CALSTRS

Board Governance Committee

Item Number 2 – Open Session

Subject: Policy Revisions and/or Creation – Information Security Incident Delegation Procedures and Authority in Existing Agreements, Exemptions, Current Policies and Practices (Appendix III)

Presenter(s): Brian J. Bartow

Item Type: Action

Date & Time: March 7, 2024 – 10 minutes

Attachment(s): Attachment 1 – Appendix III BGM Proposed - Redline Version

Attachment 2 – Appendix III BGM Proposed - Clean Version

PowerPoint(s): None

PURPOSE

The purpose of this item is to propose and recommend a revision to the Board Governance Manual in the instance of an Information Security Incident. The change would give authority to the Chief Executive Officer (CEO) or Chief Operating Officer (COO) to quickly respond to such an incident. With the recommendation of the General Counsel and with the approval of either the chair or vice chair, the CEO or COO would have authority to approve on behalf of the board non-investments contracts exceeding $1,000,000 and up to $5,000,000, and sole source contracts exceeding $100,000 and up to $5,000,000, when it is not practicable to timely secure full board approval, to address such an information security incident.

DISCUSSION/SUMMARY

California Education Code section 22208 allows for the board to delegate its authority to perform any act to the CEO or to two members (or more) of the board.

Consistent with Ed. Code section 22208, the board has delegated certain authority to the CEO for approval of non-investment contracts under "Authorities and Duties" paragraph (b) for contracts that do not exceed $1,000,000 in cumulative value and sole source contracts that do not exceed $100,000 in cumulative value. Current policy language mirrors these limitations with the exception of additional authority limits for contracts in the event of a declared state of emergency. These additional emergency limits were added during the early stages of the COVID-19 Pandemic to allow staff to react and act quickly to secure necessary resources and services.

Consistent with Ed. Code section 22301, the CEO has sub-delegated to the COO the full and continuous use of the CEO's powers and the ability to act in the CEO's stead at all times.

Section 2(a) of Appendix III of the Board Governance Manual currently specifies the following delegated authority:

> **Delegation of Authority**: Any contract or purchase which exceeds $1,000,000 in cumulative value must be approved by the board itself. For goods and/or services obtained with a vendor through CMAS, approval by the board itself is required when cumulative purchase orders for a fiscal year with that vendor exceed $1,000,000. When requesting board approval for CMAS purchase orders exceeding $1,000,000 with a vendor, staff shall provide the board with a breakdown of the total amount for the vendor by project and/or program name. Approval authority for contracts and purchases below $1,000,000 is delegated to the Chief Executive Officer or his/her designee. Additionally, any sole source contract exceeding $100,000 will require advance approval by the board itself.
>
> In the event of an officially declared state of emergency applicable to CalSTRS, the board chair and vice chair, on the recommendation of the Chief Executive Officer, have the authority to approve on behalf of the board, non-investment contracts exceeding $1,000,000 and up to $10,000,000 and sole source contracts exceeding $100,000 and up to $1,000,000, when it is not practicable in light of the emergency to timely secure full board approval. Any contract approved under this emergency exception will adhere to CalSTRS normal procurement process, including fiscal and legal review, and will be compliant with state contracting laws. The full board will be immediately notified if any contract is approved under this emergency exception and a complete report will be provided at the next publicly noticed board meeting.

All organizations continually and increasingly face a high level of risk from information security. Cybersecurity presents ever-growing and ever-changing threats to the data contained within the CalSTRS systems, as well as with our third-party vendors and business partners. CalSTRS remains diligent in its efforts to assess and protect the organization and our members' data. However, the rapid increase in both the number and frequency of reported breaches worldwide continues to be one of the biggest risks our organization faces.

In the event of an information security incident, the organization must respond quickly and effectively to minimize the impact and prevent reoccurrence. There may be significant costs associated with responding. These costs may include engaging certain vendors, in coordination with our Cyber insurer. Vendors may include, but are not limited to, a breach coach, outside counsel, digital forensic services, incident notification services, and an incident call center.

In such instances, having in place a more rapid approval process will allow CalSTRS to respond to the information security incident quickly and appropriately. As a control and in support of transparency, contracts approved under this limited exception will be reported to the full board as soon as possible.

RECOMMENDATION

Staff recommends amending the policy to specify that in the case of an information security incident, on the recommendation of the General Counsel and with approval by either the board chair or vice chair, the CEO or COO may approve contracts in excess of $1,000,000 up to

$5,000,000, and sole source contracts in excess of $100,000 up to $5,000,000, when they have determined that there is insufficient time for the board to consider the matter in a noticed meeting. Information regarding the contract and approval will be presented at the next noticed board meeting.

This would not change the existing delegated authority to the CEO for approval of non-investment or investment contracts.

Staff recommends adding to Section 2(a) of Appendix III of the Board Governance Manual and approving the proposed Policy as presented.