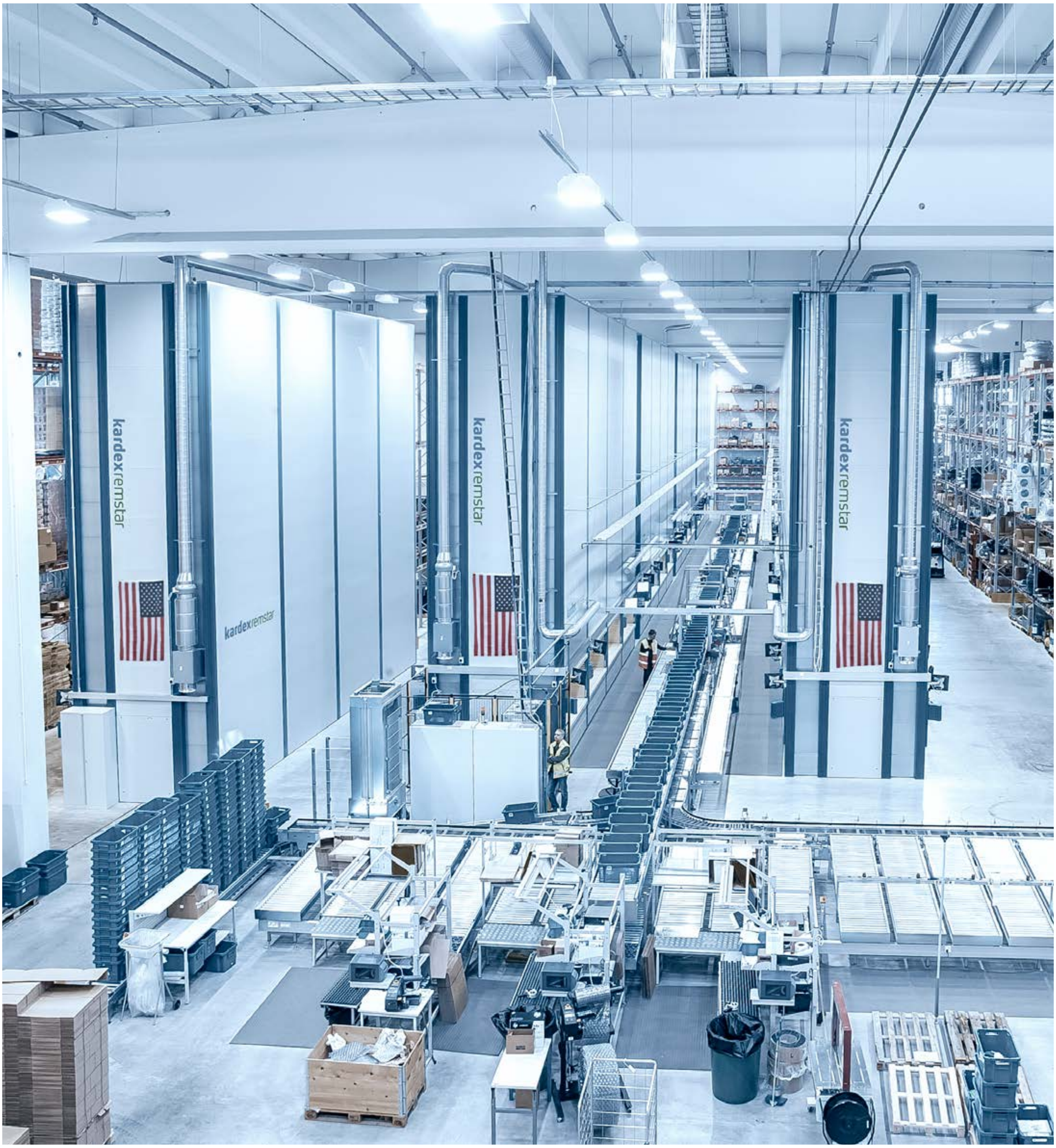
Factsheet

CMMC Compliance: Industry Leaders



kardexremstar

Kardex leads the way in CMMC compliance

Kardex is proud to announce compliance with the Department of Defense's rigorous Cybersecurity Maturity Model Certification (CMMC) program to safeguard the information that supports and enables our warfighters.

Our CMMC compliance brings a new level of assurance in cybersecurity for government customers partnering with Kardex. This ensures that we have achieved a standardized level of cybersecurity readiness, providing the government with increased confidence in the protection of sensitive information such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) data. The rigorous standards set by the CMMC program mean we are well-equipped to defend against cyber threats, ensuring that sensitive data remains secure in an increasingly digital and interconnected world.

Furthermore, our CMMC compliance ensures our consistent adherence to best practices while also complying with federal cybersecurity regulations. Our CMMC compliance significantly mitigates the risk of cyber incidents that could jeopardize national security or disrupt critical supply lines, thus maintaining a secure, reliable, and trustworthy defense infrastructure.

Want to learn more about getting ASRS approved for your base?
Click here to read our guide to the Military Buying Process.

Enhanced cybersecurity sssurance

Standardization and **compliance**

Risk mitigation and **Supply chain security**

Cybersecurity is a top priority for the DoD

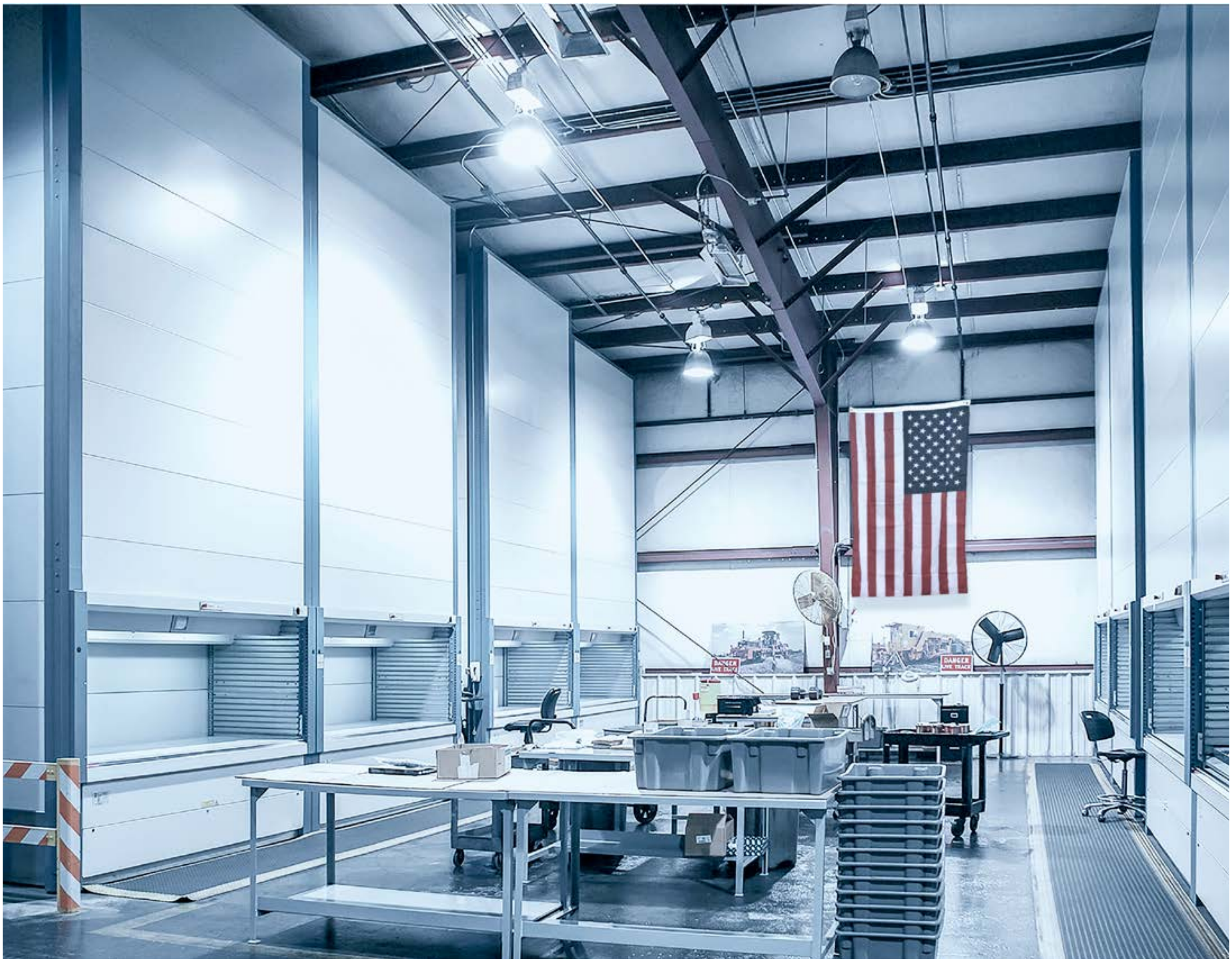
Due to the Defense Industrial Base (DIB) experiencing a rise in sophisticated cyber threats, the DoD has initiated the Cybersecurity Maturity Model Certification (CMMC) program. This initiative emphasizes the critical role of cybersecurity within the DIB to ensure the protection of American innovation and sensitive national security data, which are vital in supporting the capabilities of U.S. military personnel.

The Cybersecurity Maturity Model Certification (CMMC) program aligns with the DoD's security protocols for Defense Industrial Base (DIB) associates, ensuring the safeguarding of sensitive, unclassified data shared with contractors and subcontractors. It offers the DoD enhanced confidence in the cybersecurity measures of its contractors through:

A tiered Model
Mandating incremental cybersecurity standards for handling national security information, extending protections to subcontractors.

Assessment requirement
Enables the DoD to validate compliance with specified cybersecurity standards.

Implementation through contracts
Requires certain DoD contractors to meet specified CMMC levels to qualify for contract awards, ensuring controlled unclassified information is securely managed.



We’re here to help

Kardex’s commitment to CMMC compliance aligns with the DoD’s goal of fortifying the defense supply chain's resilience against cyber threats and ensuring the secure handling of sensitive unclassified information critical to national security.

Our sales representatives, who are U.S. military veterans themselves, possess the necessary experience and understanding to navigate these complex projects successfully. This dedicated group has the unique capability to navigate base protocols, working closely with you and other military personnel to bring these projects to fruition.

If you're considering ASRS for your base, our team is ready to assist. With extensive experience and a commitment to excellence, Kardex ensures a seamless integration of ASRS technology to meet your operational needs.

Contact specialist online