As of 9/16/25

The Walt Disney Company

CYBERSECURITY

Topic Summary

We have implemented processes for assessing, identifying and managing material risks from cybersecurity threats as part of our overall risk management program. Our cybersecurity program is informed by the National Institute of Standards and Technology Cybersecurity Framework as well as other globally recognized standards. We use a layered defense model, incorporating a wide range of technologies and practices in an effort to prevent, detect and mitigate threats. These measures include intrusion detection and prevention systems, multi-factor authentication, encryption and endpoint protection tools. We also implement threat detection and response solutions. To address emerging threats, we employ automated monitoring, vulnerability scans and patch management processes. Regular assessments, such as penetration tests, security audits and table-top exercises, are conducted to identify vulnerabilities and promote incident response and risk mitigation. We also provide privacy and information security trainings for our employees on a recurring basis. From time to time, we engage assessors, consultants and other third parties to assist with assessing, identifying and managing cybersecurity risks, including assisting us to conduct some of the foregoing assessments. Our cybersecurity risk management processes also are informed by intelligence received from recognized cybersecurity industry experts and other third-party sources, and as appropriate we engage outside counsel to advise on regulatory compliance and other cybersecurity risk management efforts.

In addition, we have processes designed to oversee and identify cybersecurity risks associated with our use of third-party service providers. Where appropriate based on the data and intellectual property to which these providers are reasonably expected to have access, we conduct security assessments and due diligence reviews of third-party systems for compliance with our security standards, and we include data protection language in our agreements with these third parties.

Further, as part of our cybersecurity risk management processes, we maintain an incident response plan (IRP) that establishes a set of procedures for reporting and handling cybersecurity events. The IRP delegates to an internal incident response team the initial assessment, investigation and remediation of the event and includes, among other procedures, guidelines for escalation to senior management and engagement with law enforcement. In certain instances, events are escalated to the Cybersecurity Incident Disclosure Subcommittee, which is a subcommittee of the Company's Risk Management Committee (RMC) (discussed further below) and is responsible for, among other things, the accurate and timely disclosure of material cybersecurity incidents under the federal securities laws, including making the materiality determination and approving related securities disclosures.

Governance

The Company’s Board of Directors has delegated to the Audit Committee oversight responsibility for information technology risks, including cybersecurity and data security risks and mitigation strategies. The Audit Committee at least annually receives reports from the Senior Vice President, Chief Information Security Officer (CISO) concerning the Company’s cybersecurity and data security risks, including ongoing efforts to prevent, detect, monitor, remediate and manage such cybersecurity threats, the threat environment, incident updates and emerging cybersecurity practices and technologies. The Chair of the Audit Committee reports on its discussion, including concerning cybersecurity matters, to the full Board. In addition, from time to time, senior management briefs the Audit Committee, the Audit Committee Chair and the Board on cybersecurity matters potentially of interest, including cybersecurity events, regulatory disclosures and regulatory trends.

Day-to-day management of our information security strategy and operations is currently the responsibility of our CISO, who reports to our Chief Information and Data Officer, and our Chief Information and Data Officer reports to our Chief Financial Officer.

In addition, the Company’s RMC, a management level committee that includes, among others, the Chief Financial Officer and Chief Legal and Compliance Officer, oversees and supports the Company’s ongoing efforts to identify, assess and prioritize, manage and monitor the Company’s enterprise risks, including risks related to privacy and cybersecurity, and periodically reports certain discussions to the Company’s Chief Executive Officer and Audit Committee. The RMC’s Cybersecurity Incident Disclosure Subcommittee, whose members include the members of the RMC, the CISO and lead securities counsel, is tasked with assessing significant events for materiality, related timely and accurate disclosure under the securities laws and, as appropriate, escalating such events to the Audit Committee and the Board of Directors.