CMMC 2.0: What You Need to Know

To provide solutions to the US DoD, certain security standards must be adhered to. This guidance is evolving in the form of the Cybersecurity Maturity Model Certification (CMMC) framework, a revised 2.0 version of which has just been released. But what is CMMC, and how do defense contractors ensure they are compliant? We explore more in this blog.

What is the history of CMMC?

A notable rise in government-targeted cybercrime has been identified in recent years, particularly state-sponsored attacks that are increasingly sophisticated in their execution. Attackers began to specifically hunt for data, potentially compromising US national security.

In 2019 it was determined that existing cybersecurity guidance needed to be solidified further, at which point the Cybersecurity Maturity Model Certification (CMMC) was introduced, which has NIST 800-171 at the heart of it (more below). CMMC proposed a level-based approach for DoD contractors and was due to roll out in 2021.

The initial framework covered requirements for the safeguarding of the separation of data, access to data, physical security – i.e. access granted to buildings that handle data – and workflows, ensuring they adhered to the framework requirements.

The CMMC ranged from levels one through five, with level one being the ability to demonstrate a basic level of network and physical security hygiene. Level three showed that the contractor had implemented the guidance of NIST 800-171 from a technical implementation point of view, as well as adding

additional policies and procedures around that.

Level five, meanwhile, applied mainly to prime contractors that deliver complex programs to the DoD and needed to show full compliance. Levels two and four were transitionary stages to levels three and five, respectively.

Importantly, CMMC introduced a certification process for all companies to prove they are compliant with the standard, and only by keeping up with your certification would you be able to bid on defense contracts.

For small and medium enterprises, this process posed challenges, and a potentially disproportionate amount of work would have to be carried out to win small pieces of work.

It also posed a heavy burden on the government to ensure that companies were certified in time for the 2025 deadline by which the majority of contracts would contain a CMMC certification clause.

While everybody agrees that cybersecurity compliance is essential to the interests of the DoD, companies called for a more accessible approach to demonstrating this compliance.

What is CMMC 2.0?

On November 4, 2021 the Pentagon announced a revised CMMC 2.0, which maintains the original framework's goal of safeguarding sensitive information, but eases the burden on contractors and simplifies the process they have to follow.

So what are the major changes and implications from CMMC 1.0 to CMMC 2.0?

The tiers have been reduced from five to three, namely:

- **Level 1**, a foundational level (also level one in the first iteration of CMMC);

- **Level 2**, an advanced level (replacing level three); and
- **Level 3**, an expert level (replacing level five).

Additionally, CMMC 2.0 waives the mandate for *all* contractors to be certified. Companies planning to achieve level one and subsets of level two requirements no longer need to be externally examined, but can instead self-assess against the clearly articulated cybersecurity standards.

Only the contractors managing information critical to national security – which will be categorized as a subset of level 2 – will be required to undergo third-party assessments. And all level three programs will require triannual assessments because they are critical defense acquisitions.

Another significant change is the removal of the hard requirement that contractors need to have certification in order to win any contracts. Plan of action & milestones (POA&M) with a firm timeline will be accepted for contracts, showing that companies have a timeline of when they expect to implement changes required to achieve particular levels.

While more information on the framework is expected to be released shortly, CMMC 2.0 is already showing itself to be a more simplified and achievable approach to safeguarding Controlled Unclassified Information (CUI). We also know that NIST 800-171 still remains at the heart of the DoD's guidance and all its future frameworks.

What is NIST 800-171?

Security safeguard requirements such as multi-factor authentication are now commonplace, and more often than not, access to applications and online accounts needs to be verified in multiple ways before being granted.

But why is this important for defense? If cybersecurity is now a vital function for commercial devices, then the requirements

for the safeguarding of government-level systems that process sensitive national security information must be an order of magnitude higher.

In the case of the US Department of Defense, defense contractors must adhere to the National Institute of Technology and Security's (NIST) 800-171 Special Publication, which outlines the technical practices that contractors should follow to protect any networked systems from potential security breaches.

The 800-171 framework is mandated under Defense Federal Acquisition Regulation Supplement – or DFARS – regulation 7012, and covers all CUI, which is information either created or owned by the US government.

This has become the standard in the security and cybersecurity industry for implementing good cybersecurity hygiene practice and required if supplying to federal or state agencies.

Where does Elotek fit in and what are we doing?

We strongly believe in the importance of implementing best security practices at Elotek, so we have achieved level two adherence under CMMC 2.0. In order to continue to provide value to our customers and manufacturers, and to protect their sensitive data, we have also upgraded Office 365 to GCC High and our SalesForce to Government Cloud.