STATEMENT ON APPROACH AND RESULTS REGARDING CYBERSECURITY AT CRANE

Tone at the Top:

Our approach to cybersecurity begins with our desire to maintain strong governance and controls to effectively manage and reduce security risks. Security begins with our "tone at the top", where Company leadership consistently communicates the requirements for vigilance and compliance throughout the organization, and then leads by example. The cybersecurity program is led by Crane's Chief Information Security Officer, who provides periodic updates to the Audit Committee of our Board of Directors, annual updates to the full Board of Directors, and regular reports to the Executive Management Team about the program, including information about cyber risk management governance and the status of ongoing efforts to strengthen cybersecurity effectiveness. At Crane, our entire board of directors ultimately is responsible for overseeing management's risk assessment and risk management processes designed to monitor and mitigate information security risks, including cyber risks. Our Company maintains cyber risk and related insurance policies as a measure of added protection.

Our Team and Capabilities:

Our cybersecurity program is staffed by a team of highly skilled cybersecurity professionals, including 28 dedicated internal cybersecurity resources. Six members of the security team currently have Certified Information Systems Security Professional (CISSP) credentials, five members hold one or more Global Information Assurance Certification (GIAC)/The Sans Institute (SANS) cybersecurity certificates, and in total the team has over 76 security and network certifications. Our response team members are located in various global locations to ensure 24/7 monitoring and response capabilities and are backed by a 24/7 Managed Security Services Provider (MSSP) who monitors cybersecurity alerts. The program incorporates industry standard frameworks, policies and practices designed to protect the privacy and security of our sensitive information, backed by a suite of best-in-breed security technologies and tools to implement and automate security protections for our networks, employees, and customers.

Our Program and Results:

Specifically, we utilize a risk-based, multi-layered information security approach following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the Center for Internet Security (CIS) critical security controls. We have adopted and implemented an approach to identify and mitigate information security risks that we believe is commercially reasonable for manufacturing companies of our size and scope and commensurate to the risks we face. During the past 5 years, no attempted cyber-attack or other attempted intrusion on our information technology networks has resulted in a material adverse impact on our operations or financial results, in any penalties or settlements, or in the loss or exfiltration of Company data. In the event an attack or other intrusion were to be successful, we have a response team of internal and external resources engaged and prepared to respond.

Education and Awareness:

We educate and share best practices globally with our employees to raise awareness of cybersecurity threats. As part of our internal training process, we maintain an annual training for all employees on cybersecurity standards, as well provide monthly trainings on how to recognize and properly respond to phishing, social engineering schemes and other cyber threats. Crane uses advanced systems to block and analyze all email for threats, as well as equip our employees with an intuitive mechanism to easily report suspicious emails which are analyzed by our security systems and dedicated incident response team. Monthly "test" phishing emails are sent to our associates. Any failures trigger a retraining exercise if not properly reported and a monthly training vignette on cybersecurity awareness. To round out our robust awareness program, we have specific and regular training for our IT professionals, and we regularly engage independent third parties to test our information security processes and systems as part of our overall enterprise risk management program.

January 2023