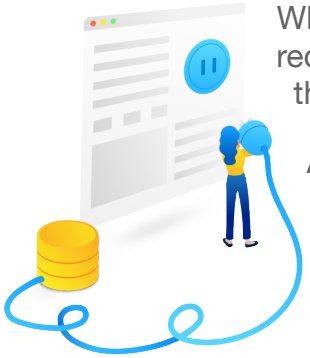
THE FASTEST WAY TO GET READY FOR A LEVEL 3+ CMMC AUDIT

Identify CUI, enforce governance, secure your data

How CMMC works and what it means to the defense sector

The Department of Defense (DoD) promulgated the Cybersecurity Maturity Model Certification (CMMC) to improve cybersecurity across the Defense Industrial Base (DIB). It puts cybersecurity as a first-class citizen in acquisition activities to enhance the protection of Controlled Unclassified Information (CUI) within the DIB supply chain.

From 2021, the CMMC will be implemented in a phased rollout until 2026, when all contracts will require CMMC certification. There are expected to be around 1,500 prime contractors requiring CMMC certification in 2021 and 48,000 by 2026. While there are lower CMMC certification levels, level 3 is the minimum requirement to show the ability to protect CUI and to have implemented the NIST SP 800-171 security requirements.



Although the different levels of CMMC are designed to accommodate for the diversity of acquisition activities and members of the DIB, level 3+ is expected to play a key role in DIB procurement and acquisition procedures in the future.

A company may not self-certify and must be audited by a certified third-party assessment organization (C3PAO). To get ready for a Level 3 audit, there are a number of steps an organization needs to take.

1. Examine your current security posture and document your existing security policies, data taxonomies, and controls.

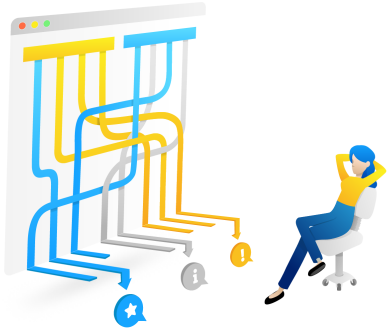
2. Actually confirming those policies, taxonomies, and controls over time as data changes and new projects come online.

3. Demonstrate those controls to a C3PAO (as of late 2020, no C3PAOs have yet been credentialed by DoD) in an audit environment.

Get ready by understanding your data

At its heart, the CMMC is about data—where it comes in, how it is stored, and how it is retired. With a modern data stack with possibly several petabytes of data across network drives, cloud storage, databases, and more, classifying what data you have and how it conforms to your declared policies and taxonomies can be a daunting task. If done manually, this initial classification may take years and with data changing every day, still only provide a snapshot of your true security posture.

OHALO



An automated solution to get CMMC Level 3+ ready

The CMMC Level 3+ presents many challenges for those in the DIB but these challenges are surmountable. Ohalo's Data X-Ray automated CUI identification algorithms means that you can quickly achieve proof points in preparation for your CMMC audit. We have data labeling tools that help you keep that classification up to date over time as your data changes by the second and we also have full integrations with data catalogs like Collibra if you want to power your data governance even further.

Data X-Ray: achieving key proof points in days through automated data classification

Ohalo's Data X-Ray connects to native datasources from network drives to cloud storage and has a full API suite to deal with data in motion. The Data X-Ray's machine learning powered crawler comes with a base CUI-tuned (hard matches as well as probable) algorithm that you can customize with data that is specific to your organization. Since the Data X-Ray is always crawling your data, you can be assured that data is identified from the time it is connected and every minute of the day.

The Data X-Ray seamlessly integrates to your data governance platform to ensure that decisions are recorded and responsibilities are properly allocated so that actions can be taken if anomalies are detected.

Applied to CMMC audit preparation, the power of Data X-Ray's automated unstructured data classification, means that your organization will be able to look across petabytes of data across dozens of silos to ensure that you will be ready for your CMMC audit and to respond to future DoD RFPs.

SCHEDULE A DEMO TODAY

Kyle DuPont, kyle@ohalo.co (+1 415 800 2913) or ohalo.co/demo

OHALO