REQUEST FOR COMMENT

SEC PROPOSED RULE: CYBERSECURITY RISK MANAGEMENT, STRATEGY, GOVERNANCE, AND INCIDENT DISCLOSURE

SUBMISSION

Submitted by
Organization: (ISC)^2

Category: Other – (ISC)^2 – Information Security Industry Body – Not for Profit
Consent: This submission can be made public and published.

EXECUTIVE SUMMARY

(ISC)² is pleased to submit comments and views in relation to the SEC Proposed rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.

(ISC)² is an international not-for-profit membership association of more than 170,000 certified cyber security professionals, focused on inspiring and delivering a safer and more secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, the Certified Cloud Security Professional (CCSP®) certification, the Systems Security Certified Practitioner (SSCP®) certification, and the Certified Secure Software Lifecycle Professional (CSSLP®) certification, amongst others, (ISC)² offers a portfolio of certifications that are part of a holistic, programmatic approach to security. Our membership consists of certified cyber, information, software and infrastructure security professionals who are making a positive impact and helping to advance the cyber security, information security and privacy industries. Our vision is supported by our commitment to educate and reach the public through our charitable foundation – The Center for Cyber Safety and Education.™

(ISC)²'s mission is to support and provide members and constituents with certifications, resources, and leadership to address cyber, information, software, and infrastructure security to deliver value to society. The first information security certifying body to meet the requirements of the ANSI ISO/IEC 17024 standard, a global benchmark for personnel certification. (ISC)² certifications including the CISSP, CCSP, SSCP, CSSLP, CISSP-ISSMP, CISSP-ISSAP, CISSP-ISSEP and HCISPP have been accredited against this standard. (ISC)² certifications are a must-have among information security professionals and employers. (ISC)² certifications are recognized across the globe including by the United States Department of Defense (DoD) through the 8140.01 and 8570.1 Directives.

Around the world, (ISC)² has formed strong and long-lasting partnerships with the International Standards Organization (ISO) as well as the National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI) and National Institute for Cybersecurity Education (NICE). (ISC)² works closely with numerous government agencies and bodies. As a result of the leadership position (ISC)² has taken to promote a safer and more secure cyber world, (ISC)² certifications are regarded as the gold standard in cyber security certification and excellence around the world.

(ISC)² requests that the SEC will consider the response submitted by (ISC)² to assist in creating and evolving a more secure cyber security landscape in the United States. (ISC)² selected several questions that we deemed pertinent to our work and expertise to address in our response.

TABLE OF CONTENTS

PREAMBLE

On March 9, 2022, the SEC released its much anticipated proposed rules relating to cybersecurity risk management, incident reporting, and disclosure for investment advisers and funds.

The proposal would require a company to report, to the extent known: when an incident was discovered and whether it remained ongoing; a brief description of the incident; what data has been determined to be taken, changed, accessed; how the incident affected the company's operations and; what steps, if any, have been taken to address the situation.

It is noted that the SEC does not expect initial disclosures to include specific or technical information about its response plans, its security systems, its networks, its vulnerabilities, or other information that could assist attackers or obstruct remediation efforts. The proposed SEC amendments would also require disclosure of directors' cybersecurity 'expertise'.

As the world's largest nonprofit association of certified cyber security professionals, (ISC)^2 strives toward a vision of a safer and more secure cyber world. Core to this vision is that the organizations which power the American economy, such as those that fall under the scope of the proposed SEC rules, operate in a cyber safe, secure and responsible manner. This submission highlights the position of (ISC)^2.

RESPONSES TO CONSULTATION QUESTIONS

QUESTION 1. WOULD INVESTORS BENEFIT FROM CURRENT REPORTING ABOUT MATERIAL CYBERSECURITY INCIDENTS ON FORM 8-K? DOES THE PROPOSED FORM 8-K DISCLOSURE REQUIREMENT APPROPRIATELY BALANCE THE INFORMATIONAL NEEDS OF INVESTORS AND THE REPORTING BURDENS ON REGISTRANTS?

RESPONSE:

(ISC)^2 believes that investors would benefit from reporting about material cybersecurity incidents on Form 8-K.

The proposed reporting requirements require disclosure of 'material cybersecurity incidents' within four business days after the company determines that it has experienced a material cybersecurity incident[1]. The proposed rule expands on the SEC's 2018 guidance, which, among its points, recommends issuers disclose cybersecurity incidents and risks that would be material to its investors prior to the offer and sale of securities[2].

The current and proposed rules are designed to help ensure informed decisions are made by investors regarding cybersecurity breaches. In relation to proposals to amend 8-K, (ISC)^2 suggests a 'material' cyber breach be wholly defined and determined as part of the new rules and regulations. Under the proposed Item 1.05 to Form 8-K, 'material cyber incident' is defined as 'an unauthorized occurrence on

1

1 Form 6-K General Instruction B would be similarly amended to add "cybersecurity incidents" as a potential reporting event.
2 See Commission Statement and Guidance on Public Company Cybersecurity Disclosures at 11, Release No. 33-10459 (Feb. 26, 2018) No. 33-10459 (Feb. 21, 2018) [83 FR 8166].

or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.' Furthermore, the SEC has stated that 'cybersecurity incident' should be interpreted and construed 'broadly; and may include 'an accidental exposure of data'.

(ISC)^2 recommends that proposed terms be further defined to be more specific as to which incidents should or could be determined to be 'material'. This would serve to further help organizations determine if an incident is in fact, 'material'.

(ISC)^2 understands and appreciates that a broad definition is designed to afford companies the flexibility to determine the magnitude of a cybersecurity incident and obtain pertinent details surrounding the incident prior to the start of the 72-hour clock. However, (ISC)^2 contends that a more specific definition that articulates the standard of materiality, would as help to curb confusion and doubts as to the relevance of an incident.

QUESTION 4. WE ARE PROPOSING TO REQUIRE REGISTRANTS TO FILE AN ITEM 1.05 FORM 8-K WITHIN FOUR BUSINESS DAYS AFTER THE REGISTRANT DETERMINES THAT IT HAS EXPERIENCED A MATERIAL CYBERSECURITY INCIDENT. WOULD THE PROPOSED FOUR-BUSINESS DAY FILING DEADLINE PROVIDE SUFFICIENT TIME FOR REGISTRANTS TO PREPARE THE DISCLOSURES THAT WOULD BE REQUIRED UNDER PROPOSED ITEM 1.05? SHOULD WE MODIFY THE TIMEFRAME IN WHICH A REGISTRANT MUST FILE A FORM 8-K UNDER PROPOSED ITEM 1.05? IF SO, WHAT TIMEFRAME WOULD BE MORE APPROPRIATE FOR MAKING THESE DISCLOSURES?

RESPONSE: Disclosure and incident reporting of cybersecurity incidents is a positive step forward. Disclosure of such events will be useful for the public to understand the nature, scope and ramifications of material cyber incidents and the effect those incidents can and will have on both investors and customers.

(ISC)^2 believes, however, that premature incident disclosure based merely on the suspicion of a breach, without a complete and adequate assessment of the incident, may be detrimental to both businesses and services supplied by that business. While (ISC)^2 contends that reporting of material cyber security incidents is both positive for the public and for data protection, (ISC)^2 is concerned that companies suffer unnecessarily on account of notifying based on an incident which is later determined to not be material.

(ISC)^2 believes that the proposed timeframe of 72 hours following an incident being determined as 'material' is sufficient time for an initial incident disclosure assuming a business has prepared responses to SEC disclosure requirements ahead of time and has adequate cybersecurity resources in place. This timeframe is consistent with, or more generous than, similar regimes in foreign jurisdictions. In Australia, the Australian Prudential Regulation Authority (APRA) has allotted for 72 hours to report an incident under APRA CPS-234.[3] Similarly, the European Union has also set forth a 72-hour disclosure period under the GDPR[4], as has the UK under its domestic implementation of the GDPR rules.[5] In the United States, the *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, enacted by Congress on March 10, 2022, requires critical infrastructure entities to report cyber incidents to the Department of

[3] APRA CITATION
[4] GDPR CITATION
[5] UK GDPR Citation

Homeland Security's (**DHS**) Cybersecurity and Infrastructure Security Agency (**CISA**) within 72 hours of an incident being discovered and to report ransom payments in response to ransomware attacks within 24 hours.[6]

QUESTION 18. ARE THE PROPOSED DEFINITIONS OF THE TERMS "CYBERSECURITY INCIDENT," "CYBERSECURITY THREAT," AND "INFORMATION SYSTEMS," IN ITEM 106(A) APPROPRIATE OR SHOULD THEY BE REVISED? ARE THERE OTHER TERMS USED IN THE PROPOSED AMENDMENTS THAT WE SHOULD DEFINE?

RESPONSE: (ISC)[2] proposes the following definitions to the terms sought under this question:

- 'Cybersecurity incident' should be defined as 'an unauthorized occurrence on or conducted through [an adviser's or a fund's] information systems that jeopardizes the confidentiality, integrity, or availability of [an adviser's or a fund's] information systems or any [adviser or fund] information residing therein.' See proposed rules 206(4)-9 and 38a-2. This proposed term is derived from the 44 U.S.C. 3552, which is incorporated into PPD-41 (defining 'cyber incident') and included in the NIST Glossary (defining 'incident').[7] (ISC)[2] believes this term is sufficiently understood and broad enough to encompass incidents that could adversely affect an adviser's or fund's information systems or information residing therein, such as gaining access without authorization or by exceeding authorized access to such systems and information that could lead, for example, to the modification or destruction of systems and information.
- 'Cybersecurity Threat' should be defined as 'any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of [an adviser's or a fund's] information systems or any information residing therein.'[8]
- 'Information System' should be defined as 'information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of a registrant's information to maintain or support the registrant's operations.'

QUESTION 21. AS PROPOSED, A REGISTRANT THAT HAS NOT ESTABLISHED ANY CYBERSECURITY POLICIES OR PROCEDURES WOULD NOT HAVE TO EXPLICITLY STATE THAT THIS IS THE CASE. IF APPLICABLE, SHOULD A REGISTRANT HAVE TO EXPLICITLY STATE THAT IT HAS NOT ESTABLISHED ANY CYBERSECURITY POLICIES AND PROCEDURES?

(ISC)[2] believes that any organization that employs people and provides services should have security policies and procedures in place. Regardless of these policies being provided and maintained internally or externally, policies should be mandatory to secure confidence.

A lack of policies and procedures undermines cyber defenses and leaves all stored and valuable systems vulnerable to attack. The cyber protocols and practices of a business should consider people, process and technology. All three are necessary for a successful practice. Relying too heavily on any one of these could prove detrimental to the business and the information and systems being protected. SEC-governed organizations should be mandated to have formal policies and procedures related to cyber (ISMS).

[6] *Cyber Incident Reporting for Critical Infrastructure Act of 2022 – full citation*

[7]

[8]

QUESTION 22. ARE THERE CONCERNS THAT CERTAIN DISCLOSURES REQUIRED UNDER ITEM 106 WOULD HAVE THE POTENTIAL EFFECT OF UNDERMINING A REGISTRANT'S CYBERSECURITY DEFENSE EFFORTS OR HAVE OTHER POTENTIALLY ADVERSE EFFECTS BY HIGHLIGHTING A REGISTRANT'S LACK OF POLICIES AND PROCEDURES RELATED TO CYBERSECURITY? IF SO, HOW SHOULD WE ADDRESS THESE CONCERNS WHILE BALANCING INVESTOR NEED FOR A SUFFICIENT DESCRIPTION OF A REGISTRANT'S POLICIES AND PROCEDURES FOR PURPOSES OF THEIR INVESTMENT DECISIONS?

$(ISC)^2$ recognizes that a balance needs to be found to achieve the goals of transparency and disclosure to allow investors and customers to make informed decisions, and the need for a business to protect their assets, interests and viability. Investing in cybersecurity practices and protocols from a people, process and technology perspective is essential for a business to successfully maintain secure data and systems, maintain the trust of the public and the interests of stakeholders and regulators alike.

Disclosure of non-essential information could lead to social engineering attacks, exploitation of vulnerabilities and additional potential harm to organizations and their shareholders. As such, any notifications made by affected organizations should be made in simple language following industry-accepted verbiage. Notifications should avoid detailing any specific aspects of an organization's information systems. For example, vendor technology used for cyber defense should not be listed in a notification to ensure that a cybercriminal employing social engineering techniques does not further target an organization with vendor-specific vulnerabilities.

$(ISC)^2$ also recognizes that not disclosing enough information could in fact prove detrimental to the reputation of the business and public confidence in the long term.

In addressing both investor and registrant concerns around best practice, preventative cybersecurity courses of action, $(ISC)^2$ contends that an organization's cybersecurity posture is entirely reliant on three essential pillars to ensure achieving good outcomes:

- The first pillar is an understanding that **PEOPLE** are the most essential ingredient in any successful cyber security strategy. This involves ensuring that people are aware of the risks, appreciate how those risks can impact their day to day lives and take proactive steps to prevent those risks from eventuating. This involves ensuring that professionals tasked with protecting the information assets of organisations and government are competent, skilled and certified in being able to do so, which is a significant element of what $(ISC)^2$ as an organisation seeks to achieve. This also involves ensuring that these people have access to relevant resources, training and skills that help to provide timely information in an industry that changes by the second.
- The second pillar is the understanding that **PROCESS** needs to exist when seeking to implement strong cyber security measures. Many of the items listed within the terms of reference for this Inquiry relate to process. The adoption of industry standards for the management of information security systems is critical. Many of the recommendations in the Submission discuss this pillar. However, it is vital to emphasise the point that without the **PEOPLE** in an organisation possessing the right set of knowledge, skills, experience and mindset, any attempt to create processes that minimise the risk will be flawed from the outset. We know this to be self-evident.

Consider, for example, mature industries such as aviation where there is no question that best practice dictates that the people working in the sector are competent, skilled and accredited.

- Finally, the third pillar is **TECHNOLOGY**. We all know that this is a high-tech sector. However, (ISC)2 strongly emphasises that the technology functioning as is intended is entirely dependent on the fact that **PEOPLE** are duly trained, skilled and accredited to deploy, manage and maintain that technology to begin with.

QUESTION 26. WOULD PROPOSED ITEM 407(J) DISCLOSURE PROVIDE INFORMATION THAT INVESTORS WOULD FIND USEFUL? SHOULD IT BE MODIFIED IN ANY WAY?

(ISC)² supports proposed item 407(j) and forms the opinion that investors would find it useful. The proposed item does not impose any additional obligations on the directors. Strategically, proposed item 407(j) could prove beneficial as it demonstrates commitment to cybersecurity which would elevate confidence in the organization with the public and other entities.

QUESTION 30. AS PROPOSED, ITEM 407(J)(1) INCLUDES A NON-EXCLUSIVE LIST OF CRITERIA THAT A COMPANY SHOULD CONSIDER IN DETERMINING WHETHER A DIRECTOR HAS EXPERTISE IN CYBERSECURITY. ARE THESE FACTORS FOR REGISTRANTS TO CONSIDER USEFUL IN DETERMINING CYBERSECURITY EXPERTISE? SHOULD THE LIST BE REVISED, ELIMINATED, OR SUPPLEMENTED?

(ISC)^2 supports the requirement that corporate officeholders, including directors, demonstrate a level of expertise in cybersecurity commensurate with the organizational risk that cybersecurity presents in the digital era. Information risk represents a set of risks that holds the same level of importance in terms of potential impact as financial risk, human risk and other major organizational risks. As such, information security requires a similar level of scrutiny and controls at a board level.

(ISC)^2 does not contend that all corporate officeholders should be required to become fully accredited cybersecurity professionals. However, (ISC)^2 does contend that a nominated director who is tasked with information security responsibilities for the organization should be duly accredited and certified as a cybersecurity professional. (ISC)^2 strongly contends that such a director, nominated to hold responsibility for information security should attain and hold a relevant ANSI / ISO / IEC 17024 accredited certification in cybersecurity to adequately demonstrate the requisite levels of expertise in the field. Such a scheme already exists for the US government - the US Department of Defense (DoD) 8570.01M lists a pre-defined list of ANSI / ISO / IEC 17024 valid cybersecurity certifications which must be held by all information assurance professionals pursuant to their level of responsibilities and roles. All nine (ISC)^2 certifications meet the requirements for eligibility for both the DoD 8140.01 and DoD 8570.01-M at various levels of work roles and responsibilities.

QUESTION 34. AS PROPOSED, ITEM 407(J) DOES NOT INCLUDE A DEFINITION OF THE TERM "EXPERTISE" IN THE CONTEXT OF CYBERSECURITY? SHOULD ITEM 407(J) DEFINE THE TERM "EXPERTISE"? IF SO, HOW SHOULD WE DEFINE THE TERM?

Yes. (ISC)² believes that the term "expertise" should be defined. (ISC)² proposes the definition include or be wholly defined as "a person who demonstrates advanced or expert skill or knowledge within cybersecurity and who has the ability to perform a task, function or role up to a set of prescribed standards."
(ISC)² supports the requirement that corporate officeholders, including directors, demonstrate a level of competence in cybersecurity commensurate with the organizational risk that cybersecurity presents in the digital era.

(ISC)² does not believe all corporate officeholders should be required to become fully accredited cybersecurity professionals. However, (ISC)² contends that a director(s) who is tasked with information security responsibilities for the organization should be duly accredited and certified as a cybersecurity professional

(ISC)² strongly contends that such a director, nominated to hold responsibility for information security should attain and hold a relevant ANSI / ISO / IEC 17024 accredited certification in cybersecurity in order to adequately demonstrate the requisite levels of competence in the field such as the Certified Information Systems Security Profession (CISSP). A CISSP certification demonstrates the individual can effectively design, implement and manage a best-in-class cybersecurity program.

Such a scheme already exists for the US government - the US Department of Defense (DoD) 8570.01M lists a pre-defined list of ANSI / ISO / IEC 17024 valid cybersecurity certifications which must be held by all information assurance professionals pursuant to their level of responsibilities and roles. All nine (ISC)2 certifications meet the requirements for eligibility for both the DoD 8140.01 and DoD 8570.01-M at various levels of work roles and responsibilities. 11 of the 14 work roles defined in DoDD 8140.01 and DoD 8570.01-M.

QUESTION 42. WOULD THE PROPOSED CYBERSECURITY INCIDENT DISCLOSURE PROVIDE ENOUGH INFORMATION FOR INVESTORS TO ASSESS THE IMPACT OF A CYBERSECURITY INCIDENT IN MAKING AN INVESTMENT DECISION? BECAUSE THE PROPOSED INCIDENT DISCLOSURE WOULD NOT REQUIRE QUANTIFICATION OF AN INCIDENT'S IMPACT, WOULD THE LACK OF QUANTIFICATION CREATE ANY UNCERTAINTY FOR INVESTORS WHICH MAY CAUSE THEM TO UNDER OR OVERREACT TO THE DISCLOSURE? WOULD INVESTORS BENEFIT MORE IF REGISTRANTS WERE TO PROVIDE THE DISCLOSURE AFTER THE INCIDENT'S IMPACT IS QUANTIFIED OR CAN BE REASONABLY ESTIMATED? IF SO, WHAT METRICS SHOULD BE DISCLOSED TO HELP INVESTORS UNDERSTAND THE IMPACT?

(ISC)² believes that incident disclosure is beneficial to members of the public to understand when breaches are material from both an investor and customer perspective. (ISC)² believes that information sharing contributes to better understanding of the impacts of a breach for a business. Additionally, it helps inform investors and the public.

(ISC)² holds firm the view that it is critical to demonstrate competent cybersecurity policies and practices are in place. However, (ISC)² contends that it would be unwise and counterproductive to the purposes of the proposed SEC goals to significantly penalize businesses based on minor timeline infractions.

(ISC)² firmly believes recognition of demonstrated cybersecurity expertise is an important part of cybersecurity, defining cybersecurity competence and encouraging uniform and informed cybersecurity policies, procedures and disclosures. (ISC)² welcomes the opportunity to support and help define the parameters for rules and requirements on this issue based on our vast expertise and market experience. (ISC)² appreciates the opportunity to submit comments to the SEC and would welcome an offer to further support and assist on this matter. (ISC)² looks forward to the decision of the SEC regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.