REQUEST FOR COMMENT ON PROPOSED RULE TSA-2022-0001

ENHANCING SURFACE CYBER RISK MANAGEMENT

January 17, 2023

I. INTRODUCTION

In response to the Transportation Security Administration's ("TSA") Advanced Notice of Proposed Rulemaking on Enhancing Surface Cyber Risk Management, 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

We appreciate the TSA's efforts to strengthen the nation's cybersecurity and resiliency in the pipeline and rail (including freight, passenger, and transit rail) sectors. Pipeline operations are critical to the nation's supply chains, national security, and commerce. The rail sector enhances the nation's global economic competitiveness by enabling legitimate trade, transportation and travel. However, cyber risk management in these sectors is particularly difficult. The integration of operational technologies (OT) and information technologies (IT) leaves more surfaces exposed and vulnerable to cyberattacks.

Cybersecurity threats are evolving and increasing. Illustrative of this, in CrowdStrike's 2022 *Global Threat Report*, we observed a 82% increase in

ransomware-related data leaks (from 2021 - 2022).[1] Critical infrastructure sectors are included in that figure and also saw a sharp increase in data leaks from ransomware attacks – making steps to enhance cybersecurity in the sector timely and appropriate.

Furthermore, the legal and regulatory environment surrounding cybersecurity is becoming increasingly complex on account of (i) reliance on globally-distributed infrastructure, and (ii) evolving and potentially overlapping compliance obligations domestically and abroad. In order to ensure the most robust cybersecurity methods and disclosure, and compliance obligations remain feasible, regulators must endeavor to create clear and future-flexible expectations.

While we do not have feedback on every aspect of the proposed amendment, we do want to offer several points that may be of value to the TSA as it considers the proposed rule.

A. Cybersecurity Risk Management Practices

As the TSA revises the proposed amendment, CrowdStrike recommends the consideration of the following principles and technologies as best practices for cybersecurity programs. We view the following as best practices for a comprehensive, risk-based, cybersecurity strategy.

- **Extended Detection & Response (XDR).** Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. The next evolution of the ***Endpoint Detection and Response* (EDR)** concept, XDR seeks to leverage rich endpoint telemetry and integrate other security-relevant network or system events, wherever they exist within the enterprise, and generate intelligence from what otherwise may be an information overload.

- **Identity Protection and Authentication.** As pipeline and rail

[1] 2022 *Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/global-threat-report/

owner/operators embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, and cloud services multiply, enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.

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

- **Threat Hunting.** Whether through supply chain attacks or otherwise, we know that adversaries periodically breach even very-well defended enterprises. Properly trained and resourced defenders can find them and thwart their goals. In our experience, whether organizations accept this premise -- that cybersecurity involves not just a passive alarm, but a sentry actively looking for trouble -- is the leading indicator of the strength of their cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. And the better-instrumented the environment, the more chances defenders give themselves to intervene as a breach attempt progresses through phases, commonly referred to as the *kill chain*. Multiple opportunities for detection help avert "silent failures" -- where a failure of security technology results in security events going completely unnoticed.

- **Machine Learning-Based Prevention.** The core of next-generation cybersecurity solutions is the ability to defeat novel threats. Machine learning and artificial intelligence are essential to this end, and leveraging these technologies is the best way to gain the initiative against adversaries.

- **Zero Trust.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a

compromise. This is especially relevant for the pipeline and rail industries, who could have overlap between OT and IT systems, to prevent attackers from moving across systems.

- **Consideration of Managed Service Providers**. Some entities lack the cybersecurity maturity to run effective security programs internally. Increasingly, such entities should rely upon managed service providers to achieve the level of security appropriate for listed companies. Organizational transformations along these lines often involve a cross section of departments or teams (*e.g.*, personnel, finance, security, human resources) and can be most expeditiously resolved at the leadership level.

B. Harmonization

As TSA considers this proposed rule and other regulatory approaches, CrowdStrike urges alignment where possible with existing rules and obligations. We commend TSA for already identifying industry and government standards that could be used to develop a cyber risk management program. CISA's Cross-Sector Cybersecurity Performance Goals, and the forthcoming sector-specific controls and goals, share the same purpose of raising cybersecurity practices for important sectors. CrowdStrike recommends that TSA and CISA collaborate to create cohesion between any pipeline and rail sector-specific performance goals and regulations from TSA. Alignment between the two will ensure pipeline and rail providers, particularly small- and medium-sized businesses, can focus on raising the baseline of their cybersecurity practices holistically rather than focusing on checking boxes or compliance for the sake of compliance.

We also recommend alignment with the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and the forthcoming implementing regulation. Specifically, we recommend adhering to emerging best practices such as a 72-hour timeline for reporting requirements. Having varying reporting requirements for critical infrastructure sectors may yield confusion, when victims' full attention should be placed on remediating a cyber incident. Additionally, TSA should align with the definitions of a covered incident and covered entity from CIRCIA. Finally, there will be harmonization recommendations resulting from the ongoing work of

the Cyber Incident Reporting Council to align federal cyber incident structures and requirements that should be followed when appropriate by organizations.

III. CONCLUSION

The TSA's proposed rule represents a timely attempt to strengthen security outcomes in a critical industry and a complex legal and policy environment. CrowdStrike recognizes the TSA's proactive effort to develop a comprehensive and forward-looking approach to surface cyber risk management. As the TSA moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any proposed legislative updates focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about 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 CIPP/E
VP & Counsel, Privacy and Cyber Policy

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***