CYBERSECURITY AND INFORMATION SECURITY STATEMENT

We rely on internal and third-party information technology and computer control systems in many aspects of our business. In addition, our business involves the use, storage, and transmission of information about our employees, customers, and suppliers. Information security, including the protection from cyber threats of our systems and proprietary information and information about our employees, customers, and suppliers, is critical to us.

CF Industries' cybersecurity strategy prioritizes detection, analysis, and response to known, anticipated or unexpected cyber threats, effective management of cyber risks, and resilience against cyber incidents. CF Industries maintains a formal cybersecurity program structured around the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), a voluntary framework created by industry and the US government to promote the protection of our infrastructure from cybersecurity risks. CF contracts with an external auditing firm annually to assess CF's cyber security controls relative to industry peers using the NIST Cyber Security Framework. CF Industries also has a third-party risk management program that assesses risks from vendors and suppliers.

This document provides an overview of our approach to cybersecurity and our program and practices to secure technology, systems and data aligned around the five functions of the NIST CSF:

Identify

- **Risk Governance and Oversight**

  Risk governance and risk management are embedded in CF's "Do It Right" culture. CF's Information Technology organization, led by CF's Chief Information Officer, is responsible for administration of the cybersecurity and information security framework and risk management. The governance model is achieved by the day-to-day activities of managers and their teams, supported by various working groups and committees.

  The Audit Committee of our Board of Directors provides oversight in connection with management's cybersecurity and information security efforts. The Audit Committee receives regular reports and updates on the efficacy of our cybersecurity and information framework and risk management at least quarterly and actively engages with our Chief Information Officer and other members of senior management who are tasked with monitoring cybersecurity risks. In addition, the Audit Committee receives periodic reports summarizing threat detection and mitigation plans, audits of internal controls, training and certification, and other cyber priorities and initiatives, as well as timely updates from senior leaders on material incidents relating to information systems security.

- **Information Security and Cybersecurity Policies and Standards**

  CF Industries maintains a comprehensive set of information security policies and standards to document the company's approach to comply with laws, rules, regulations, best practices, and management directives.

- **Asset Management**

  CF Industries maintains an asset management program to appropriately inventory, classify, and protect applications, data, and hardware.

Protect

- **Training and Awareness**

  CF Industries has an established and mature cybersecurity and information security awareness training program. Formal training on topics relating to the company's cybersecurity, data privacy and information security policies and procedures is mandatory at least annually for all employees and contractors with access to our network. Training is administered and tracked through online learning modules. Training generally includes how to escalate suspicious activities including phishing, viruses, spams, insider threats, suspect human behaviors or safety issues.

- **Identity and Access Management**

  CF Industries has implemented controls to identify, authorize, authenticate, and manage individuals' access to the organization's systems and information assets. Improper or illegitimate access or use of the company's information system resources or violation of the company's information security policies and procedures is subject to disciplinary action.

- **Infrastructure Security**

  CF Industries protects its infrastructure through a control framework which includes vulnerability testing, system hardening, and malware protection.

- **Data Protection and Data Privacy**

  CF Industries has implemented policies designed to safeguard company, employee, customer, and supplier information, which covers data classification, secure storage, handling and transmission, and destruction.

- **Physical Security**

  CF Industries has implemented physical access controls at all company facilities, including office spaces, manufacturing plants and distribution facilities, data centers, and storage facilities.

- **Vendor Security**

  Information security risk management is built into CF's vendor management process, which covers vendor selection, onboarding, performance monitoring, and risk management.

Detect

- **Continuous Monitoring**

  CF Industries maintains detective controls at the network, endpoint, and application layers to detect anomalous activity that is potentially indicative of threat activity. We further implement continuous control monitoring to assess the adoption and performance of security controls.

- **Anomaly Detection**

  CF Industries ensures that security anomalies and events are detected quickly, and their potential impact is understood.

- **Enforcing Protective Measures**

  CF Industries tests and confirms all protective security measures to verify the effectiveness and coverage.

Respond

- **Security Incident Management**

  CF Industries' security incident management program enables effective detection and management of security threats and incidents that have a potential impact on the confidentiality, integrity, or availability of the company's information and technology environment, including notification to employees, customers and partners as required by applicable laws and regulations.

  CF Industries is not aware of any material incidents relating to CF Industries or third-party information systems security affecting the safety of our operations or ability to serve customers or significant breaches of personal information in the past three years. CF Industries has had no fines from data protection authorities in the past three years.

- **Response Planning**

  CF Industries incorporates coordinated response planning processes during and after any security incidents, which include managing communications and analyzing the effectiveness of response activities.

Recover

- **Business Continuity and Technology Resilience**

  CF Industries has a mature and comprehensive global Business Continuity Program which includes IT Disaster Recovery (BCP/DR). The program covers both business and technology resilience.

While information security measures will change over time and may differ across the range of CF's services, this document provides an overview of our security practices.

Please contact your CF Industries representative if you have any additional questions.

November 2023

Julie Scheck Freigang X: Julie Scheck Freigang
VP, Chief Information Officer

Khurram Anwar X: Khurram Anwar
Sr. Director, Cyber Security