Certifications: CMMC 2.0 and NIST 800-171

DriveLock helps manufacturing companies fulfill standards mandated by the Federal Government.

Industrial companies seeking U.S. Department of Defense (DoD) contracts must demonstrate IT security controls for data exchange between themselves, DoD, and subcontractors. However, many industrial computers, such as programmable logic controllers (PLCs) and machines, still run outdated operating systems such as Win-XP, Win-7 and Linux without operating system updates. Under these circumstances, manufacturing companies cannot meet the NIST 800-171 or CMMC 2.0 cybersecurity requirements defined by Federal Government if they want to win these contracts. DriveLock can help companies meet these requirements with our Zero Trust Platform solutions, saving their business and allowing you to use their machine environment for many years to come.

CMMC certification

What is CMMC?

CMMC or Cybersecurity Maturity Model Certification, is a unified compliance framework designed to be implemented across the realm of industrial defense. It is designed with the aim of ensuring that US Department of Defense contractors adhere to federal guidelines on cybersecurity and other security controls, to protect data.

How is CMMC 1.0 evolving and developing into CMMC 2.x?

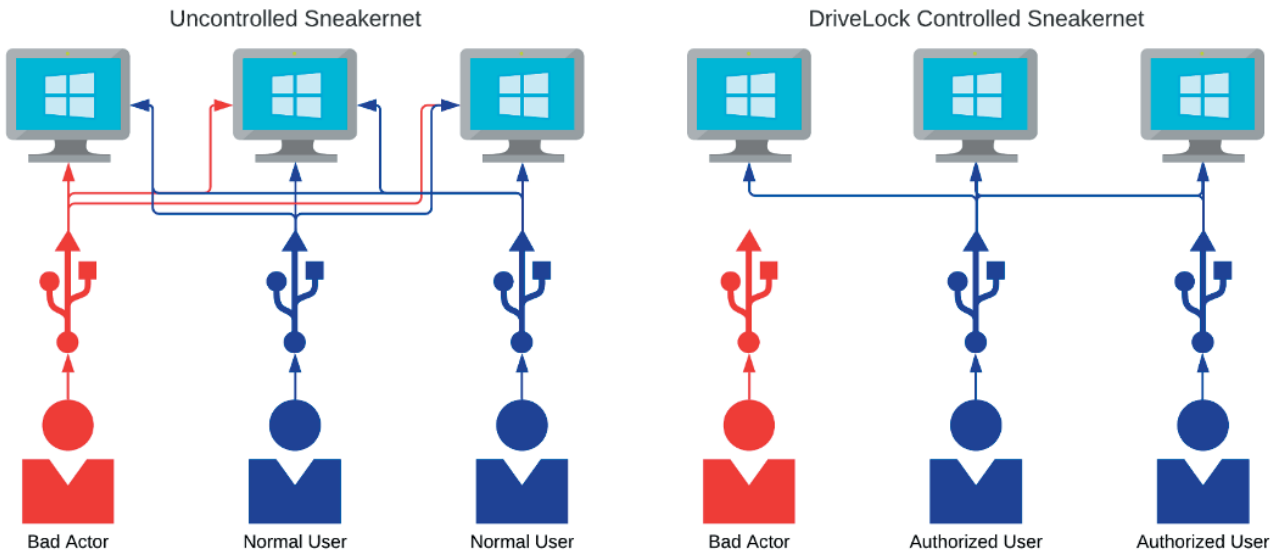
What does CMMC 2.0 look like at each level?

- **Level 1 Foundational:**
  - These 17 controls are taken from FAR 52.204-21
  - Certification can be achieved via annual self-assessments
- **Level 2 Advanced:**
  - These 110 CUI controls are taken from NIST SP 800-171
  - Path to certification is dependent on the form of acquisition (prioritized or non-prioritized)
- **Level 3 Expert:**
  - 110 CUI controls are taken from NIST SP 800-171 and roughly 35 controls are taken from NIST 800-172.

Certification Paths and CMMC 2.0

- **Level 1**
  - Can be achieved through an annual self-assessment.
- **Level 2 Prioritized Acquisitions**
  - A CMMC-AB approved C3PAO assessment must be conducted every 3 years.
- **Level 2 Non-Prioritized Acquisitions**
  - An OSC conducted annual self-assessment suffices.
- **Level 3 High-Priority Acquisitions**
  - A DoD-staffed (DIBCAC) assessment must be conducted every 3 years.

Controlling the flow of CUI for Removable Medias



DriveLock can provide access control at most layers and segments to provide a mature cybersecurity posture. In the case of removable medias, such as USB devices, DriveLock can effectively relegate each USB device to a user and a computer. This can greatly reduce the chances of insider threat and other forms of internally proliferated attacks.

Protecting CUI[1] on Removable Medias for CMMC

DriveLock can help establish formal processes and controls for handling USB and other removable media exceptions to protect CUI. In the case of USB devices, the following list demonstrates how controls can be met, but this list is not exhaustive:

- Enforces users to only be able to use the USB on specific machines within the company
- Allows the user to access data on the USB on company issued assets
- Allows logging and shadowing of files and file types going onto the USB device for better control, and the ability to build the chain of custody
- Encrypts all data on the USB device with FIPS compliant encryption to prevent CUI from being lost in the case of the device being lost
- Secure deletion allows CUI to be sanitized after exception periods expire for the USB device, making CUI arduously more difficult to restore
- Exceptions can be granted for users for set periods of time which is automatically enforced by the DriveLock agent

[1] CUI – Controlled Unclassified Information

NIST certification

What are the NIST 800 Series Documents?

These documents combine the extensive research conducted by NIST into efficient methods to optimize computer security policies, procedures, and guidelines. This is to align information technology systems for non-federal organizations to better security standards when handling CUI (Controlled Unclassified Information).

What is CUI?

Controlled Unclassified Information is any information that is owned or created by the federal government that is sensitive but not classified. This information generally can be used on unclassified networks by manufacturing organizations and others. Luckily, NIST's 800 series documents details effective ways to protect CUI, because although it is not classified, if a breach occurred it could result in national security events.

What are the different kinds of CUI?

+ CRITICAL INFRASTRUCTURE INFORMATION
+ DEFENSE INFORMATION
+ FINANCIAL INFORMATION
+ INTELLIGENCE INFORMATION
+ LEGAL INFORMATION
+ NATO RESTRICTED INFORMATION
+ NATO UNCLASSIFIED INFORMATION
+ PATENT INFORMATION
+ PROCUREMENT AND ACQUISITION INFORMATION

**Partial list*

Which 800 Series Documents are relevant?

Mainly when achieving NIST compliance, it is ultimately up to contract specifications to determine which documents are pertinent to internal controls. However, for CMMC version 1.0 the relevant documents are:

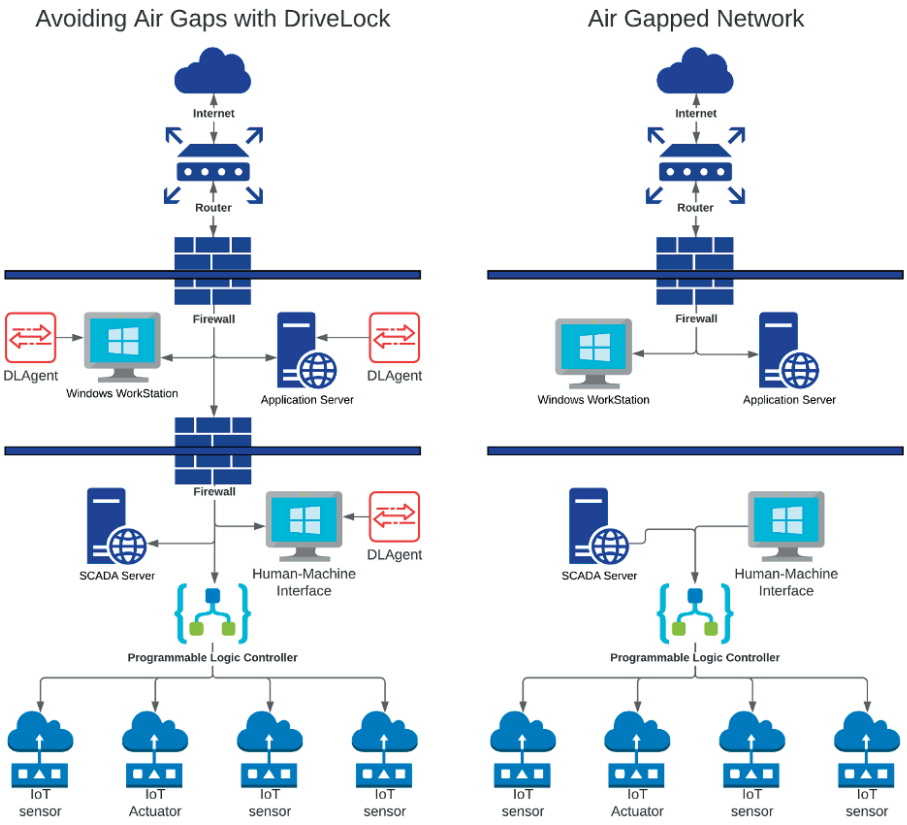
- NIST 800-171's CUI Controls
- NIST 800-171B
- NIST 800-53

800-171 Control Families DriveLock Covers

+ ACCESS CONTROL
+ AWARENESS AND TRAINING
+ AUDITING AND ACCOUNTABILITY
+ CONFIGURATION MANAGEMENT
+ IDENTIFICATION AND AUTHENTICATION
+ INCIDENT RESPONSE
+ MAINTENANCE
+ MEDIA PROTECTION
+ PERSONNEL SECURITY
+ PHYSICAL PROTECTION
+ RISK ASSESSMENT
+ SECURITY ASSESSMENT
+ SYSTEM COMMUNICATIONS PROTECTIONS
+ SYSTEM AND INFORMATION INTEGRITY

Legacy Assets – Air Gapping is Simply Not Enough

Commonly in manufacturing environments assets are air gapped due to their age or operating system. Although this can help prevent many different forms of network-based attacks, it takes away from the full functionality of these endpoints, as much of this comes from them being networked.



Many HMIs (Human-Machine Interfaces) tend to have legacy operating systems, which are open to many different security risks due to their age. This means that although they still serve their function, organizations are left to dealing with these risks in different fashions. The DriveLock tool can help implement different compensating measures and controls on these legacy assets so that their full-functionality can be used rather than relying on air-gapping. DriveLock supports most major Linux distributions, and back to Windows XP Service Pack 3. This can be helpful when determining what needs to be done to establish NIST 800-x compliance.