THE PORT
OF LOS ANGELES
Executive Director's
Report to the
Board of Harbor Commissioners

DATE: AUGUST 23, 2023

FROM: INFORMATION TECHNOLOGY

SUBJECT: RESOLUTION NO. _____ - FIRST AMENDMENT TO AGREEMENT 20-3776 BETWEEN THE CITY OF LOS ANGELES HARBOR DEPARTMENT AND INTERNATIONAL BUSINESS MACHINES CORPORATION FOR THE CYBER RESILIENCE CENTER PROJECT

SUMMARY:

Staff requests approval of the First Amendment to Agreement No. 20-3776 with International Business Machines Corporation (IBM) for the Cyber Resilience Center (CRC) project.

The proposed First Amendment is to continue enhancements and operation of the CRC, a first-of-its-kind solution that reduces the risk of a port-wide cyber incident that could disrupt the flow of cargo at the Port of Los Angeles by serving as an early warning system for its ecosystem with improved quality, quantity, and speed of cyber information sharing. The Port of Los Angeles ecosystem are stakeholders that consist of terminal operators, shipping lines, railroad companies, trucking companies, chassis providers, cross-sector companies (e.g. – utilities), marine exchange, the Port's Cyber Security Operations Center (CSOC), and relevant cyber-physical intelligence sources. By sharing relevant Port of Los Angeles cyber information across the ecosystem, the CRC results in greater collective knowledge and stronger Port community cyber resiliency.

The proposed First Amendment will extend the term of Agreement No. 20-3776 by two additional years, for a total of five years, and increase the not-to-exceed compensation by an additional $5,000,000, for a total not-to-exceed compensation amount of $11,800,000. The proposed First Amendment is for hardware, software and services required to continue to enhance, operate, maintain, and support the turn-key CRC solution.

The recommendation to select IBM for Agreement No. 20-3776 was based on the competitive Request for Proposals (RFP) process performed by the City of Los Angeles Harbor Department (Harbor Department). IBM is headquartered in New York, with offices throughout Southern California.

The Harbor Department will continue to be financially responsible for the payment of expenditures incurred under the Agreement.

SUBJECT: AGREEMENT WITH IBM FOR THE CYBER RESILIENCE CENTER

RECOMMENDATION:

It is recommended that the Board of Harbor Commissioners (Board):

1. Find that the Director of Environmental Management has determined that the proposed action is administratively exempt from the requirements of the California Environmental Quality Act (CEQA) under Article II Section 2(f) of the Los Angeles City CEQA Guidelines;

2. Find that, in accordance with the Los Angeles City Charter Section 1022, it is more feasible for outside contractors to perform this work than City employees;

3. Approve the First Amendment to Agreement No. 20-3776 with International Business Machines Corporation to extend the term of the existing Agreement to five years and increase the not-to-exceed compensation amount to $11,800,000 in order to continue to enhance, operate, maintain and support the turn-key Cyber Resilience Center solution;

4. Direct the Board Secretary to transmit said Agreement to the Los Angeles City Council for approval pursuant to Section 373 of the Charter of the City of Los Angeles and Section 10.5 of the Los Angeles Administrative Code;

5. Authorize the Executive Director to execute and the Board Secretary to attest the said First Amendment to Agreement No. 20-3776 for and on behalf of the Board; and

6. Adopt Resolution No. _____.

DISCUSSION:

Background and Context – The Cyber Resilience Center (CRC) is the first-of-its-kind solution that reduces the risk of a port-wide cyber incident that could disrupt the flow of cargo at the Port of Los Angeles by serving as an early warning system for its ecosystem with improved quality, quantity, and speed of cyber information sharing. If a cyber-attack hit any of the stakeholders in the port ecosystem, others may be vulnerable as well, and the disruption to the flow of cargo may be at risk. By sharing relevant cyber information across the Port of Los Angeles ecosystem, the CRC results in greater collective knowledge and stronger Port community cyber resiliency. The CRC will also provide a secure, technical foundation upon which other Port of Los Angeles technological innovations can be better protected.

At its meeting on December 3, 2020, the Board approved Agreement No. 20-3776 with IBM for hardware, software, and services to design, install, operate, maintain, and support the CRC project.

On December 16, 2021, the CRC went live, enabling participating stakeholders from the Port of Los Angeles ecosystem to share relevant cyber threat indicators and defensive measures with each other. The CRC provides a means to reduce the impacts of a cyber incident experienced by one of the Port's stakeholders, from disrupting multiple operations within the Port of Los Angeles. In addition to defensive measures, the CRC serves as an information resource that stakeholders may use to help restore operations following an attack. The CRC receives, analyzes, and shares relevant information to and from direct stakeholders (e.g. – cargo handlers and tenants) and cross-sector stakeholders (e.g. – providers of essential services to direct stakeholders) who choose to become members of the CRC.

CRC objectives include the following:

- Provide both automated and manual information sharing among participating stakeholders,
- Improve the quality, quantity, and speed of available analysis of ecosystem cyber risks,
- Create new collaboration with stakeholders to increase cyber resilience, and
- Provide a new source of information to stakeholders that could allow them to improve their cyber security posture.

The CRC is different from the scope and function of the Port's Cyber Security Operations Center (CSOC). The CRC is a "system of systems" that the CSOC and stakeholder cyber security systems connect to, but will not replace them, nor is it intrusive, disruptive, or burdensome to stakeholder systems. Stakeholders have the control to decide if, and how, to use information from the CRC.

Proposed First Amendment – The proposed First Amendment (Transmittal 1) will be required to complete remaining tasks, to complete new tasks, and include all hardware, software, and services required to enhance, operate, maintain, and support the turn-key CRC solution.

The proposed First Amendment will extend the term of Agreement No. 20-3776 by two additional years, for a total of five years, and increase the not-to-exceed compensation by an additional $5,000,000, for a total not-to-exceed compensation amount of $11,800,000. The proposed First Amendment includes the following, which will be conducted in collaboration with ecosystem stakeholders:

Complete remaining tasks:

1. Stakeholder On-Boarding – This includes set-up and training for up to 100 stakeholders. Training will include use of the CRC platform, use of dashboards, use of data and available reports, methods of communication and interactions

between stakeholders and CRC Operations. On-boarding documentation will be updated, which will be detailed and organized such that it can later be used as a stakeholder operations manual.

2. ISO 27001 Certification – ISO 27001 is an international standard used in cyber security operations. The initial certification is estimated to be completed by October 2023, and verifies that the documented policies and procedures conform with the ISO 27001 standard. After the initial certification, annual surveillance audits will be conducted to verify that the CRC's actual operations conform to the ISO 27001 standard. Initial certification and annual surveillance audits are conducted by an independent 3rd party firm.

Complete new tasks:

3. Enhancements – Replace limited and inefficient technologies with a new threat intelligence platform and external threat intelligence sources. Activities include design, development, implementation, integration, documentation, and migration to the enhanced CRC platform used for threat collection, analysis, enrichment, and dissemination of high-fidelity finished threat intel provided to stakeholders. Additional activities include ongoing collaboration with stakeholders to validate requirements to facilitate manual and automated data collection, data analysis, and data distribution.

Continued operations and contingency:

4. Operations and Maintenance – This is for operating the CRC, 24 hours per day, 7 days per week (24x7) with qualified cyber security analysts. This also includes annual CRC refresher training and tabletop exercises for stakeholders that interface with the CRC. The CRC will also provide annual general cyber security awareness training that participating stakeholders may use, as appropriate for their company's cyber program. This also includes maintenance for all items provided under the Agreement, including but not limited to the hardware, software, subscriptions, furniture consoles and equipment.

5. Contingency – This is for new requirements that are beyond the original scope and are required to meet the objectives of the CRC. This amount is approximately 11 percent of the known costs for this first-of-its-kind solution. Contingency funds will be used only if authorized by written directive from the Executive Director.

Selection Process – Agreement No. 20-3776 was awarded to IBM based on a competitive RFP process performed by the Harbor Department. IBM is headquartered in New York, with offices throughout Southern California.

ENVIRONMENTAL ASSESSMENT:

The proposed action is the approval of the First Amendment to Agreement No. 20-3776 with IBM to continue enhancements and operation of the CRC project, which is an administrative activity. Therefore, the Director of Environmental Management has determined that the proposed action is administratively exempt from the requirements of CEQA in accordance with Article II, Section 2(f) of the Los Angeles City CEQA Guidelines.

FINANCIAL IMPACT:

Approval of the proposed First Amendment with IBM will extend the term of Agreement No. 20-3776 by two additional years, for a total of five years, and increase the not-to-exceed compensation amount by an additional $5,000,000, for a total not-to-exceed compensation amount of $11,800,000, in order to enhance, operate, maintain and support the turn-key CRC solution.

Fiscal Year (FY) 2023/24 capital funding in the amount of $1,683,359 is available within Work Order 2555500, Center 1179, Program 640.

FY 2023/24 operating funding in the amount of $1,286,959 is available within Account 54310 (Information Systems Consulting Services), Center 0640, Program 000. Funding for future fiscal years will be requested to be budgeted, upon Board approval each fiscal year, as part of the annual budget adoption process. It is expected that should the Board approve funds for the Agreement in each subsequent future fiscal year, funds will be expended as follows:

Fiscal Year	Original No. 20-3776		Proposed First Amendment		TOTAL
	Capital	Operating	Capital	Operating	
2020/21	$912,941	$0	$0	$0	$912,941
2021/22	$2,385,661	$600,445	$0	$0	$2,986,106
2022/23	$454,735	$1,200,890	$0	$0	$1,655,625
2023/24	$444,735	$800,593	$1,238,624	$486,366	$2,970,318
2024/25	$0	$0	$491,626	$1,882,512	$2,374,138
2025/26	$0	$0	$113,122	$787,750	$900,872
Total Not-To-Exceed	**$4,198,072**	**$2,601,928**	**$1,843,372**	**$3,156,628**	**$11,800,000**

The actual expenditures may differ from the estimated amounts in the accounts and in any given fiscal year presented in the table above. However, the total aggregate amount will not exceed $11,800,000.

SUBJECT: AGREEMENT WITH IBM FOR THE CYBER RESILIENCE CENTER

A Termination for Non-Appropriation of Funds Clause (also known as a Funding Out Clause) is included in the Agreement.

CITY ATTORNEY:

The Office of the City Attorney has prepared and approved the proposed First Amendment as to form and legality.

TRANSMITTALS:

1. First Amendment to Agreement No. 20-3776
2. Agreement No. 20-3776

FIS Approval: MB
CA Approval: SO

Sheeba Varughese
dc=pola, dc=lahd, ou=HQ, ou=ITD, ou=USERS, ou=EMP, cn=Sheeba Varughese, email=SVarughese@portla.org
2023.08.29 13:11:53 -07'00'

SHEEBA VARUGHESE
Chief Information Officer

Digitally signed by Thomas E. Gazsi
Date: 2023.08.29 13:39:45 -07'00'

THOMAS E. GAZSI
Chief of Public Safety and Emergency Management

APPROVED:

Mark Blevins FOR

EUGENE D. SEROKA
Executive Director

SV:tz:dpy