FEEDBACK/OBSERVATIONS SUBMISSION FORM

Name: Līga Rozentāle

Employer / Organization: CrowdStrike

Job Title / Position: Director, Public Policy EMEA

Email: policy@crowdstrike.com

Contact Number: +32473944836

The Authority may contact us regarding any inquiries or questions regarding CrowdStrike comments.

GENERAL NOTES:

DRAFT NATIONAL FRAMEWORK FOR CYBERSECURITY INFORMATION SHARING AND INCIDENT RESPONSE

July 10, 2026

I. INTRODUCTION

In response to the Kingdom of Saudi Arabia's ("the Kingdom") National Cybersecurity Authority's ("NCA") request for feedback on the Draft National Framework for Cybersecurity Information Sharing and Incident Response ("Draft Framework"), CrowdStrike offers the following views.

We approach these comments as a leading international, U.S.-headquartered, cybersecurity provider that defends enterprises from globally distributed threats. Our AI-powered, cloud-native platform delivers state-of-the-art, real-time detection, automated protection, and threat intelligence across endpoints, cloud, identity, data, and AI workloads. Our insights are informed by applied, real-world experience across global industries through our software-as-a-service cybersecurity platform, incident response, managed threat hunting, and managed security services. CrowdStrike's recommendations are grounded in this operational experience.

II. COMMENTS

CrowdStrike commends the NCA for its continued leadership in advancing a secure, resilient, and trusted cyberspace for the Kingdom. We strongly support the NCA's goal of better protecting Saudi Arabia's critical infrastructure, priority sectors, government services, businesses, and citizens from cybersecurity threats. The Draft Framework is an important step toward reinforcing the cyber resilience needed to support Saudi Arabia's Vision 2030 digital transformation and economic diversification objectives. We also welcome the Framework's emphasis on sharing timely and actionable cybersecurity information with entities in scope, and believe that effective, two-way information sharing between government and industry can play a critical role in improving collective defense, accelerating incident response, and strengthening trust across the Kingdom's digital ecosystem.

A. *Definition of Cybersecurity Incident*

CrowdStrike encourages the NCA to consider achieving balance in defining "cybersecurity incident." The volume of resulting reports should be sufficient to discover and alert entities about systemic and/or widespread threats; but not be so great as to create "noise" for analysts and extra work for those affected by low-impact commodity threat activity.

In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and regulations. In most cases, organizations using contemporary cybersecurity solutions are alerted to malicious activity occurring in their environment. The nature of these alerts may vary, and could cover something like the installation of malicious software on one system, or the compromise of a single account. In scenarios where defenders see these alerts and address them quickly, the alert may not rise to the threshold of a cybersecurity "incident," where the threat actor has not meaningfully achieved their objective, accessed sensitive information, and the like.

The attack vector alone should not be a predicate for a covered incident; the outcome of the attack (e.g., a material impact) should determine reportability regardless of the means. This approach ensures the definition remains durable as adversary tactics, techniques, and procedures evolve over time.

B. *Reporting of Potential Cyber Incidents*

CrowdStrike respectfully recommends that the NCA carefully reconsider the requirement to report "potential" cybersecurity incidents. As noted above, an important distinction exists between alerts and incidents. The volume of resulting reports should be sufficient to discover and alert entities about systemic and/or widespread threats; but not be so great as to create "noise" for analysts and extra work for those affected by low-impact commodity threat activity. Extending mandatory reporting obligations to potential incidents, without clear definitional thresholds, risks precisely that outcome.

It is extremely difficult, if not impossible, to create a uniform threshold for when a "potential" incident becomes reportable that could be applied consistently across various types of entities and incidents. Consideration of the impact and severity of an incident is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures. As a part of the framework's implementation, the NCA should consider developing guidance, such as case studies, for covered entities as to what it believes is "reasonable" in varying circumstances to ensure entities are in a position to best comply with the requirements of the framework.

C. *Incident Reporting Timeline*

To further support the Framework's objectives, CrowdStrike encourages the NCA to reconsider the requirement that entities report cybersecurity incidents "immediately" upon detection. Based on our experience performing incident response services for a variety of cyberattack victims, entities confront significant constraints in the immediate hours of an incident. In some cases, satisfying reporting obligations may divert resources and attention from the incident remediation process itself. This, in turn, could amplify the impact of the incident.

A 72-hour initial reporting window is rapidly emerging as the common international timeframe, reflected in frameworks such as the European Union's NIS2 Directive and the U.S. Cyber Incident Reporting for Critical Infrastructure Act. Rather than requiring immediate reporting, CrowdStrike recommends the NCA adopt this 72-hour standard for an initial notification, with supplemental and final reports submitted as the investigation matures and additional facts become available.

Notably, incidents with divergent impacts could look similar in the early investigation stage. Requiring immediate reporting before an entity has had adequate time to assess the nature and scope of an intrusion will result in the submission of incomplete,

extraneous, or potentially inaccurate information. A 72-hour window allows entities to conduct necessary triage while still ensuring the NCA receives timely notification of significant events.

D. *Reporting of Threats Observed Affecting Other National Entities*

CrowdStrike respectfully recommends the NCA to remove the third-party reporting requirement — that is, no obligation for one entity to report cybersecurity threats or incidents observed affecting a separate national entity. The "duty to report" should be the responsibility of the impacted entity itself.

Today, many entities rely upon third parties such as cybersecurity companies, incident response providers, law firms, and insurance providers to comply with notification obligations. This is appropriate and should be preserved. However, there is an important distinction between a third party reporting on behalf of an impacted entity — at that entity's request — and an affirmative obligation to report on another entity's behalf without that entity's knowledge or consent.

Mandating that entities file reports about threats observed affecting other organizations creates significant practical problems. An entity observing indicators that suggest another organization may be affected is, by definition, working with incomplete information. They lack visibility into the other entity's systems, cannot confirm whether an incident has actually occurred, and cannot assess scope or impact. Requiring formal reports based on such incomplete observations risks flooding the NCA with unverified information, while simultaneously creating potential legal and reputational harm to the organizations being reported upon. The most accurate and complete information about an incident will always come from the affected entity itself, and the framework should be structured to reinforce that principle rather than displace it.

E. *Mandatory Immediate Vulnerability Disclosure*

CrowdStrike recommends that the NCA align any vulnerability disclosure requirements with established industry best practices rather than requiring immediate notification upon discovery of a vulnerability.

Within the private sector, coordinated vulnerability disclosure norms have developed to balance timely information sharing with the need to prevent avoidable harm.

Security researchers commonly provide a remediation window after discovering and reporting a vulnerability in another vendor's software, often allowing up to 90 days before public disclosure, while shorter timelines may be appropriate where active exploitation or other heightened risk factors are present. This window is especially important where premature disclosure could increase risk, including where data extortion is involved, where confidentiality is necessary to support law enforcement activity, or where additional time is needed to validate the issue and develop effective mitigations.

CrowdStrike respectfully recommends that the NCA clarify Article 6.1.6 to distinguish between threat or incident information that warrants immediate reporting and vulnerability information that is better handled through a coordinated vulnerability disclosure process. This distinction is increasingly important as AI accelerates both defensive and malicious vulnerability discovery, increasing the speed and volume of potential findings. Requiring immediate disclosure of every unvalidated or unprioritized vulnerability could overwhelm the NCA with information that may not yet be actionable and, in some circumstances, risk exposing exploitable weaknesses before patches or mitigations are available. A coordinated, risk-based approach would better support timely, actionable information sharing while preserving the flexibility needed to assess reachability, exploitability, asset criticality, attack paths, and real-world adversary behavior.

III. CONCLUSION

CrowdStrike respectfully commends the NCA for its leadership in developing the Draft Framework, which represents an important step forward in strengthening the Kingdom's national cybersecurity posture and advancing a secure, resilient, and trusted cyberspace. We appreciate the opportunity to provide comments and would welcome continued engagement with the NCA as the Draft Framework moves toward implementation, including opportunities for industry stakeholders and potential covered entities to provide practical technical input. In recognition of the pace at which cybersecurity capabilities continue to evolve for both defenders and adversaries, CrowdStrike respectfully recommends that the Framework, where appropriate, prioritize principles-based requirements and include mechanisms for periodic review, updates, and revisions to ensure it remains effective, risk-informed, and aligned with the Kingdom's long-term cybersecurity objectives.

IV. ABOUT CROWDSTRIKE

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform 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/.

CONTACT

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

Drew Bagley
Chief Privacy and Policy Officer

Līga Rozentāle
Director, Head of Public Policy, EMEA

Email: policy@crowdstrike.com

***