Information Security Overview

In order to minimize the likelihood and impact of a cybersecurity incident we have deployed cyber security protections to protect ADI's networks, devices and data from external & internal threats. These protections are deployed in a risk-based program designed to also maintain compliance with current and evolving regulations such as GDPR or new reporting regulations issued by the various governments where we operate.

ADI's Enterprise Security program has been developed based on industry standards, including those published by International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST). Highlights of the ADI program includes:

- **Polices:** We have developed a comprehensive set of enterprise security policies and procedures to guide our protection strategy.
- **Program Elements:** ADI protects against threats by adopting all five elements of the NIST framework including:
    - Identifying critical assets and high-risk threats
    - Implementing cybersecurity detection with a 24x7x365 operations center
    - Implementing security controls and remediation practices
    - Having an Incident Response and Disaster Recovery capability
    - Evaluating our partners' cyber posture through the implementation of a Third-Party Risk Management program

  Risks identified by our cybersecurity program are analyzed to determine the potential impact on us and the likelihood of occurrence. Such risks are continuously monitored to ensure that the circumstances and severity of such risks have not changed. We evaluate our security program effectiveness by performing internal audits and periodic external audits by an independent information systems expert to determine both the adequacy of, and compliance with, controls and standards. We will continue integrating the Maxim and ADI programs over the upcoming 12-18 months.
- **Governance:** ADI's Board of Directors includes four members with cyber security expertise to assist the Board in its oversight of the Company's information security program. Senior leadership and Internal Audit regularly provide the Audit Committee with updates on the performance of our cyber program. At least annually, the Chief Information Officer, updates the full Board of Directors on information security matters and risk, including cybersecurity.
- **External Inputs:** ADI regularly conducts threat assessments and benchmarks best practices. Intel sharing is conducted with leading global security providers, the National Defense Information Sharing and Analysis Center as well as industry peers, which help all participating companies improve their cyber security programs.
- **Security Awareness & Training** is an important part of our overall program. We conduct regular workforce training to instruct our employees to identify cyber concerns and to take the appropriate action. We install and regularly update antivirus software on all company managed systems and workstations to detect and prevent malicious code from impacting our systems.

- **External Certification**: Cybersecurity Maturity Model Certification (CMMC) is a unified standard for the implementation of cybersecurity across an Enterprise that is designed to help protect sensitive unclassified information. It was developed by the US Department of Defense (DoD) and is expected to apply to the 300,000 companies supplying the DoD. The framework covers 110 controls specified in NIST 800-171. Analog Devices is pursuing its CMMC certification and is awaiting the publication of the final rule in the Federal Register**.**

Safeguarding our Products

Product Security Engineering: We have a dedicated product assurance team, who work closely with our development teams, to integrate risk and security best practices into our product development life cycle. For example, as the electronic content grows to support vehicle electrification, connectivity, and autonomy trends, the risk of a cybersecurity attack increases and threatens the functional safety of the vehicle and wellbeing of passengers. ISO 21434 is a new cybersecurity standard for automotive components for production road vehicle electrical and electronic systems that focuses on the end-to-end lifecycle for cybersecurity relevant E/E solutions from component to vehicle level. In October 2021, ADI achieved ISO/SAE 21434 certification for our engineering processes. ADI will be integrating Maxim products into this process in the upcoming 12-18 months.

Product Security Incident Response: ADI seeks to mitigate the risk associated with security vulnerabilities that may be discovered in our products. We aim to accomplish this objective by analyzing reported and discovered vulnerabilities and providing our customers with timely information, analysis, and guidance on appropriate mitigation. We have a robust Product Security Incident Response program to address product vulnerability investigation and response. Our global team manages the intake, investigation, remediation and any necessary disclosures of a security vulnerability reported to ADI. We are in the process of integrating Maxim products into this process.

Product Security Capabilities: Having confidence that data from an edge device is not manipulated or altered in any way is increasingly critical. Validating the integrity of the data at its source enables higher levels of trust, so that customers can be more confident in the decisions they make based on that data. ADI has developed components, solutions, and systems knowledge to protect the integrity of vital data at the device level. To protect the integrity of vital data, ADI’s cyber security defenses begin at the device level, where the data is born. By rooting identity in hardware, in tandem with cryptography, our security solutions enable a chain of trust from the edge to the cloud. Additional information on the cyber security solutions that ADI has developed to root an identity in hardware is available on our website [here].