STATEMENT ON APPROACH AND RESULTS REGARDING CYBERSECURITY AT CRANE

Governance and Approach

Our cybersecurity program is led by Crane Company's Chief Information Security Officer, who regularly reports to our executive team about our program, including a review of cyber threat trends, our information security organization and staffing, and the status of ongoing efforts and investments to strengthen our cybersecurity defenses. We utilize a risk-based, multi-layered information security framework 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 a systematic approach measuring ourselves against this multi-layered framework which we formally review on a quarterly basis (with more frequent updates as necessary) to identify and mitigate security risks that we believe are commercially reasonable for manufacturing companies of our size and scope and commensurate with the risks we face. In addition, we provide a minimum of two formal program updates each year to the Audit Committee.

Our Team and Capabilities

Our cybersecurity program is staffed by a team of skilled cybersecurity professionals, including approximately 20 dedicated internal cybersecurity resources. Three members of the security team currently have Certified Information Systems Security Professional (CISSP) credentials, many hold one or more Global Information Assurance Certification (GIAC)/The Sans Institute (SANS) cybersecurity certificates, and in total the team has over 70 security and network certifications. Our response team members are 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.

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 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. The Company 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.

Our Program Results

Crane Company was separated from its parent company, Crane Holdings, on April 3, 2023, and since the separation and during the preceding 5 years as Crane Holdings, 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 material or sensitive Company data. Crane has not been materially impacted by any third-party information security breach, but recognizes the inherent cyber risks associated with relying on third-party vendors such as cloud service providers, software vendors, data processors, and IT service providers with access to company information, systems, or processes. Crane is committed to managing these risks responsibly and transparently and has an active process in place to assess and reduce that risk, including performing due diligence on third-party vendors before onboarding and evaluation and

assessing their cybersecurity policies. 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. The Company maintains cyber risk and related insurance policies as a measure of added protection.

June 2025