Celanese

Cyber and Information Security Statement

Maintaining security of information and mitigating against the risk of cyber threats are key to protecting our proprietary information, safeguarding information about our employees, customers and suppliers and preserving the trust of parties with whom we do business. While our specific measures regularly evolve, this statement provides an overview of certain elements of our current information security risk mitigation efforts.

TRAINING AND EDUCATION: Our "Keep Cyber Safe" global cybersecurity awareness training program includes 12 modules covering key risk topics such as laptop security, phishing, unsecured networks, and malware. October is Cybersecurity Awareness Month at Celanese, and in 2021, we launched the next chapter in our cybersecurity awareness program with a new comprehensive cybersecurity awareness course in our learning management system assigned to all employees with computers. Annually, our global code of conduct training administered to all employees reinforces key information security concepts and policies. This course covers topics such as identifying workplace cyber hazards and attacks. We also have an ongoing rigorous phishing awareness program that regularly is administered to all employees with computers.

THIRD-PARTY ASSESSMENT AND OTHER KEY CONTROLS: The Celanese cybersecurity program is designed to align to National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) and ISO 27001 standards that are assessed annually by a third party. Through an independent registered public accounting firm and internal audit, we validate the information security internal controls over financial reporting as part of Sarbanes-Oxley Act compliance. Celanese plans on obtaining ISO 27001 certification as part of the cybersecurity strategic plan. The Company also prepares security vulnerability assessments as required by laws and regulations applicable to chemical manufacturing sites.

We perform information security risk assessments of third parties we do business with and we have a formal Incident Response Plan which including measures to protect third-party data from unauthorized access or disclosure.

OVERSIGHT: Our information security efforts are led by our Chief Information Security Officer and overseen by our Chief Information Officer, the rest of our Executive Leadership Team, our Board Committees, and our Board of Directors. The Board and its Environmental, Health, Safety, Quality and Public Policy Committee receive regular and at least annual updates that include information about cybersecurity governance processes, the status of projects to strengthen internal cybersecurity, and the results of security breach simulations. To our knowledge, as of March 31, 2024, we have not experienced any material information security breaches, incurred material expenses or been assessed any fines from data protection authorities in the past three years.

05.17.24