In order to meet the stringent requirements of leading global security export companies, Kratos Israel is committed to upholding the highest industry standards. We dedicate substantial resources to ensure compliance with rigorous information security demands, positioning our products as among the most reputable in the market.

**Cyber Security Policy:** Our security protocols are aligned with the guidelines set forth by the local Ministry of Defense, which adhere to the Cybersecurity Maturity Model Certification (CMMC). Our production test area has no access to the internet.

Regular monitoring by the Ministry of Defense ensures compliance with physical security practices. Additionally, suppliers must sign nondisclosure agreements (NDAs) prior to accessing our systems or data.

**Chief Information Security Officer (CISO):** We have engaged the services of a Chief Information Security Officer (CISO) who acts as both a cybersecurity consultant and provides ongoing advisory support.

**Implemented Tools:** Our cybersecurity arsenal includes regularly updated firewalls, centrally managed endpoint protection, enterprise backup and recovery infrastructure, safe browsing, network/endpoint monitoring, host configuration management, and system patching.

**Recent Enhancements:** We continuously improve our security posture through system hardening, network segmentation and monitoring, and optimization of our Disaster Recovery (DR) strategy. Kratos also leverages industry-leading boundary protection devices and software in a layered security approach.