REQUEST FOR COMMENT ON THE NATIONAL CYBER INCIDENT RESPONSE PLAN UPDATE

February 14, 2025

I. INTRODUCTION

In response to the Cybersecurity and Infrastructure Security Agency's ("CISA") proposed update to National Cyber Incident Response Plan ("NCIRP Update") 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 CISA's engagement with stakeholders and the opportunity to provide comments on the NCIRP Update. We support the NCIRP Update's role of creating a framework to coordinate U.S. government response to incidents, and also outlining the potential roles of agencies, State, Local, Tribal, and Territorial (SLTT) governments, and the private sector. A well-planned and practiced incident response strategy can shorten response times and mitigate negative effects of a cyber attack.

The NCIRP Update correctly highlights that the U.S. must be prepared to handle significant cyber incidents that threaten our economy, national security, and public health and safety. National-state sponsored, along with eCrime, threat activity continues to increase. For example, over the past year, China-nexus intrusions increased 150 percent across all sectors on average compared to 2023. Among the top three sectors China-nexus adversaries most commonly target — government,

technology, and telecommunications — intrusion activity from China increased 50 percent in 2024 compared to 2023, making the NCIRP Update very timely and needed.[1]

A. Increased Collaboration with the Private Sector

The NCIRP Update states one of its goals is to harness the expertise, capabilities, and authorities of both public and private sectors to tackle significant incidents. The private sector is a key partner for the U.S. government's cybersecurity strategy. Cybersecurity vendors, like CrowdStrike, provide cyber threat intelligence, technology offerings, and participate in formal public-private partnerships, like CISA's Joint Cyber Defense Collaborative (JCDC) to improve not only the U.S. government's cybersecurity, but also the broader cybersecurity ecosystem. The NCIRP Update highlights many areas where the private sector should be involved in incident response to a severe cyber incident. However, there are still opportunities for additional collaboration.

As a community, it is a pivotal time for a serious conversation about expanding national Incident Response (IR) capacity. IR demand is incredibly elastic, and IR supply is relatively fixed. The best practice for private entities is to have an IR retainer in place, so a skilled provider can offer assistance within a stipulated time frame, and under other terms outlined in a Service Level Agreement. While this best practice might not be exactly replicable in the public sector, a program, likely led by CISA, that retained skilled private sector providers in advance for use during significant cyber incidents could expand the cybersecurity workforce and strengthen national resilience.

Eligibility for benefits under such a program could be based on the severity scale in the NCIRP Update and leveraging this group could be in the response flow. In the NCIRP Update, part of the response phase is to "determine key non-governmental stakeholders to contribute to solution development and implementation." A predetermined group like described above could save valuable time, mitigate crippling impacts, ensure CISA had the ability to orchestrate response activities, and maintain insight into findings in real-time throughout multiple concurrent IRs.

The NCIRP Update correctly notes that "at times, technology ecosystem companies or other non- governmental stakeholders may have relevant capabilities to disrupt threat actors." As collaboration efforts like CISA's Joint Cyber Defense Collaborative (JCDC) continue to evolve, groups should conduct more focused, applied planning regarding

[1] *CrowdStrike Testimony before the U.S. Committee on Homeland Security*, 2025. https://homeland.house.gov/wp-content/uploads/2025/01/2025-01-22-FC-HRG-Testimony.pdf

such activities. Further, efforts should cover proactive operations seeking to disrupt adversary infrastructure based on defined criteria, rather than waiting to do so in response to a major incident. Disruption activities should be aligned to coordinated law enforcement actions where possible, and broader diplomatic and defense activities where appropriate.

B. Consider Detection and Response Functions Holistically

Over the past number of years, there has been a convergence of detection and response within cybersecurity to create a continuous cycle. Due to radically reduced *breakout time* (the time it takes an adversary to move laterally from an initially compromised resource) from sophisticated adversaries, serialized approaches to finding and stopping threats have failed. Endpoint Detection and Response (EDR) solutions helped define and continue to embody this concept. CrowdStrike has advocated for a unified approach to these functions in other contexts, but the point applies here as well.[2] We recommend that CISA consider approaches to unifying the "Detect" and "Respond" phases of the NCIRP Update to face threats in a more adaptive manner.

III. CONCLUSION

The NCIRP Update represents a thoughtful attempt to strengthen incident response in a complex legal and policy environment. As this update moves forward, we recommend continued engagement with stakeholders, especially given the important role the private sector plays in this effort. Finally, because the underlying technologies evolve faster than law and policy, we recommend CISA continue to focus on principles rather than prescriptive requirements and conduct regular updates to the plan.

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.

---

[2] *CrowdStrike Comments on NIST Cybersecurity Framework 2.0*, 2023. https://cs-staging-2-www.crowdstrike.com/wp-content/uploads/2023/06/NIST-CSF-2.0-Discussion-Draft-Comments.pdf

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 CIPP/E
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

©2025 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are trademarks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

***