COMMUNICATIONS OF CYBERSECURITY INCIDENTS: COMPARISON BETWEEN SEC RELEASE 33-10459 AND THE AICPA'S CYBERSECURITY RISK MANAGEMENT FRAMEWORK

In 2018, the SEC issued Release Nos. 33-10459 and 34-82746, Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Statement), to assist public companies in preparing disclosures about cybersecurity risks and incidents. While some of the matters described in the Statement apply only to public companies, others apply to all companies that operate in the digital world. The purpose of this paper is to compare the SEC's recommendations in the Statement to the AICPA's Cybersecurity Risk Management Framework, which was issued in 2017.

Matters Addressed by the Statement

In the Statement, the SEC acknowledged that "cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries." To manage those risks and threats, the Statement stresses the importance of:

- Maintaining comprehensive policies and procedures related to cybersecurity risks and incidents.
- Establishing and maintaining appropriate and effective disclosure controls and procedures that enable companies to make accurate and timely disclosures of material cybersecurity events. The Statement also articulates the belief that the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons are informed about the cybersecurity risks and incidents that companies face or are likely to face.

Finally, the Statement reminds companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the federal securities laws and of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.

AICPA's Cybersecurity Risk Management Framework

In April 2017, the AICPA issued its cybersecurity reporting Framework(Framework) designed to serve as a common language to enable organizations of all sizes and in all industries to evaluate their cybersecurity controls and communicate to interested parties (both internal and external) information about their cybersecurity risk and the ways in which they manage them. The Framework may also be used by CPAs engaged to provide an opinion on such information, thereby increasing the confidence in which users (both internal and external) can place on the cybersecurity information disclosed.

To support the Framework, the AICPA issued two sets of criteria:

- *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (description criteria), which may be used by companies to describe the company's cybersecurity risk management program.

- *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (trust services criteria), which may be used by a company to evaluate the suitability of design and operating effectiveness of controls within the company's cybersecurity risk management program.

Both sets of criteria describe the objectives of effective cybersecurity processes and controls that companies should design and implement to have a robust cybersecurity risk management program. Like the Statement, the Framework supports the need for companies to have robust cybersecurity risk management program to manage cybersecurity risks unique to their organizations.

The trust services criteria also include several criteria relevant to the cybersecurity processes and controls companies should establish and maintain to enable them to effectively communicate material cybersecurity events to key shareholders, as required by the Statement. Those criteria include the following:

- CC2.2, *The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.* Points of focus for this criterion address how relevant internal control information is communicated on a timely basis to employees, management and the board of directors.
- CC2.3, *The entity communicates with external parties regarding matters affecting the functioning of internal control.* Points of focus for this criterion address the processes and controls that are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.
- CC7.4, *The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.* Points of focus for this criterion address the protocols for communicating security incidents and actions taken to affected third parties.
- CC7.5, *The entity identifies, develops, and implements activities to recover from identified security incidents.* Points of focus for this criterion address communications that should be made to management and others as appropriate (internal and external) about the nature of the security incident, recovery actions taken, and activities required for the prevention of future security incidents.

In addition, the description criteria contain a criterion (DC6) that discusses the need to disclose, in the cybersecurity report, information about identified cybersecurity incidents.

Like the Statement, the trust services criteria also recognize that, for most effective cybersecurity risk management programs, senior management and the board of directors have established effective oversight over the processes and controls within the program. Such oversight includes, among other things, setting the "tone at the top" within the company with respect to the importance of cybersecurity matters. It also includes assessing identified deficiencies, monitoring the results of in-house evaluations of the effectiveness of cybersecurity controls, and overseeing corrective actions taken to remedy them.

Because the Framework is designed to be used by both public and private organizations, it does not address the need for directors, officers, and other corporate insiders to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents. That requirement, as set forth in the Statement, applies only to public companies.