Thomas P. DiNapoli
State Comptroller

110 State Street
Albany, New York 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

July 20, 2023

Jackie Bray
Commissioner
Division of Homeland Security and Emergency Services
1220 Washington Avenue
State Office Campus – Building 7A
Albany, NY 12242

Re: Cyber Incident Response Team
Report 2023-F-8

Dear Commissioner Bray:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law, we have followed up on the actions taken by officials of the Division of Homeland Security and Emergency Services (Division) to implement the recommendations contained in our initial audit report, *Cyber Incident Response Team* (Report 2020-S-58).

Background, Scope, and Objective

Cybercrimes continue to rise. According to the Federal Bureau of Investigation (FBI), complaints of phishing and similar cyberattacks often used to deliver ransomware increased by 162%, from 114,702 in 2019 to 300,497 in 2022. These attacks can have a significant impact on the public when they target public authorities and local governments that oversee a variety of services the public depends on, including water systems, utilities, airports, schools, and health care facilities. In 2022, there were 2,385 complaints of ransomware according to the FBI's Internet Crime Report.

In 2017, the Cyber Incident Response Team (CIRT) was created to provide cybersecurity support to more than 2,800 non-Executive agencies, local governments, and public authorities in New York. (For the purposes of this report, we consider non-Executive agencies to be those not supported by the Office of Information Technology Services, or ITS.) CIRT is part of the Division's Office of Counter Terrorism and currently has 17 members – 11 Division employees and six members of the National Guard. The Division's mission is to provide leadership, coordination, and support for efforts to prevent, protect against, prepare for, respond to, and recover from terrorism and other man-made and natural disasters, threats, fires, and other emergencies. A stated goal of New York State's Homeland Security Strategy for 2022-2025 is the expansion of CIRT to ensure the State successfully addresses and mitigates cyber threats and provides cybersecurity-related support to local governments, State authorities, non-Executive agencies, and certain critical infrastructure entities.

According to the State Comptroller's "Standards for Internal Control in New York State Government" (Internal Control Standards), a mission is an organization's reason for existing;

it provides a sense of direction and purpose to all members of the organization and serves as a guide for making critical decisions. Objectives detail an organization's areas of focus for accomplishing its mission and meeting its expectations and should be written in specific and measurable terms, clearly defining what is to be achieved, who is to achieve it, how it will be achieved, and the time frames for achievement. Goals are objectives translated into specific, measurable targets. They are quantifiable and provide a means for assessing the accomplishment of objectives. While objectives should be translated into attainable goals, some objectives are not easily adaptable into quantifiable goals. In such instances, management should identify some other appropriate indirect measure. Evaluation is the process that management uses to determine whether an organization has achieved or will achieve its goals and objectives and involves conducting periodic assessments of the organization's performance against established expectations or measurement standards.

The objective of our initial audit, which was issued on November 12, 2021 and covered the period January 1, 2018 to March 26, 2021, was to determine whether CIRT was achieving its mission of providing cybersecurity support to non-Executive agencies, local governments, and public authorities. The audit found that CIRT developed lines of service to guide its work, which includes cyber incident response services, technical cyber services, and information sharing and outreach, but did not establish specific and measurable objectives or quantifiable goals that can be measured to evaluate its accomplishments.

The objective of our follow-up was to assess the extent of implementation, as of April 14, 2023, of the two recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

Division officials made progress in addressing the issues we identified in the initial audit report; however, additional actions are needed. Of the initial report's two audit recommendations, one was implemented, and one was partially implemented.

Follow-Up Observations

Recommendation 1

Develop specific, measurable objectives and quantifiable, attainable goals, along with associated reporting mechanisms, to allow CIRT to evaluate if it is achieving its mission.

Status – Partially Implemented

Agency Action – CIRT has developed reporting mechanisms to capture several key metrics, including the number of incidents, type of incidents, time spent resolving incidents, and types of forensics performed, among others. CIRT has developed reporting mechanisms to track incident responses and has also begun to gather data to guide its outreach, which can further its development of measurable objectives and quantifiable goals. However, it has not yet established goals for its lines of service, including for incidents, phishing, tabletop exercises, and risk assessments. Officials stated that prior attempts to set specific goals for their lines of services were limited by customer response. Without specific, measurable objectives as well as quantifiable, attainable goals, CIRT officials cannot evaluate their performance and, consequently, their progress toward achieving their mission. Furthermore, CIRT cannot ensure that its limited resources are being maximized to provide the greatest benefit to the entities it was created to support.

Recommendation 2

Take steps to determine the cybersecurity needs of the non-Executive agencies, local governments, and public authorities CIRT is charged with supporting.

Status – Implemented

Agency Action – CIRT continues to attend conferences and events to obtain a broad idea of the needs of the entities it serves. Additionally, since our original audit, CIRT has begun to take targeted approaches in its outreach to offer services. CIRT receives an annual threat assessment report to determine the sectors that are at an increased cybersecurity risk and provide a more targeted outreach to promote its services. In addition, CIRT uses other factors – including history of past incidents, the population an entity serves, sensitivity of data assets, and the critical nature of the services an entity provides – to guide its outreach. CIRT tracks all the individualized outreach to entities based upon the service it is promoting.

Major contributors to this report were Daniel Raczynski, Christopher Bott, and Jonathan Julca.

We would appreciate your response to this report within 30 days, indicating any actions planned to address the unresolved issues discussed in this report. We thank the management and staff of the Division of Homeland Security and Emergency Services for the courtesies and cooperation extended to our auditors during this follow-up.

Very truly yours,

Amanda Eveleth, CFE
Audit Manager

cc: Brian Jackson, Internal Audit