May 9, 2022

Vanessa A. Countryman
Secretary, Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Subject: File Number S7-09-22, Comments to Proposed Rule “Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure”

Dear Ms. Countryman:

On behalf of the Aerospace Industries Association of America (AIA), I am pleased to offer the enclosed comments in response to the Securities and Exchange Commission’s proposed rule, “Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure.” For over 100 years, AIA has been the industry voice shaping the policies that matter most to our members, comprising over 320 of the nation’s leading aerospace and defense manufacturers and suppliers of civil, military, and business aircraft, helicopters, unmanned aerial systems, space systems, aircraft engines, missiles, and related components, equipment, services, and information technology. As you finalize the proposed rule, AIA appreciates the SEC’s consideration of our comments on four specific areas of concern: national security implications, four business day reporting, aggregation of prior incidents, and third-party systems.

National Security Considerations Beyond Law Enforcement Investigations

Our members understand the intent of the SEC in bringing greater transparency and consistency to registrants’ material cybersecurity incident disclosures for the benefit of current and potential shareholders. Given the nature of the national security and intelligence work our member companies perform in support of our nation, we particularly appreciate the SEC’s recognition that “cybersecurity attacks can have systemic effects on the economy as a whole, including serious effects on critical infrastructure and national security.” We also appreciate the opportunity to provide input regarding whether the final rule should “provide that the Commission shall allow registrants to delay reporting of a cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General’s written determination that the delay is in the interest of national security.” We fully support this authority to delay reporting, and we believe it should be both expanded and clarified.

Because aerospace and defense (A&D) manufacturers perform vital national security functions, our members’ business and classified networks contain both proprietary data – their own, and data from their suppliers and subcontractors – but also highly sensitive (frequently classified) information related to the critical products and services they provide to the Department of Defense (DOD), the Department of Homeland Security (DHS), U.S. Intelligence Community (IC) agencies and the Office of the Director for National Intelligence (ODNI). This data can range from technical details that could help an adversary replicate or defend against our advanced technologies, to logistical details...
associated with operationally critical support that could reveal the planned deployment or
movement of troops or critical equipment. If the material cybersecurity incident involved
national defense or intelligence capabilities, products, or platforms, public disclosure of
the information contemplated by the proposed rule could cause further damage to
national security interests well beyond the damage of the event itself. For example, it
may alert malicious actors that we have uncovered their illegal activities in
circumstances where our defense and intelligence agencies wish to keep that
information secret, both to better protect the networks under attack, and to have time to
alert other companies and government agencies that may not have yet discovered the
same vulnerability. Our adversaries could accelerate and expand their attacks once they
realize they have been discovered, leading to greater damage to national security and
critical infrastructure. Similarly, a company’s public disclosure of the event would help
the adversary authenticate the data that was taken.

While the Attorney General may be well-suited to making national security
determinations in instances involving ongoing law enforcement activities, the
Department of Justice may not recognize the national security implications of other cyber
incidents. A&D manufacturers are already required to report cyber incidents to their
government customers, who may in turn – through contract clauses or other
mechanisms – determine that a cyber event is classified and thus restrict the company
from making the mandatory public disclosure in the timeframe prescribed by this
proposed rule. To resolve this untenable position, we believe that authority to exempt or
delay public reporting of an event not be limited to the Attorney General but should be
granted whenever a company reports an event that impacts national security to the
DOD, DHS, or the IC (including ODNI) via the applicable prescribed reporting
mechanisms; and that each of those agencies should designate which specific officials
shall have the authority to grant such determinations on behalf of their agencies. This
expanded authority could be achieved by adding “unless public disclosure would have
an adverse impact on national security, as determined by the Department of Justice,
Department of Defense, Department of Homeland Security or the Office of the Director
of National Intelligence” to the instructions of the proposed Form 8-K Item 1.05.

Four Business Day Reporting Period
The SEC’s proposal to require reporting of material cyber incidents to investors within
four business days of a materiality determination could require companies to make
complex determinations in the early stages of a forensics examination while many of the
underlying facts are evolving and yet unknown, potentially resulting in disclosures with
information that ultimately turns out to be incorrect or incomplete. This release of early,
flawed information could harm the company and its shareholders by needlessly and
artificially reducing the value of the company’s shares, thus causing financial instability
for that company and weakening the defense industrial base more broadly.

Early public disclosure of material cyber incidents could also create opportunities for
malicious actors to further victimize the company. Given the material nature of an
incident that triggers reporting, companies may not have fully mitigated the incident and
secured their networks. Public disclosure would not only tip off the original actor that the
cyber incident had been uncovered but also alert other bad actors to the potential vulnerability of a company’s systems.

Aggregation of Prior Immaterial Cybersecurity Incidents

The SEC’s proposal to require companies to disclose when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate is impractical. Instructing companies to “analyze related cybersecurity incidents for materiality, both individually and in the aggregate” does not provide sufficient guidance as how and under what circumstances such prior incidents are “related” and thus should be aggregated. AIA urges the SEC to remove this proposed requirement, as it would likely result in highly subjective determinations.

Third Party Systems

A&D companies have significant experience managing complex and proliferated supply chains and can thus attest to the potential difficulties of reporting material third party cybersecurity incidents as contemplated by the proposed rule. As a customer/user of a third-party system, companies may not be provided sufficient information about an incident and could be bound by confidentiality obligations with respect to the information they are provided. This makes it difficult to make a materiality determination and/or provide relevant information for disclosure.

AIA and its member companies remain fully committed to securing the sensitive information entrusted to them. Thank you for your consideration of our comments; please direct any questions to Jason Timm, AIA’s Director of Defense Policy & Integration, at [redacted] or [redacted].

Sincerely,

John Luddy
Vice President, National Security Policy