REQUEST FOR COMMENT ON CYBERSECURITY RULES FOR INFORMATION TECHNOLOGY

September, 12 2025

I. INTRODUCTION

In response to New York's Public Service Commission ("Commission") proposed regulation to create cybersecurity rules for regulated utilities within New York ("proposed regulation") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike appreciates the Commission's engagement with stakeholders and the opportunity to provide comments on the proposed regulation. We continue to support the proposed regulation's goal of better protecting New York's critical utilities and citizens from cybersecurity threats. Previously, CrowdStrike has commented on similar regulations from the Department of Financial Services[1] and the Department of Health.[2] Cyber threats continue to evolve and grow more severe. CrowdStrike's latest Global Threat Report notes that interactive intrusion activity against critical infrastructure sectors continues to be significant.[3] Additionally, in 2024, China-nexus activity surged

[1] Request for Comment on Revised Proposed Second Amendment to 23 NYCRR Part 500, CrowdStrike, https://www.crowdstrike.com/wp-content/uploads/2023/09/New-York-Cyber-Amendment-Comments.pdf.
[2] Request for Comment on Revised New York Hospital Cybersecurity Requirements, CrowdStrike, https://www.crowdstrike.com/wp-content/uploads/2024/07/NY-Hospital-Cybersecurity-Draft-2-Comments.pdf.
[3] "2025 *Global Threat Report*," CrowdStrike, https://www.crowdstrike.com/en-us/global-threat-report/.

150% and common eCrime technique "Vishing" attacks skyrocketed 442% between the first and second half of 2024 across all sectors – making steps to enhance cybersecurity in the sector timely and appropriate.

We do not have feedback on every aspect of the proposed regulation, but we do want to offer several points that may be of value to the Commission.

A. Cybersecurity Risk Management Practices

We commend the Commission for strengthening cybersecurity by amplifying attention given to this issue and defining expectations. There are some key steps organizations should take to strengthen their security posture that would help accomplish the proposed regulation's directive of adopting a sound, risk-based cybersecurity practice to mitigate their risk-of and risk-from a cyberattack. The proposed regulation includes some of today's most effective cybersecurity practices. We view the following as best practices for a comprehensive, risk-based, cybersecurity strategy.

Organizations should leverage several key technologies to defend against cyber threat actors:

- **Cloud Security**. Leveraging cloud systems provides numerous operational efficiencies and security enhancements. Given today's rapidly evolving threat landscape, organizations must address cloud-specific and cross-domain threats (where adversaries traverse cloud and on-premise environments). Security teams must protect data, manage identity and access, and hunt for and respond to threats in real-time. Capabilities of particular relevance include cloud workload protection, cloud-native application protection platform (CNAPP), cloud security posture management (CSPM), and Software-as-a-Service (SaaS) security.

- **Endpoint Detection and Response (EDR)**: EDR solutions defend endpoints such as desktops, laptops, servers, mobile devices, and cloud workloads from malicious activity. EDR provides granular visibility of potential threats. This enables holistic, real-time threat detection and proactive threat prevention. Leveraging EDR, defenders can perform threat hunting, incident response, and a variety of other essential cybersecurity tasks. EDR capabilities are a core pillar of most contemporary sophisticated security programs.

- **Next-Generation Security Information and Event Management (SIEM) solutions.** Sophisticated threats mean that modern enterprises must achieve visibility, context, and protection across systems and resources, including cloud and ephemeral resources. This often implies the need for multiple security and monitoring tools or capabilities. Next-Gen SIEM solutions leverage rich endpoint telemetry (like that captured by Endpoint Detection and Response [EDR] tools) and integrate it with other security-relevant event information from an array of sources. Supported by AI, this provides defenders a more coherent view, intuitive workflows, and ultimately better control of their environments.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats based on behavior cues rather than known signatures. Machine learning and artificial intelligence are essential to this end. Leveraging these technologies is essential to meeting constantly-evolving threats.

- **Identity Threat Detection and Response (ITDR)**: As organizations increase deployment of cloud services, work from anywhere models, and Bring-Your-Own-Device policies, enterprise boundaries continue to erode. Threat actors exploit resulting gaps and weaknesses from traditional authentication methods. In fact, compromised valid identities are a common initial access vector in incidents. However, emerging identity-centric approaches to security defeat these threats using a combination of real-time authentication traffic analysis, telemetry from endpoints, and machine learning analytics to quickly identify and prevent identity-based attacks.

Additionally, there are multiple security program requirements that bolster organizations' security posture:

- **Speed**. When responding to a security incident or event, every second counts. The more defenders can do to detect adversaries at the outset of an attack, the better the chances of preventing them from achieving their objectives. Adversaries work rapidly at the outset of breach to move laterally and escalate privileges, seeking to gain access to more systems and data and ensure persistence. This means that organizations should consistently measure and reduce their response time.

- **Threat Hunting**. Whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, skilled defenders can find them and thwart their goals. Proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The more well-instrumented the environment, the more opportunities defenders give themselves to identify malicious activity as an attack progresses through phases. Optimally defenders or their service providers continually hunt for threat activity 24/7, 365 days per year.

- **Zero Trust Architecture.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate security protections focused on identity and authentication. By eliminating transitive trust, Zero Trust Architecture concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. This constrains threat actors' ability to achieve actions on objective and provides additional opportunities for defenders to detect threats. The proposed regulation has MFA requirements to protect entities from identity and credential theft attacks. Importantly, Zero Trust architecture and identity threat protection concepts are important adjuncts to MFA-based guidance because they can stop attacks even if legitimate credentials are compromised and MFA is bypassed.

- **Logging Practices**. Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **Managed Security Service Providers**. Some entities lack the cybersecurity maturity to run effective security programs internally, or lack the scale to support a robust, 24/7, 365 days per year security capability. Increasingly, such entities should rely upon managed service providers, which can be more efficient overall and enable organizations to apply internal IT/security resources toward domain-specific challenges, including governance, risk, and compliance. Adopting an MSSP can radically strengthen organizations' security posture.

B. Reporting and Definition Harmonization

The Commission has not drawn from an existing "cybersecurity incident" definition, nor noted alignment with forthcoming federal definitions, but rather has created a new definition. As the Commission reviews this proposed regulation, and drafts other pieces of regulation, CrowdStrike urges alignment where possible with existing rules and regulations. The proposed regulation has the opportunity to strengthen cybersecurity for organizations that play critical roles in the everyday lives of many New Yorkers. Nonetheless, the new regulation will not be issued in a vacuum, but a variety of cybersecurity regulations. We recommend the Commission align future drafts with Cyber Incident Reporting for Critical Infrastructure Act's (CIRCIA) cybersecurity incident definition, and its forthcoming implementing regulation.

CrowdStrike recommends clarifying that there is no obligation to report "cybersecurity events," as currently defined. There are significant distinctions between cybersecurity events and incidents, and reporting of issues mitigated or resolved at the event-level is unlikely to provide additional value.

C. Secure-by-Design

The proposed regulation requires in-house developed applications use secure development practices. CrowdStrike views Security-by-Design and -Default principles as a positive change in driving greater security accountability for product makers. These principles are also a priority of the U.S. government. In April 2023, and updated in October 2023, the Cybersecurity and Infrastructure Security Agency ("CISA") and 17 international partners released a joint Secure-by-Design document which urges software manufacturers to take steps to design, develop, and deliver products that are secure from the very beginning of the process.[4] We recommend that engineers building applications reference the material publicly available from CISA, and other government agencies, on Security-by-Design and -Default principles to inform best practices in building secure applications.

D. Cybersecurity Audits

Cybersecurity audits have significant limitations as a cybersecurity tool. They are a useful tool for an organization to capture a snapshot of the existence of cybersecurity plans, strategies, or controls; however, audit results are only reflective of a point in time and cannot reflect a real-time measure of the state of an organization's security

[4] *Secure-By-Design*, CISA, October 2023.
https://www.cisa.gov/resources-tools/resources/secure-by-design

practices. While we recognize that it is the Commission's intention to create an auditing scheme, we would caution organizations against being overly reliant on the results. In addition to a cybersecurity audit, organizations should deploy cybersecurity best practices to continuously protect themselves from cyberattacks and data breaches and reevaluate if those technologies are working to the best of their ability more regularly than a yearly audit. Creating non-prescriptive mandates that nonetheless encourage organizations to analyze their risks, plans, and strategies is important for ensuring cybersecurity practices evolve with the threat landscape.

III. CONCLUSION

The Commission's proposed regulation represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. With an emphasis on adoption of practical security practices, these new requirements can raise the standard of cybersecurity across some of the most critical sectors. As the Commission moves forward, we recommend continued engagement with stakeholders.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***