occurred with the contracting and/or services provided. These meetings are scheduled as follows:

- May 15th, 2pm: Backups and Recovery (RSVP link)
    - Ensuring data integrity and availability through robust backup strategies.
- May 17th, 11am: Vulnerability Assessments vs. Penetration Tests (RSVP link)
    - Unpacking the differences between vulnerability assessments and penetration tests, both crucial for identifying and addressing security weaknesses.

As noted above, districts are encouraged to engage in focused conversations with prospective vendors about their local needs to understand how the vendor’s solution(s) can be best integrated into existing technology infrastructure and plans.

For more information and support in conducting a local assessment, please contact your representative with the relevant contracted partner(s). Contact information and relevant contracts can be found at purchasing.collegebuys.org. For additional information about CollegeBuys and how it can help streamline the procurement, please reach out to cbcontracts@foundationccc.org.

cc: Sonya Christian, Chancellor
Daisy Gonzales, Deputy Chancellor
John Hetts, Executive Vice Chancellor
Wrenna Finche, Vice Chancellor
David O’Brien, Vice Chancellor
Rebecca Ruan-O'Shaughnessy, Vice Chancellor
John Stanskas, Vice Chancellor
CollegeBuys Team