CITY OF HOUSTON
Houston Information Technology Services

Sylvester Turner
Mayor

Lisa Kent
Chief Information Officer
Houston IT Services Dept.
611 Walker Street
Houston, Texas 77002

T. 832-393-0082
f. 832-393-0075
www.houstontx.gov

March 3, 2023

The Honorable Charles Schwertner
Senate Committee on Business and Commerce
Texas Senate
P.O. Box 12068-Captiol Station
Austin, Texas 78711

Dear Chairman Schwertner and Members of the Committee,

The City of Houston appreciates the opportunity to provide written testimony in opposition to Senate Bill 271 (SB 271) relating to state agency and local government security incident procedures. For the following below reasons, the City of Houston opposes SB 271 as it would require an onerous, challenging, and unworkable process relating to Security Incidents for not only the City of Houston, but also with other entities under SB 271.

SB 271 defines "Security Incident" to mean both the "actual or suspected unauthorized access, disclosure, exposure, modification, or destruction…" and applies that defined term throughout this SB 271. The inclusion of situations where such actions are "suspected" extensively broadens the scope of applicable circumstances under this SB 271's purview, including notification and reporting requirements. Other laws defining "Security Incident", such as under 45 CFR Section 164.304, where the Security Incident is defined as "the attempted or successful unauthorized access…", limits the application to actual attempts or successful actions. This SB 271 broadens the use of "Security Incident" and is one of the fundamental reasons that this SB 271 will be an enormous challenge to entities subject to this statute's requirements.

Not unlike other entities – in both public and private sectors, each day there are thousands of cyber attempts on the City of Houston's environment. And like other entities, the City of Houston, would be hard pressed to determine the intent of the attackers without taking the time to investigate. SB 271 requires that no later than 48 hours after the discovery of a Security Incident notification be made to the Department (including the Chief Information Security Officer, and in cases of election data, the Secretary of State). Therefore, to comply with SB 271, entities like the City of Houston, would be compelled to assume the intent was unauthorized access, disclosure, exposure, modification, or destruction of sensitive personal information, confidential information, or other information the disclosure of which is regulated by law, including breach and suspected breach of system security and introduction to ransomware into a computer, computer network, or computer system. This requirement for the City of Houston to report on all Security Incidents no later than 48 hours after the discovery of a Security Incident (which not only includes actual access, disclosure, exposure, modification, destruction, breach, or ransomware, but also *suspected* cases of such as well) makes compliance with SB 271 realistically impossible and unworkable and is an enormous challenge to other entities as well as the City of Houston.

Furthermore, as with any suspected Security Incident, often the process of investigation may take days, weeks, and months to determine the cause and how the incident transpired. Certainly, it is not the norm for an

investigation to complete within 48 hours. Therefore, if local governments are required to report and notify within a 48-hour deadline, this may result in premature, inaccurate, or even harmful notifications to be made to the Department (and potentially overwhelm the Department with an enormous volume of notifications that the actual true Security Incidents are lost in the flood of notifications it receives, defeating the purpose of such notifications). Premature notifications may also cause harm as it may alert adversaries and foreign governments actors to existing potential vulnerabilities that may not been patched, mitigated, or remedied yet, further putting other entities at harm for the same or similar attacks; or alert adversaries and foreign government actors that they have been detected.

SB 271 requires that local governments to, no later than the 10th business day after the date of eradication, closure, and recovery from a Security Incident, notify the Department of the details of the Security Incident and include an analysis of the cause of the Security Incident. Although a Security Incident may be eradicated from the environment and/or the entity has recovered, often the cause and details of what transpired are still under investigation. Under SB 271, this 10-day requirement may lead to a rushed submission, inaccurate, or missing information in the reports submitted. In addition, if the vulnerability that resulted in the Security Incident remains unpatched or otherwise still incurable, the notification and disclosure of the details of the Security Incident may put other entities in harm's way by describing how other adversaries may also use the same or similar attack method on others. This collection of reporting and analysis will require robust security measures to ensure that such reports and analysis are not disclosed to the public and potentially increase vulnerabilities.

The City of Houston appreciates the importance of cyber security and striving to continue to strengthen governmental security postures. However, for the reasons stated above, the City of Houston opposes SB 271. We hereby submit our written testimony in opposition.

Respectfully submitted,

Lisa Kent

Lisa Kent, CIO
City of Houston
Houston Information Technology Services