Cybersecurity

Ensuring the protection of our information and systems and that of our customers and other stakeholders is of critical importance. Our security protocols and practices are designed to protect sensitive information and systems.

Our cybersecurity program is designed to protect and preserve the confidentiality, integrity and continued availability of all information that we own or is in our care. We apply stringent cybersecurity and data privacy protocols and practices throughout our systems. Our program is based on the U.S. National Institute for Standards and Technology (NIST) standards, and Woodward has successfully completed the Cybersecurity Maturity Model Certification (CMMC) that requires formal third-party audits of defense industrial base (DIB) contractor cybersecurity practices.

Our cybersecurity program includes:

- a cyber incident response plan that provides controls and procedures for timely and accurate reporting of any material cybersecurity incident(s);
- annual security training for employees, including periodic phishing testing to ensure our employees remain vigilant and compliant with our expectations;
- easy-to-use tools for employees to report potential phishing emails; and
- periodic testing of cybersecurity posture using third parties.

The Audit Committee of our Board of Directors has responsibility for the oversight of risk management activities related to cybersecurity and other information security and technology risks. Our Vice President of Information Technology leads our cybersecurity program and provides the Audit Committee a strategic review of cybersecurity matters and risk management action plans at least annually, as well as periodic updates as required. Periodic updates may include, among other topics, results of exercises performed by advisors that provide an independent assessment of our cybersecurity program and internal response preparedness.

In the last three years, Woodward has not experienced any material information security breaches, and there were no expenses or fines related to breach penalties and settlements. Nonetheless, we maintain insurance covering certain costs that we may incur in connection with cybersecurity incidents.