STAFF REPORT

DATE: November 13, 2023

TO: Sacramento Regional Transit Board of Directors

FROM: Shelly Valenton, Deputy General Manager/CEO

SUBJ: DELEGATING AUTHORITY TO THE GENERAL MANAGER/CEO TO AMEND OR APPROVE AND EXECUTE PROCUREMENT CONTRACTS FOR CYBERSECURITY INCIDENT RESPONSE

RECOMMENDATION

Adopt the Attached Resolution.

RESULT OF RECOMMENDED ACTION

The proposed Resolution will allow the General Manager/CEO to enter into or amend existing procurement contracts over $150,000, with one or more vendors, to purchase Information Technology (IT) equipment and professional services as needed to respond to a potential or realized cybersecurity incident and to protect SacRT assets.

FISCAL IMPACT

There is no fiscal impact due to the approval of this Resolution. Fiscal impact will only be incurred in response to a potential or actual incident that would jeopardize the confidentiality, integrity, or availability of SacRT's digital information or information systems.

Any expenditure for cybersecurity incidents will be covered by the approved Information Technology Operating Budget. If the amount exceeds the approved budget, a budget amendment will be brought to the Board of Directors to the extent required by Title VI of the Administrative Code.

DISCUSSION

A cybersecurity incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems.

- **Confidentiality** protects sensitive information from unauthorized access, allowing only authorized individuals to utilize it.
- **Integrity** ensures the data remains accurate, complete, and unaltered throughout its entire lifecycle, defending against unauthorized modifications.
- **Availability** ensures that authorized users can access information and systems without interruption, minimizing potential disruptions.

Cyber-attacks can come in many forms – from ransomware targeting critical infrastructure to data breaches jeopardizing sensitive personal and business information. Each year the cybersecurity challenges facing SacRT increase due to the increasing sophistication of attacks employed by threat actors, and the ever-changing design of IT infrastructure (i.e., cloud migration).

Cybersecurity risks are becoming more systemic and more severe. Although the short-term impacts of a cyberattack on an agency are quite severe, the long-term consequences can be devastating, for example: damage to reputation, reduction in credit rating, increase in cyber insurance premiums, operational disruptions, and legal ramifications.

Cybersecurity threats include, but are not limited to: phishing, where attackers trick users into revealing sensitive information; malware, which is harmful software that can damage or infiltrate systems; cloud vulnerabilities, which expose data stored or processed in cloud services; and ransomware, which encrypts data until a ransom is paid.

In 2017, SacRT was the victim of a cyberattack when the SacRT systems were breached using ransomware. This breach impacted all systems and 90% of the SacRT virtual machine infrastructure was deleted. SacRT did not pay the ransom, and over the course of four days, the IT Department had to work quickly around the clock, in coordination with third-party vendors, to restore all major systems. It took several weeks to fully restore the environment; in addition to damaging critical technology infrastructure, the incident created major impacts to the delivery of transit services.

SacRT is committed to protecting the Confidentiality, Integrity, and Availability of digital information and information systems from cybersecurity attacks.

The long-term vision is to continuously improve SacRT's cybersecurity posture. This requires SacRT to be able to identify and respond to the latest threats while simultaneously building defenses against the existing threats. Because of the sophistication and breadth of cybersecurity attacks, SacRT's internal resources are often insufficient to fully respond. This often can only be accomplished in concert with SacRT's Information Technology services providers and subject matter experts.

The evolving threat landscape makes it challenging to defend against future attacks. If an incident is suspected, this delegation will allow the General Manager/CEO to:

- Confirm an incident or intrusion has occurred
- Identify and prioritize vulnerabilities
- Recover the environment
- Expel the bad actor
- Implement controls to prevent further intrusions

Currently, the General Manager/CEO's procurement contract authority is as follows:

(1) New contracts up to $150,000;
(2) Amendments of up to $150,000 to Board-approved contracts;
(3) Amendments to General Manager-approved contracts up to an aggregate total (between the initial contract and amendments) of $150,000.

(4) Contract Change Orders for public works – authority varies based on the original value of the Contract, but the aggregate limit for smaller public works projects is generally 10% of the original contract price and the individual limit is $150,000 for a single Contract Change Order regardless of the original contract value.

When these limits are exceeded, the Board must approve the contract before it can be executed and the Board may, in addition, be required to make findings related to non-competitive procurements or a decision to amend a contract above the informal solicitation threshold.

To allow the agency to nimbly respond to cybersecurity threats and protect SacRT's systems, assets, and ongoing provision of transit service, this delegation will, in the event of a cybersecurity incident, delegate authority to the General Manager/CEO to enter into or amend existing contracts over $150,000, and up to an aggregate of $1,000,000 per incident, for IT equipment and professional services with one or more vendors, to purchase equipment and services to the extent necessary and as needed to respond to a cybersecurity incident to protect SacRT assets prior to the next regularly-scheduled Board meeting.

The Procurement and Legal Departments will ensure that all purchasing is compliant with the Board-approved Procurement Ordinance. Procurement will identify the most-efficient path forward while ensuring that competitive pricing is obtained.

As these threats are ever evolving, it is impossible to predict what equipment or services will be needed to respond to a cybersecurity incident until that incident presents itself.

Any contract entered into under this delegation will be limited to those actions that are deemed reasonably necessarily to be taken prior to the next-scheduled Board meeting. The General Manager must report any action under this delegation as soon as reasonably possible but in no event more than 45 days after the action is taken. If further contracts or amendments are needed to provide supplies or services to respond to the cybersecurity incident after the next regularly-scheduled Board meeting, those contracts and amendments must be approved by the Board.

RESOLUTION NO. 2023-11-108

Adopted by the Board of Directors of the Sacramento Regional Transit District on this date:

November 13, 2023

DELEGATING AUTHORITY TO THE GENERAL MANAGER/CEO TO AMEND OR APPROVE AND EXECUTE PROCUREMENT CONTRACTS FOR CYBERSECURITY INCIDENT RESPONSE

NOW, THEREFORE, BE IT HEREBY RESOLVED BY THE BOARD OF DIRECTORS OF THE SACRAMENTO REGIONAL TRANSIT DISTRICT AS FOLLOWS:

THAT, authority is hereby delegated to the General Manager/CEO to approve Procurement contracts and amendments, to one or more vendors, that would otherwise be in excess of their authority, as set forth in the Procurement Ordinance (2022-12-001, as it may be amended), up to a maximum aggregate amount of $1,000,000 per incident, for IT equipment and professional services deemed reasonable and necessary to respond to cybersecurity emergencies to protect SacRT's systems, information, assets, and the provision of transit services prior to the next regularly-scheduled Board meeting.

THAT, any Procurement undertaken pursuant to this delegation of authority must be undertaken in compliance with the otherwise-applicable provisions of the Procurement Ordinance.

THAT, any contract or amendment entered into under this delegation will be limited to those actions deemed reasonably necessarily to be taken prior to the next-scheduled Board meeting. The General Manager/CEO must report any action under this delegation to the Board as soon as reasonably possible but in no event more than 45 days after the action is taken. If further contracts or amendments are needed to provide supplies or services to respond to the cybersecurity incident after the next regularly scheduled Board meeting, those contracts and amendments must be approved by the Board.

THAT, this delegation of authority will expire, without further action of the Board, on December 31, 2028.

_____
PATRICK KENNEDY, Chair

A T T E S T:

HENRY LI, Secretary

By:_____
Tabetha Smith, Assistant Secretary