May 9, 2022

U.S. Securities and Exchange Commission
Washington, DC 20549

File Number S7-09-22 – Comments on Proposed Rule

The undersigned submit these comments in support of the objectives of the rules regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies proposed by the Commission on March 9, 2022 (the "Proposed Rules").

The undersigned are Principals of the Cyber Initiatives Group, a committee formed and sponsored by The Cipher Brief, a private media organization that engages with the private sector in the United States to promote awareness of cybersecurity and national security matters. Many of us currently have direct involvement in cyber matters in the private sector and have significant experience in both policy and operational aspect of cybersecurity; many of us have served at the highest levels of our nation's armed forces or intelligence community, while others have leading roles at the nation's most significant cybersecurity firms and technology providers. (We are writing in our individual capacities and the affiliations noted below are merely for identification purposes.)

Our purpose in submitting these comments is to support the objectives of the Proposed Rule, to advise the Commission that in our opinion national security concerns are a valid and significant rationale for the rulemaking, and to underscore that the Proposed Rule has the potential to benefit not only investors and registrants but also, and in our view more importantly, our national security. In doing so, we are not commenting on the scope, regulatory burden, or other technical aspects of the Proposed Rule – as others can more appropriately address those details. We are, however, in a position to comment on the national security ramifications of a better cybersecurity posture for public companies.

As the Commission notes in its Background Statement accompanying the Proposed Rule, "[l]arge scale cybersecurity attacks can have systemic effects on the economy as a whole, including serious effects on critical infrastructure and national security."

All of the undersigned are familiar with the technical sophistication of our cyber adversaries and believe that this will continue to increase, imposing greater risks to our nation. In that regard, we note that the *Annual Threat Assessment of the U.S. Intelligence Community* (dated February 7, 2022) cited cyber-malevolence from four nation-state adversaries – China, Russia, Iran and North Korea – as top-ranked threats. Unfortunately, as the adversarial threat increases, so too has our vulnerability, as we increasingly rely on digital technology throughout all aspects of our commercial, governmental and personal lives. The advent of the internet of things, and the vast amounts of data that are being generated, stored, and used by 5G telecom technology, artificial intelligence and potentially quantum computing (to name just a few developments), will create additional attractive targets for malicious cyberactivity, thus increasing the risk to our nation's infrastructure, businesses and citizens. Much of this technology is owned and operated by public companies. These vulnerabilities can directly affect our national security.

We believe that the goals of requiring current reporting about material cybersecurity incidents, as well as periodic disclosures regarding (1) a registrant's policies and procedures to identify and manage cybersecurity risks, (2) management's role in implementing cybersecurity policies and procedures and (3) the board of directors' cybersecurity expertise and its oversight of cybersecurity risk, are appropriate and are likely to enhance the cybersecurity posture of registrants. Public companies own critical infrastructure, operate or manage key businesses in every industrial, agricultural and service sector, and in many respects form the backbone of the American economy. Consequently, improved cybersecurity within public companies translates directly into a national economy that is more cyber-secure and cyber-resilient. It stands to reason that requiring additional reporting about material cyber incidents will better inform investors, the public generally and governmental agencies, and increased disclosure about cyber policies and board experience will encourage public companies (and by extension, private companies, at least to some degree) to meet if not exceed market expectations in those areas.

By their inherent nature, these benefits cannot be easily quantified, but lack of precise measurement cannot in this case be a reason to deny what is manifestly obvious and logical. We believe that these benefits to our national wellbeing are critical and may and should be taken into account in policy development and rulemaking by the Commission.

We understand that interested parties will have different views on the scope and other technical aspects of the Proposed Rule and as noted above, are not expressing an opinion here on those issues. But we do wish to point out that any effort to standardize and harmonize notification and disclosure with other requirements (such as those that will be implemented under the Cyber Incident Reporting for Critical Infrastructure Act of 2022) will obviously have the effect of increasing robust compliance with, and further the purposes of, the Proposed Rule.

Questions regarding these comments may be addressed to signatory Glenn Gerstell (at [redacted]) or Cipher Brief CEO Suzanne Kelly [redacted]

Thank you for the opportunity to submit these comments.

Very truly yours,

Kelly Bissell
Global Security Services Lead, Microsoft Corporation

Glenn S. Gerstell
Former General Counsel, National Security Agency

HON. Sue Gordon
Former Principal Deputy Director of National Intelligence

Matt Hayden
Former Assistant Secretary of Homeland Security for Cyber, Infrastructure, Risk and Resilience

GEN Michael Hayden (Ret.)
Former Director of the Central Intelligence Agency and the National Security Agency

HON. S. Leslie Ireland
Former Assistant Secretary of the Treasury for Intelligence and Analysis

Richard H. Ledgett, Jr.
Former Deputy Director, National Security Agency

RADM Mark Montgomery (Ret.)
Former Executive Director Cyberspace Solarium Commission

Debora Plunkett
Former Director of the Information Assurance Directorate of the National Security Agency