Thomas P. DiNapoli
State Comptroller

110 State Street
Albany, New York 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

November 12, 2021

Terence O'Leary
Executive Deputy 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 2020-S-58

Dear Executive Deputy Commissioner O'Leary:

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 conducted an audit of the Cyber Incident Response Team (CIRT) at the Division of Homeland Security and Emergency Services (Division) to determine whether CIRT is achieving its mission of providing cybersecurity support to non-Executive agencies, local governments, and public authorities. The audit covered the period from January 1, 2018 to March 26, 2021.

Background

Cybercrimes, such as those involving phishing and ransomware, are on the rise. Phishing is a type of online scam where criminals impersonate legitimate organizations, often via email or text message, in order to access and steal sensitive information. Ransomware is malicious software that is often deployed via phishing emails and is designed to trick users into clicking on malicious links. Once clicked, the users' files are encrypted and inaccessible until a ransom is paid. According to the Federal Bureau of Investigation (FBI), complaints of phishing and similar cyberattacks often used to deliver ransomware increased by 110%, from 114,702 in 2019 to 241,342 in 2020. 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 2020, U.S.-based governments, health care facilities, and schools were victims of 2,400 ransomware incidents, according to the FBI's Internet Crime Report.

In 2017, 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 nine members – seven Division employees and two 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.

To carry out its mission, the Division developed the 2017-2020 New York State Homeland Security Strategy (Security Strategy) to establish goals and provide guidance for the implementation of homeland security-related policies, priorities, and programs throughout the State. One of the Security Strategy's goals is to "Enhance Cyber Security Capabilities," which has defined objectives, targets, and metrics in order to measure its progress. While the cyber-related section of the Security Strategy was designed prior to the creation of CIRT, many of the objectives align with activities CIRT performs. For example, one objective was to improve technical capabilities, and the Division's related efforts, through a two-pronged strategy: (1) conducting and supporting at least one major cyber training attended by relevant personnel at the State level and (2) making cybersecurity training available for local (e.g., county) stakeholders and the public. Another objective was to incorporate cybersecurity into exercises to build and test capabilities, and the Division's related efforts, by holding at least eight tabletop exercises per year and participate in other relevant cybersecurity exercises.

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.

Results of Audit

CIRT's mission is broadly defined to provide cybersecurity support to non-Executive agencies, local governments, and public authorities. However, CIRT has not developed specific, measurable objectives or quantifiable, attainable goals to allow Division management to evaluate whether it is achieving its mission.

CIRT officials developed three areas of focus, referred to as lines of service, to guide its work: Cyber Incident Response Services, Technical Cyber Services, and Information Sharing and Outreach. Each line of service has two or three examples of services to be provided by CIRT:

- Cyber Incident Response Services – incident response and digital forensics; vulnerability scanning and penetration testing; and remediation assistance
- Technical Cyber Services – cyber risk assessments; cybersecurity tool kits; and training exercises
- Information Sharing and Outreach – outreach to customer base and community of practice forums

While CIRT has developed lines of service to guide its work, it has not established specific and measurable objectives that clearly define what is to be achieved, who is to achieve it, how it will be achieved, or the time frames for achieving it. Further, it has not established quantifiable goals that can be measured to evaluate its accomplishments.

CIRT has performed a variety of activities related to the lines of service it has established. Between May 2018 and December 2020, it responded to 122 cyber incidents, including phishing, ransomware, malware, and compromised accounts. In addition, CIRT provided technical cyber services and information sharing and outreach. Between August 2019 and December 2020, CIRT conducted 11 risk assessments at counties, local government entities, and one non-Executive agency at the request of these entities—a small fraction of the 2,800 entities under its purview. Based on these requests, as well as identified areas of need, CIRT conducted five phishing campaigns and held or participated in 32 training sessions. CIRT also held or participated in 13 tabletop exercises for county Boards of Elections, critical infrastructure, and transportation authorities to test emergency response preparedness. Additionally, CIRT has participated in eight outreach events to promote the availability of cyber resources. Further, CIRT contributed information to the New York State Intelligence Center (NYSIC) to be used in issuing statewide alerts related to cyber incidents. However, without specific, measurable objectives and quantifiable, attainable goals, Division management is unable to evaluate the extent to which these services are achieving CIRT's mission.

As described previously, CIRT's activities overlap with certain objectives related to the cybersecurity goal in the Security Strategy and, therefore, CIRT played a role in implementing or partially implementing each of the 10 objectives in the Security Strategy. However, CIRT officials stated the Security Strategy is a statewide plan and they are not solely responsible for the cyber-related objectives. They further stated that a full evaluation of the Security Strategy was not scheduled until the 4-year period defined in the strategy was completed in 2020 and would involve meeting with other agencies, including ITS and NYSIC, to determine the status of its implementation. As of June 2021, the implementation of the Security Strategy, including CIRT's role, had not been fully evaluated.

Generally, CIRT provided technical cyber services at the request of the entities that it supports; however, it has not sought to proactively obtain information from these entities to evaluate their needs on a broad basis. For example, ransomware, which is often deployed via phishing emails designed to trick users into clicking on malicious links, is a significant threat to these entities. Of the 122 cyber incidents CIRT responded to between May 2018 and December 2020, 39 were for phishing and 23 were for ransomware attacks. CIRT officials acknowledged that, based on anecdotal conversations with participants at their trainings and outreach sessions, there is a need for training specific to detecting phishing attempts and preventing ransomware attacks. Despite this, CIRT provided only five phishing email trainings between July 2020 and March 2021. Moreover, CIRT officials acknowledged that they did not perform any surveys or collect data to determine how many or which of the entities they are responsible for have conducted or procured their own training on phishing emails, but that it is likely at least some have done so. Such information would allow CIRT officials to better understand and plan for entities that may benefit from their services in a more targeted manner.

CIRT has only identified areas of focus based on the services they currently provide, rather than establishing formal objectives and goals based on a mission statement and then working to provide services that meet those goals and objectives. CIRT officials cited the newness of the team and lack of historical information to be used for planning purposes as factors contributing to the lack of formal objectives and goals. They stated that CIRT has only been in existence since 2018, and the onset of the COVID-19 pandemic in 2020 limited their activities. They also cited difficulty in setting targets, or goals, for certain activities like response and recovery, which they noted are unpredictable. However, assessing gaps and risks is useful and achievable but cannot be done without a framework. Further, as noted in the Internal Control Standards, when it is difficult to translate an objective into a quantifiable goal, management should identify some other appropriate indirect measures.

Without specific, measurable objectives and quantifiable, attainable goals, CIRT officials cannot evaluate their performance and, consequently, their progress toward accomplishing their mission. While CIRT has undertaken a variety of activities, it has done so without clear objectives, goals, or a mechanism for reporting on and evaluating its performance. CIRT officials cannot be assured the work they are performing is having the desired outcomes and is targeted appropriately for their customers. Consequently, CIRT cannot ensure that its limited resources are being maximized to provide the greatest benefit to the entities it was created to support.

In response to our preliminary audit findings, CIRT officials indicated they have developed a sound, effective cybersecurity program that delivers valuable services to the entities they support.

Recommendations

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.

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

Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether the Division's CIRT is achieving its mission of providing cybersecurity support to non-Executive agencies, local governments, and public authorities. The audit covered the period from January 1, 2018 to March 26, 2021.

To accomplish our audit objective and assess internal controls related to our objective, we interviewed Division officials and CIRT staff, and reviewed relevant laws and regulations as well as Division policies and procedures. We reviewed the Security Strategy and documentation of cyber services provided by CIRT to the entities it supports.

Statutory Requirements

Authority

This audit was performed 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 conducted our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State.

These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. These duties could be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our professional judgment, these duties do not affect our ability to conduct this independent performance audit of the Division of Homeland Security and Emergency Service's Cyber Incident Response Team.

Reporting Requirements

We provided a draft copy of this report to Division officials for their review and comments. Rather than consider the recommendations as an opportunity to improve its oversight of the CIRT, Division officials expressed disagreement with our audit conclusions and recommendations. We also note that the Division's response includes multiple misleading and/or inaccurate statements. Our responses to those comments are included as State Comptroller's Comments, which are embedded in the Division's response at the end of this report.

Within 180 days of the final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the Division of Homeland Security and Emergency Services shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

Major contributors to this report include Cynthia Herubin, Brian Krawiecki, Christopher Bott, Nicole Cappiello, Ryan Chauvin, W. Sage Hopmeier, and Amy Tedesco.

We wish to thank the Division's management and staff for the courtesies and cooperation extended to our examiners during this audit.

Very truly yours,

Nadine Morrell, CISM, CIA
Audit Director

cc: Brian Jackson, Internal Audit

Agency Comments and State Comptroller's Comments

NEW YORK STATE | Homeland Security and Emergency Services

KATHY HOCHUL
Governor

PATRICK A. MURPHY
Commissioner

September 27, 2021

Ms. Nadine Morrell
Office of the State Comptroller
110 State Street – 11th Floor
Albany, New York 12236

Dear Ms. Morrell:

The New York State Division of Homeland Security and Emergency Services (DHSES) has reviewed the Office of the State Comptroller's (OSC) draft audit report 2020-S-58 titled, Cyber Incident Response Team Report (DAR).

The stated purpose of this audit was to determine whether DHSES/CIRT is achieving its mission of providing cyber security support to non-Executive agencies, local governments and public authorities. The two recommendations contained in the DAR are not directed at the CIRT's productivity and appear to be based on a misunderstanding of how the CIRT operates. Notwithstanding, OSC expressed no concerns with the services CIRT is providing to its customers or its general operations. Indeed, OSC's observations about current threat trends[1] align with CIRT's mission and highlights the importance of providing such cyber security support services to these supported entities.

State Comptroller's Comment – There is no misunderstanding. It is because OSC fully comprehends the current threat trends and the importance of providing proactive support services to non-Executive agencies, local governments, and public authorities that we make our recommendations. In such an environment, clear goals are critical to maximizing limited resources to better mitigate risk in order to meet CIRT's mission. The Internal Control Standards, which help enable organizations to accomplish their missions, require organizations establish goals that are specific and measurable, with quantifiable targets, to provide a means to assess the accomplishment of objectives. However, we found that CIRT had not established specific goals or measurable targets against which to assess its performance.

Since its inception, the CIRT has responded every time assistance was requested by a supported entity. The CIRT does this through a partnership with the New York State Police and the New

[1] The DAR notes that cybercrimes such as phishing and ransomware are on the rise and pose a significant risk to the CIRT's customer base. (See, DAR, pgs. 1.) Accordingly, on top of incident response services, the CIRT provides in-depth, state-of-the-art Cybersecurity Risk Assessments that help customers harden their IT infrastructure, directs its members throughout the state to provide training on these hazards, and recently operationalized a phishing training program for the benefit of its customers.

York State Intelligence Center (NYSIC), the State's all-crimes fusion center, which maintains a 24-hour emergency hotline for receiving reports of cyber incidents and relaying them to DHSES. When a report is received, the CIRT – through a highly qualified team of cybersecurity practitioners who hold the required professional credentials and advanced certifications – works with the reporting entity to help them understand and resolve the cybersecurity issues affecting them. As such, the CIRT currently maintains "objective and quantifiable, attainable"[2] metrics for the number of incidents to which it should be responding. Those metrics are the number of requests for help received (164 since inception) as well as the percentage of time help was offered (100%).

State Comptroller's Comment – We disagree with the Division's assertion that it maintains objective, quantifiable, and attainable metrics. Simply tabulating the number of services already provided is not a substitute for establishing goals and measurable targets against which to compare its tally of services provided. Moreover, responding when requested is the definition of reactive.

Rather than creating an arbitrary number of possible incidents the CIRT will respond to, the CIRT remains committed to promoting its capabilities and then providing quality services that are available as necessary. The CIRT has no statutory or regulatory authority to compel customers to take advantage of these services, and therefore they are conducted on a timeline of the customers' choosing. Nonetheless, CIRT members have consistently publicized the CIRT's services to its customers at the dozens of conferences, panels, exercises, and trainings in which it has participated (in support of this outreach, OSC was provided a list of sixty-seven trainings, panels, and exercises in which the CIRT participated).

State Comptroller's Comment – We do not suggest that CIRT should "create an arbitrary number of possible incidents" to respond to, but rather that it should develop other appropriate indirect measures. In response to our preliminary report, Division officials themselves noted, "We recognize the CIRT has not yet developed metrics to identify precisely how many risk assessments, trainings, and phishing exercises it should be conducting annually but that is a byproduct of the CIRT having only been operational since 2018 and having lost a year of consistent data collection to the COVID-19 pandemic." In fact, officials agreed that, although there are limitations to this process, they can better formalize and document its missions, objectives, and goals.

The DAR makes several factually inaccurate statements and insinuations that belie any value one could derive from its recommendations. These are addressed below:

1. The DAR inaccurately states the New York State Homeland Security Strategy was developed by DHSES for the purpose of carrying out the Agency's mission and insinuates this document, which predates the existence of the CIRT, should serve as a measure for CIRT effectiveness.[3] In fact, the Homeland Security Strategy is a federally required document required

[2] See DAR at 2.
[3] DAR at 2.

for New York State to receive federal counter terrorism funds. It is not DHSES specific and is not designed to be a program management tool. It was made clear to OSC over the course of several conversations that it should not be used as a measure of CIRT effectiveness. Yet, inexplicably, OSC recommends the New York State Homeland Security Strategy be used for this very purpose.[4]

State Comptroller's Comment – The Division is misrepresenting the facts of our report. We make no such claim that the Security Strategy should serve as a metric for CIRT effectiveness, nor do either of our recommendations make any reference to using the Security Strategy as a management tool for assessing CIRT performance, as DHSES suggests. As we state in our report, the Security Strategy was designed prior to the creation of CIRT and is a statewide plan for which CIRT is not solely responsible. Furthermore, in response to our preliminary findings, Division officials acknowledged that CIRT does contribute to meeting the goals in the Security Strategy. As CIRT is well aware, federal Homeland Security dollars help fund State and local cybersecurity efforts. As stated by the federal Secretary of Homeland Security, "As we have seen in recent events, attacks on our cyber networks can have devastating effects. …With this funding, state and local grant recipients can conduct cybersecurity risk assessments, strengthen their 'dot gov' internet domains, improve the cybersecurity of their critical infrastructure, and conduct additional cybersecurity training and planning" (Department of Homeland Security, Preparedness Grants press release, February 2021).

2. The DAR erroneously opines the CIRT "has not established specific and measurable objectives that clearly define what is to be achieved, who is to achieve it, how it will be achieved, or the time frame for achieving it." Yet, as the DAR itself notes on page 2, the CIRT *has* established several lines of service that promote better cybersecurity among the organizations it services – *i.e., what is to be achieved.* The CIRT provided OSC with the policy documents and contracts used to perform these services to assist OSC in understanding how the work will be achieved and who will perform it. Further, as noted above, the CIRT has offered assistance every time a cyber incident was reported to it, thereby achieving the most important metric to measure mission accomplishment. Regarding the timeframe, there is considerable background and follow-up work that goes into all CIRT engagements. Accordingly, the timeframe of an engagement is determined by the complexity of a customer's network and the issues that require attention.

State Comptroller's Comment – Offering several lines of service is a first step. CIRT should then assess what are the entities' needs and develop a work plan with its goals. Our report acknowledges that CIRT had developed three lines of service. However, simply listing services to be provided does not serve as a measurement standard for the purposes of the Internal Control Standards. In the Division's response to our preliminary findings, officials recognized that CIRT had not yet developed metrics to identify precisely how many risk assessments, trainings, and phishing exercises it should be conducting annually.

3. The DAR also inaccurately states "Division management is unable to evaluate the extent to which [CIRT] services are achieving the CIRT's mission." The DHSES Commissioner is

[4] DAR at 2.

briefed on a weekly basis about CIRT activities and on an ad hoc basis, as necessary. OSC did not speak with the DHSES Commissioner or other senior leadership to determine what Division management can or cannot evaluate concerning the CIRT's effectiveness. Such a sweeping statement should not be included without supporting information. Moreover, this statement fails to appreciate what Division management does and how they evaluate programs. Accordingly, as this assertion is entirely speculative and without any factual support, it should be stricken from any published report.

State Comptroller's Comment – The Division is misrepresenting our report and taking statements out of context. Our report states, "However, without specific, measurable objectives and quantifiable, attainable goals, Division management is unable to evaluate the extent to which these services are achieving CIRT's mission." While it is important that the Commissioner is briefed on CIRT's work, without performance measures, we question on what basis the work is evaluated.

4. The DAR also incorrectly claims the CIRT "has not sought to proactively obtain information from [the entities it supports] to evaluate their needs on a broad basis."[5] As explained to OSC, the CIRT achieved this, and continues to achieve it, through discussions with customer representatives (i.e., New York State Local Government Information Technology Directors' Association (NYSLGITDA), New York State Association of Counties (NYSAC), the Center for Technology in Government, and representatives from public authorities, to name a few) that are well positioned to advise on which services will be most useful to the CIRT's supported entities.[6] Moreover, surveys are sent following every risk assessment engagement. Indeed, the DAR does not suggest that CIRT is not providing the right services, it merely speculates that there may be a better way to compose the list of services.

State Comptroller's Comment – Obtaining information from various associations and groups that represent the entities CIRT is charged with serving is important and can provide CIRT with general insights. However, we disagree with the Division's assertion that our report "merely speculates there may be a better way to compose a list of services." For instance, on page 3 of our report, we highlight a specific example where CIRT has the potential to use its limited resources to target and provide ransomware and phishing trainings to those customers who could most benefit from it. Further, as noted in the report, if CIRT knew which entities have already procured their own phishing email training, it could better target those that have not. In fact, as noted on page 3 in our report, CIRT officials acknowledged that, based on anecdotal conversations with participants at trainings and outreach sessions, there is a need for training

[5] DAR at 3.

[6] OSC instead suggests that surveys would be a good way to identify what services are required by the CIRT customer base. Obviously, CIRT would be interested in any empirical support for that recommendation, as the time and resources required to issue and analyze surveys directed to all the local governments, non-Executive agencies, and state authorities in New York (over 2800 entities) would be substantial. *But this is a particularly questionable suggestion considering OSC has ignored targeted surveys regarding specific threats the CIRT sent out in the past year, thereby highlighting the limited utility of surveys.*

specific to detecting phishing attempts and preventing ransomware attacks; yet they only performed five phishing email trainings.

5. The DAR also inaccurately claims "CIRT has only identified areas of focus based on the services they currently provide rather than establishing objectives and goals based on a mission statement then working to provide services that meet those goals and objectives."[7] The CIRT designed its services based on industry standards and an assessment of current cyber threats provided by the New York State Intelligence Center. The CIRT also relied on experts in the cybersecurity field and extensive discussions with customer representatives to identify and provide services that have the most potential to meaningfully impact its customers' cybersecurity posture. In developing and offering these services, the CIRT provides the "leadership, coordination, and support" to supported entities in need of cybersecurity assistance – *in line with the DHSES' mission statement.*

State Comptroller's Comment – The Division again has misinterpreted the message of the report. We did not question how CIRT established its lines of service, but rather highlighted that CIRT has not established specific goals or measurable targets, which are necessary for evaluating its performance in providing those lines of service. In fact, the remainder of the paragraph from the Division's quote above, which the Division did not also include, presents the list of reasons the Division cited for not having developed specific goals and measurable targets needed to assess performance.

6. The report states "CIRT officials generally agreed with our recommendations." As stated above, the CIRT does not agree with either of the recommendations provided in this report. This was previously communicated to OSC.

State Comptroller's Comment – Since we removed that sentence from the report to address Division officials' concerns after the draft report was issued, we are surprised that they chose to include this comment in their response. In contrast, their response to the preliminary findings stated:

> *"We recognize the CIRT has not yet developed metrics to identify precisely how many risk assessments, trainings, and phishing exercises it should be conducting annually but that is a byproduct of the CIRT having only been operational since 2018 and having lost a year of consistent data collection to the COVID-19 pandemic. … Although, DHSES/CIRT agrees it can better formalize and document its missions, objectives and goals, there are limitations to this process."*

It is regrettable that, after the fact, the Division now chooses to deny those areas where it had previously signaled at least partial agreement with our audit conclusions included in the final audit report.

CIRT has developed a sound, effective cybersecurity program that has been validated by the DAR's findings which offer no opinion on CIRT operations. In accordance with the DHSES

[7] DAR at 3.

mission, CIRT delivers valuable services which have contributed to its supported entities' efforts to better secure their networks.

Thank you for the opportunity to respond to the report. If you have any questions regarding the Agency's response, please contact Brian D. Jackson of DHSES' Office of Internal Audit at (518) 457-5120.

Sincerely,

Benjamin Voce-Gardner
Director, Cybersecurity & Threat Mitigation Policy

cc: Commissioner Patrick A. Murphy
Terence O' Leary
Elisha Tomko
Brian Jackson