May 9, 2022

Secretary Vanessa Countryman
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Re: File Number S7-09-22, Securities and Exchange Commission (SEC) Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Secretary Countryman:

The National Defense Industrial Association (NDIA) represents more than 1,800 corporate and over 60,000 individual members from small, medium, and large contractors, educational institutions, and governments; NDIA members and their employees feel the impact of any policy change made to how the United States equips and supports its warfighters to win in all domains of warfare.[1]

Earlier this year, the Securities and Exchange Commission (SEC) proposed a rule that would require companies to implement a variety of cybersecurity incident reporting measures. The stated purpose of this proposal is to "better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents." However, our members believe that while well-intentioned, these proposed regulations will impose serious and avoidable problems for publicly traded companies operating within the defense and national security space. In this letter, we seek to address nine key areas that present possible problems or conflicts and propose alterations to the proposed rule that would best support companies performing vital government work.

I. Four Business Day Reporting Requirement:

A key tenet of the SEC's proposal will require a company to report to investors within four business days of determining that it has experienced a material cybersecurity incident. This will create situations in which the company would be required to:

-Make complex determinations on materiality with information available during the early stages of the incident, which also potentially is information that may be incorrect or incomplete

[1] NDIA is a non-partisan, non-profit, educational association that has been designated by the IRS as a 501(c)3 nonprofit organization - not a lobbying firm - and was founded to educate its constituencies on all aspects of national security. For over 100 years, NDIA has provided a platform through which leaders in government, industry, and academia can collaborate and provide solutions to advance the national security and defense needs of the nation.

-Potentially disclose information about material incidents that would benefit perpetrators of cyber attacks

Regarding the first point, much is unknown in the early days of an incident, including the type and scope of information potentially impacted. It is probable that such a short disclosure timeframe would lead to rushed disclosures of information that are ultimately incorrect. In addition, because companies may take longer than four business days to contain a major cyber incident, requiring public disclosures prior to containment could tip off bad actors and lead to additional cyber-attacks.

In the rush to report, a company also may be required to publicly report the existence of a zero-day vulnerability in vendor software without an opportunity to responsibly report the vulnerability. Public disclosure of such unpatched, zero-day vulnerabilities, could tip off bad actors to look for other victims to attack, leading to additional cyber-attacks across a wide array of industries.

Proposed Solution: NDIA urges the SEC to reevaluate the trigger for a company reporting within four business days of determining that it has experienced a material incident and to allow for a company to report after being given an opportunity to first contain the event. NDIA would also urge the SEC to specify that companies do not have an obligation to describe, with particularity, the details of any vulnerabilities in their systems that they reasonably believe could assist cyber attackers, or details of vulnerabilities in third-party software that have not been disclosed by the third-party software vendor.

II. Lack of Guidance Concerning Disclosures:

The SEC's proposal also requires companies to publicly disclose any material changes, additions, or updates to previously reported cyber incidents. While the proposed rule does not provide further guidance on what constitutes a reportable material change, addition or update, NDIA views there to be a substantial body of guidance and case law on what is viewed as material for public reporting to shareholders under SEC rules. Accordingly, NDIA does not believe further guidance is warranted at this time. Once the SEC and companies have further experience in this area, this area might be revisited.

III. Lack of Coordination to Protect Law Enforcement and/or National Security Interests:

An issue of concern to NDIA is the lack of an exception that would delay reporting of material incidents in cases where disclosure could negatively impact law enforcement or national security. NDIA members are concerned that in the rush to comply with a 4-business day reporting deadline, companies that have experienced cyber incidents impacting classified or controlled unclassified information, or that are involved in law enforcement investigations may be put in an impossible situation. They would have to choose between violating SEC disclosure obligations and violating statutes prohibiting unauthorized disclosures.

Proposed Solution: NDIA respectfully suggests the inclusion of a provision to allow a delay in reporting of material incidents under certain circumstances. Primarily, this would occur when the company has been informed by government authorities that a delay in disclosure would be in the interest of national security, or an ongoing law enforcement investigation. It would also be useful to clarify that companies do not have an obligation to describe with particularity in their reporting any information related to classified or otherwise controlled information, systems, or programs.

States reporting laws also vary from state to state. NDIA suggests that the SEC seek to harmonize these varied reporting rules once additional opportunity to observe cyber incident laws and reporting in action.

IV. Disclosure of Cybersecurity Incidents That Become Material in the Aggregate:

The SEC's proposal requiring companies to disclose when a series of previously undisclosed individually immaterial cybersecurity incidents have become material in the aggregate creates an ambiguous standard. We believe this to be a highly subjective and potentially imprecise calculation that will prove to be unworkable.

Proposed Solution: NDIA respectfully urges the SEC to remove this proposed requirement.

V. Cybersecurity Incidents Have a Scope That is Too Broad:

NDIA notes that the proposed SEC rule defines a cybersecurity incident to include an unauthorized occurrence on, or through, a registrant's "information systems." The proposed definition of which would include information resources "owned or used" by the registrant. NDIA believes that this language is problematic because a company may use many systems to process its data, including vendor systems. In such circumstances, in which companies often rely on vendors to inform them of cyber incidents impacting the systems, companies may have particular challenges in obtaining sufficient information from the vendors in time to make their disclosure.

Proposed Solution: In the definition of "information systems," NDIA would urge changing "owned or used by the registrant" to "owned or operated by the registrant." This would allow companies to more reasonably obtain sufficient information about incidents on systems that they own or actually operate.

VI. Disclosure of Cyber Expertise of Board Members

NDIA is concerned that it may not be essential that Board members themselves have specialized expertise in cybersecurity. There already is a shortage of personnel with cybersecurity expertise to address ongoing challenges and risks associated with cybersecurity and cybersecurity incident identification, reporting, and remediation. Public companies need

appropriate oversight by Board members and can hire cyber expertise for specific roles within the company and / or as consultants to the Board where and when needed.

VII. Impact of the Proposed Rule on Small Businesses

As the SEC is aware, public companies are not always behemoth corporations. Within the Defense Industrial Base (DIB) there are a number of public companies that fall within the micro-cap and nano-cap range. These companies have less resources than larger companies. The proposed rule notes that there will be a cost impact and that enhanced disclosure could "potentially increase the vulnerability of registrants" by providing "a road map for future attacks." But the proposed rule specifically subjects small businesses to the new requirements.. The SEC should re-consider the impact of the proposed rule on these small businesses which have limited resources to begin with, and may find it more difficult than large companies to identify board members with requisite cyber expertise given that there already is a lack of talent in this area. See VI, above. NDIA requests that the SEC coordinate this reconsideration with the Department of Defense, which has considerable experience with implementing its own cybersecurity rules and understands more fully the impact that such implementation has on small businesses.

VIII. Impact of the Proposed Rule on Different Industries

The proposed rule discusses that companies may be under other cybersecurity incident reporting mandates because of their particular industry. The Federal Acquisition Regulation (FAR) and National Institute of Standards and Technology (NIST) which promulgate standards on cybersecurity applicable to the DIB are mentioned but only in footnotes in the proposed SEC rulemaking. Although other mandates are mentioned, the proposed rule simply notes that there are varying standards and requirements for reporting. The SEC should consider whether it should tailor its mandates to specific industry concerns and approaches. This not only would benefit the industry member companies, but also its investors. NDIA suggests that the SEC consider the potential benefits of seeking alignment with industry-specific requirements.

IX. Risk of Third-Party Litigation

NDIA notes that, while this may be beyond the scope of the current rulemaking, the proposed rule may be the source of third-party litigation. That is a significant concern in the DIB where the goal of DIB member public companies is to assist the government with its national security mission. Third party litigation poses challenges and costs that may take up the time and resources of DIB companies, in addition to the other concerns about reporting and safeguarding national security and law enforcement information previous mentioned in these comments. NDIA and its membership firmly appreciate the SEC's desire to enhance cybersecurity related disclosures. We do, however, have significant concerns surrounding certain aspects of these proposed rules. For the reasons alluded to, we respectively suggest changes in light of the unique

challenges faced by companies that operate in the defense sector. NDIA stands ready to assist in revising and updating these proposals and would welcome this collaboration.

NDIA appreciates the opportunity to address our concerns pertaining to this matter. NDIA's point of contact is Jeff Goldberg, Director of Regulatory Policy, who may be reached at [redacted].

Sincerely,

National Defense Industrial Association